

Lag om flygpassageraravgifter i brottsbekämpningen

Betänkande av PNR-utredningen

Stockholm 2017



STATENS OFFENTLIGA
UTREDNINGAR

SOU 2017:57

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.

Svara på remiss – hur och varför

Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).

En kort handledning för dem som ska svara på remiss.

Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet

Omslag: Elanders Sverige AB

Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24637-5

ISSN 0375-250X

Till statsrådet Anders Ygeman

Den 17 mars 2016 bemyndigade regeringen statsrådet Ygeman att tillkalla en särskild utredare med uppdrag att föreslå hur EU:s direktiv om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och tillhörande överenskommelser ska genomföras i svensk rätt. Regeringen beslutade samtidigt om direktiv för utredningen (dir. 2016:22).

Till särskild utredare förordnades från och med den 17 mars 2016 rådmannen Anna Tansjö.

Till sakkunniga att biträda utredningen förordnades från och med den 18 mars 2016 ämnesrådet Gabriela Kalm, Finansdepartementet, och rättsakkunniga Ida Salomonsson, Justitiedepartementet. Till experter utsågs samma dag den seniora strategiska rådgivaren Kurt Alavaara, Säkerhetspolisen, juristen Johnny Andersson, Transportstyrelsen, den nationella specialisten Mats Pettersson, Tullverket, tf. enhetschefen Karin Tollbäck, Säkerhets- och integritetsskyddsnämnden, och handläggaren Britt-Louise Wahlberg, Polismyndigheten. Juristen Eric Åmell, Polismyndigheten, förordnades som expert i utredningen från och med den 21 oktober 2016.

Hovrättsassessorn Anna-Karin Leo har varit sekreterare i utredningen från och med den 15 april 2016.

Utredningen har antagit namnet PNR-utredningen (Ju 2016:07). Härmed överlämnas betänkandet Lag om flygpassageraruppgifter i brottsbekämpningen, SOU 2017:57.

Till betänkandet har fogats ett särskilt yttrande av experterna Kurt Alavaara, Britt-Louise Wahlberg och Eric Åmell. Med undantag från vad som framgår där har de sakkunniga och experterna i huvudsak ställt sig bakom utredningens överväganden och förslag.

Uppdraget är härmed slutfört.

Höganäs i juni 2017

Anna Tansjö

/Anna-Karin Leo

Innehåll

Förkortningar	19
Sammanfattning	21
Summary	31
1 Författningsförslag	41
1.1 Förslag till lag (2018:000) om flygpassageraravgifter i brottsbekämpningen.....	41
1.2 Förslag till förordning (2018:000) om flygpassageraravgifter i brottsbekämpningen.....	58
1.3 Förslag till lag om ändring i polislagen (1984:387).....	64
1.4 Förslag till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen.....	65
1.5 Förslag till lag om ändring i lagen (2007:258) om behandling av personavgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.....	66
1.6 Förslag till lag om ändring i polisdatalagen (2010:361).....	67
1.7 Förslag till lag om ändring i tullagen (2016:253)	68
1.8 Förslag till lag om ändring i tullbrottsdatalagen (2017:000).....	69

2	Inledning	71
2.1	Uppdraget	71
2.2	Arbetets genomförande	72
3	PNR-direktivet och överenskommelser i anledning av direktivet	73
3.1	Allmänt om direktivet	73
3.2	Bakgrund	74
3.3	Direktivets innehåll i korthet	76
3.4	Överenskommelser i anledning av direktivet	80
4	Transportörsansvaret och API-direktivet	81
4.1	Inledning	81
4.2	Internationella åtaganden på området	82
4.2.1	Chicagokonventionen	82
4.2.2	FN:s resolution 2178	83
4.3	Vissa EU-rättsliga åtaganden	84
4.3.1	Schengenkonventionen och direktivet om transportörsansvar	84
4.3.2	Kodex om Schengen gränserna	85
4.4	Svenska regler om transportörsansvar	85
4.4.1	Bakgrund	85
4.4.2	Utlänningslagens bestämmelser om transportörsansvar	86
4.4.3	Befälhavares skyldigheter	87
4.5	API-direktivet och dess genomförande i svensk rätt	87
4.5.1	API-direktivet	87
4.5.2	API-direktivets genomförande i utlänningslagen	88
4.5.3	Lagen om passagerarregister	89

5	Dagens reglering och användning av flygpassageraruppgifter i brottsbekämpningen	91
5.1	Inledning.....	91
5.2	Tillämpliga bestämmelser	92
5.2.1	Polismyndigheten och Säkerhetspolisen.....	92
5.2.2	Tullverket.....	93
5.3	Dagens användning av PNR-uppgifter.....	95
5.3.1	Polismyndigheten.....	95
5.3.2	Säkerhetspolisen	95
5.3.3	Tullverket.....	96
6	Dataskyddsreglering.....	99
6.1	Internationella konventioner	99
6.1.1	Europakonventionen m.m.	99
6.1.2	Dataskyddskonventionen	99
6.2	Gällande EU-rättslig reglering	100
6.2.1	EU-stadgan om de grundläggande rättigheterna.....	100
6.2.2	Dataskyddsdirektivet	101
6.2.3	Dataskyddsrambeslutet.....	101
6.3	Huvuddragen i den svenska regleringen.....	102
6.3.1	Regeringsformen	102
6.3.2	Personuppgiftslagen	103
6.4	Aktuella särregleringar.....	108
6.4.1	Polisdatalagen	108
6.4.2	Tullbrottsdatalag.....	111
6.4.3	Lagen om internationellt polisiärt samarbete	113
6.4.4	Lagen om internationellt tullsamarbete	114
6.4.5	2013 års lag.....	114
6.5	EU:s dataskyddsreform.....	115
6.5.1	Bakgrund till reformen.....	115
6.5.2	En dataskyddsförordning.....	116
6.5.3	Ett nytt dataskyddsdirektiv	117
6.5.4	Viss personuppgiftsbehandling faller utanför båda instrumenten	118

7	Pågående arbeten	121
7.1	Internationellt arbete.....	121
7.1.1	Arbete inom PNRGOV Working Group	122
7.1.2	Arbete inom EU.....	122
7.2	Arbete i Sverige.....	124
7.2.1	Arbete med att upprätta en nationell enhet för passageraruppgifter	124
7.2.2	Arbetet med direktivets tekniska bestämmelser	125

VÅRA ÖVERVÄGANDEN OCH FÖRSLAG

8	Utgångspunkter och inledande ställningstaganden	129
8.1	Allmänt om att genomföra EU-direktiv	129
8.2	En samlad ny lag	130
8.3	Normgivningsnivå	131
8.4	En grundläggande allmän utgångspunkt	133
8.5	Den nya lagstiftningens förhållande till relevant dataskyddsreglering.....	134
9	Den nya lagens inledande bestämmelser	147
9.1	Den nya lagens namn, innehåll och syfte.....	147
9.2	Definitioner i lagen.....	151
9.3	Terroristbrott.....	152
9.3.1	Bakgrund.....	153
9.3.2	Våra överväganden och förslag.....	154
9.4	Grov brottslighet.....	156
9.4.1	Bakgrund.....	157
9.4.2	Våra överväganden och förslag.....	158
9.5	Otillåten behandling av PNR-information.....	160
10	En enhet för passagerarinformation	163
10.1	Direktivets bestämmelser.....	163
10.2	Den svenska enheten för passagerarinformation.....	164

10.3	Enhetens organisation och utredningens uppdrag.....	166
10.4	Tillgången till PNR-information bör begränsas	168
10.4.1	Direktåtkomst	168
10.4.2	Sekretess inom Polismyndigheten?	170
10.4.3	Begränsningar via dataskyddsbestämmelser m.m.....	174
10.5	Personal anställd vid andra myndigheter.....	179
11	Luftrafikföretagens överföring av PNR-uppgifter.....	183
11.1	Om luftrafikföretag.....	183
11.1.1	Olika former av kommersiell luftfart för befordran av passagerare	183
11.1.2	Tillstånd att bedriva passagerarflygtrafik.....	184
11.1.3	Luftrafikföretagens resor till och från Sverige ...	187
11.2	Luftrafikföretagens insamlande av PNR-uppgifter.....	187
11.3	Vilka luftrafikföretag ska åläggas en skyldighet att överföra PNR-uppgifter?.....	189
11.4	Överföring av PNR-uppgifter till enheten för passagerarinformation	193
11.4.1	Omfattningen av vårt uppdrag	193
11.4.2	Överföring av uppgifter avseende flygresor både inom och utom EU.....	194
11.4.3	PNR-uppgifter och passagerare.....	197
11.4.4	PNR-uppgifter som ska överföras.....	198
11.4.5	Överföringar ska ske vid två tillfällen	202
11.4.6	Överföringar vid andra tidpunkter.....	203
11.4.7	Hur överföringarna ska gå till.....	205
11.4.8	Anlitande av personuppgiftsbiträde	208
12	Resebyråer och researrangörer	209
12.1	Medlemsstaternas överenskommelse och vårt uppdrag	209
12.2	Resebyråer och researrangörer.....	210
12.2.1	Resebyråers och researrangörers insamling och överföring av PNR-uppgifter till luftrafikföretag	213

12.2.2	Behöriga myndigheter vill kunna få tillgång till samtliga insamlade PNR-uppgifter	215
12.2.3	Insamling av PNR-uppgifter från resebyråer och researrangörer i dagsläget	215
12.3	Våra överväganden.....	216
13	Behandling av PNR-uppgifter vid enheten för passagerarinformation	225
13.1	En databas för PNR-uppgifter.....	225
13.2	Ändamål för behandling av PNR-uppgifter.....	226
13.2.1	PNR-uppgifterna får behandlas för att utföra förhandsbedömningar.....	228
13.2.2	Förfarandet vid förhandsbedömningar.....	230
13.2.3	PNR-uppgifterna får behandlas för att överföra PNR-information till behöriga mottagare och tredjeland	235
13.2.4	PNR-uppgifterna får behandlas för att utforma kriterier.....	237
13.2.5	PNR-information som tas emot från andra medlemsstaters enheter för passagerarinformation.....	238
13.3	Maskering av PNR-uppgifter.....	239
13.3.1	Direktivets bestämmelser	240
13.3.2	Våra överväganden och förslag.....	241
13.4	Begränsad tillgång till maskerade uppgifter	243
14	PNR-direktivets förhållande till API-direktivet och dess genomförande i svensk rätt.....	245
14.1	PNR- och API-uppgifter	245
14.2	Vårt uppdrag i denna del.....	247
14.3	Direktivens olika mål och syften.....	248
14.3.1	Innebörden av den personkontroll som görs inom ramen för gränskontrollen	249

14.4	Överföring av API-uppgifter ska ske även enligt PNR-direktivet	251
14.5	Skillnader mellan PNR- och API-direktiven	251
14.6	Våra överväganden	254
14.6.1	Hur PNR-direktivet påverkar det svenska genomförandet av API-direktivet	254
14.6.2	Är en samordnad hantering av PNR- och API-uppgifter möjlig?	255
15	Enhetens överföring och utbyte av PNR-information	261
15.1	Inledning.....	261
15.2	Överföring av PNR-information till behöriga nationella myndigheter	262
15.2.1	Behörig myndighet	262
15.2.2	Överföring av PNR-information till behöriga myndigheter	263
15.3	Utbyte av PNR-information med andra medlemsstater	269
15.3.1	Medlemsstat	269
15.3.2	Utbyte mellan medlemsstaternas enheter för passagerarinformation	270
15.3.3	Överföring på direkt begäran från en behörig myndighet i en annan medlemsstat	276
15.3.4	Enhetens inhämtande av PNR-uppgifter från andra medlemsstaters motsvarande enheter	277
15.3.5	Former för informationsutbytet	278
15.4	Europols tillgång till PNR-information	279
15.4.1	Europol och dess verksamhet	279
15.4.2	Europolförordningen	280
15.4.3	Direktivets bestämmelser.....	282
15.4.4	Våra överväganden och förslag	283
15.5	Överföring av avmaskerade PNR-uppgifter	285
15.5.1	Direktivets bestämmelser.....	285
15.5.2	Vilka överföringar kräver att särskilda förutsättningar är uppfyllda?	287
15.5.3	Vilken prövning ska enheten göra?	288

15.5.4	Vem ska lämna tillstånd till överföring av fullständiga uppgifter?.....	289
16	Behöriga myndigheters behandling av PNR-information	307
16.1	Behöriga myndigheters rätt att motta och begära tillgång till PNR-information.....	307
16.1.1	Behöriga myndigheters rätt att motta PNR-information.....	308
16.1.2	Behöriga myndigheters möjlighet att begära tillgång till PNR-information.....	308
16.1.3	Våra överväganden och förslag.....	309
16.2	Behandling av PNR-information vid de behöriga myndigheterna.....	311
16.2.1	Tillämpliga dataskyddsbestämmelser hos de behöriga myndigheterna.....	311
16.2.2	Våra generella överväganden i denna del	312
16.2.3	Myndigheternas behandling av den överförda PNR-informationen.....	314
16.2.4	Automatiserade beslut	316
17	Överföring till tredjeland.....	319
17.1	Direktivets bestämmelser.....	319
17.2	Bakgrund.....	320
17.2.1	Dataskyddsrambeslutet och 2013 års lag.....	320
17.2.2	Brottsdatalagen.....	322
17.3	Våra överväganden och förslag	324
17.3.1	Grundläggande begrepp.....	324
17.3.2	Förutsättningar för överföring till tredjeland	325
17.3.3	Överföring utan medgivande	330
17.3.4	Säkerställande av direktivets bestämmelser	332
18	Lagringstid och gallring	335
18.1	Inledning.....	335
18.2	Rättslig bakgrund	335

18.2.1	Gällande rätt	336
18.2.2	Brottsdatalagen	340
18.3	Inledande radering hos enheten för passagerarinformation	341
18.3.1	Direktivets bestämmelser.....	341
18.3.2	Våra överväganden och förslag	341
18.4	Lagringstiden hos enheten för passagerarinformation för PNR-uppgifter som mottagits från lufttrafikföretag	343
18.4.1	Direktivets bestämmelser.....	343
18.4.2	Våra överväganden och förslag	343
18.5	Radering av PNR-uppgifter som utgör känsliga personuppgifter.....	345
18.5.1	Direktivets bestämmelser.....	345
18.5.2	Allmänt om känsliga personuppgifter.....	345
18.5.3	PNR-uppgifter som kan utgöra känsliga personuppgifter	346
18.5.4	Våra överväganden och förslag	347
18.6	Enhetens bevarande och gallring av resultatet av en förhandsbedömning	349
18.6.1	Direktivets bestämmelser.....	349
18.6.2	Våra överväganden och förslag	350
18.7	Enhetens bevarande och gallring av resultat av behandling av PNR-uppgifter på begäran.....	353
18.8	Bevarande och gallring av PNR-information hos behöriga myndigheter.....	354
18.8.1	Direktivets bestämmelser.....	354
18.8.2	Våra överväganden och förslag	355
19	Personuppgiftsansvarigas skyldigheter	357
19.1	Personuppgiftsansvar.....	357
19.1.1	Direktivets bestämmelser.....	357
19.1.2	Nya dataskyddsdirektivet och brottsdatalagen ...	358
19.1.3	Våra överväganden och förslag	358
19.2	Generella datasäkerhetsbestämmelser	361
19.2.1	Direktivets bestämmelser.....	361

19.2.2	Dataskyddsrambeslutet och dess genomförande i svensk rätt	362
19.2.3	Brottsdatalagen.....	363
19.2.4	Våra överväganden och förslag.....	364
19.3	Bevarande av dokumentation och loggning.....	365
19.3.1	Direktivets bestämmelser	365
19.3.2	Nuvarande reglering.....	367
19.3.3	Brottsdatalagen.....	368
19.3.4	Våra överväganden och förslag.....	369
19.4	Personuppgiftsincident	372
19.4.1	Direktivets bestämmelser	372
19.4.2	Nuvarande reglering.....	373
19.4.3	Brottsdatalagen.....	373
19.4.4	Våra överväganden	375
19.5	Dataskyddsombud.....	377
19.5.1	Direktivets bestämmelser	377
19.5.2	Nuvarande reglering.....	378
19.5.3	Brottsdatalagen.....	378
19.5.4	Våra överväganden och förslag.....	379
20	Enskildas rättigheter	383
20.1	Direktivets bestämmelser.....	383
20.2	Rätten till information	384
20.2.1	Dataskyddsrambeslutet	384
20.2.2	Brottsdatalagen.....	384
20.2.3	Dataskyddsförordningen.....	387
20.2.4	Våra överväganden och förslag.....	388
20.3	Rätt till rättelse, radering eller begränsning av behandlingen av uppgifter	391
20.3.1	Dataskyddsrambeslutet	391
20.3.2	Brottsdatalagen.....	392
20.3.3	Våra överväganden och förslag.....	393
20.4	Rätt till ersättning.....	395
20.4.1	Dataskyddsrambeslutet	395
20.4.2	Brottsdatalagen.....	395

20.4.3	Våra överväganden och förslag	396
20.5	Rätt till rättsmedel	396
20.5.1	Dataskyddsrambeslutet	396
20.5.2	Brottsdatalagen	397
20.5.3	Våra överväganden och förslag	398
21	Tillsyn	399
21.1	Direktivets bestämmelser	399
21.2	Bakgrund	400
21.2.1	Dagens tillsyn över behandling av personuppgifter	400
21.2.2	Förslag om förändrat tillsynsansvar	402
21.2.3	Dataskyddsrambeslutet	403
21.2.4	Brottsdatalagen	403
21.2.5	Dataskyddsförordningen	407
21.3	Våra överväganden och förslag.....	407
22	Sanktioner	411
22.1	Direktivets bestämmelser och vårt uppdrag.....	411
22.2	Olika typer av sanktioner	412
22.3	Sanktioner mot lufttrafikföretag.....	413
22.3.1	Chicagokonventionens bestämmelser.....	413
22.3.2	Jämförbara nationella sanktionsbestämmelser	414
22.3.3	Sanktioner som tillämpas i andra länder.....	419
22.3.4	Valet av sanktionsform.....	420
22.3.5	När ska sanktionsavgift få användas?	423
22.3.6	Utformningen av sanktionsavgiftssystemet	425
22.3.7	Förfarandet vid beslut om sanktionsavgift	429
22.4	Sanktioner vid felaktig behandling av PNR-uppgifter	433
22.4.1	Dagens sanktionssystem vid felaktig behandling av personuppgifter	433
22.4.2	Administrativa sanktionsavgifter enligt brottsdatalagen	434
22.4.3	Sanktionsavgiftssystemet i brottsdatalagen bör användas	436

23	Bestämmelser i direktivet som inte kräver lagstiftningsåtgärder	441
24	Sekretess	443
24.1	Vårt uppdrag i denna del	443
24.2	Sekretess i brottsbekämpande verksamhet m.m.....	444
24.3	Våra överväganden.....	451
24.3.1	Skyddet för PNR-information hos enheten för passagerarinformation.....	451
24.3.2	Skyddet för PNR-information hos behöriga myndigheter.....	454
24.3.3	Behövs nya sekretessbrytande bestämmelser?	456
25	PNR-direktivets betydelse för den nuvarande regleringen.....	459
25.1	Nuvarande reglering.....	459
25.2	Våra överväganden och förslag	461
26	Konsekvenser	465
26.1	Inledning	465
26.2	En effektiv användning av PNR-uppgifter i brottsbekämpningen	466
26.3	Konsekvenser för lufttrafikföretagen.....	467
26.4	Konsekvenser för staten.....	471
26.5	Konsekvenser för enskilda	473
26.6	Konsekvenser i övrigt.....	475
27	Ikraftträdande	477
28	Författningskommentar	479
28.1	Förslaget till lag om flygpassageraruppgifter i brottsbekämpningen	479

28.2	Förslaget till lag om ändring i polislagen (1984:387)	515
28.3	Förslaget till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen	515
28.4	Förslaget till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.....	516
28.5	Förslaget till lag om ändring i polisdatalagen (2010:361)...	516
28.6	Förslaget till lag om ändring i tullagen (2016:253)	517
28.7	Förslaget till lag om ändring i tullbrottsdatalagen (2017:000).....	517

Särskilt yttrande 519

Bilagor

Bilaga 1	Kommittédirektiv 2016:22	521
Bilaga 2	Europaparlamentets och rådets direktiv (EU) 2016/681	529
Bilaga 3	Rättelse till Europaparlamentets och rådets direktiv (EU) 2016/681	547
Bilaga 4	Uttalande från Europeiska unionens råd.....	549

Förkortningar

BDL	brottsdatalagen (2018:000), förslag till ramlag för genomförande av det nya dataskyddsdirektivet, lämnat av Utredningen om 2016 års dataskyddsdirektiv (SOU 2017:29)
BDF	brottsdataförordningen (2018:000), den till den föreslagna brottsdatalagen tillhörande förordningen
dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
dataskyddsrambeslutet	rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete
dir.	direktiv
Ds	Departementsserien
EU	Europeiska unionen
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna

FN	Förenta Nationerna
JK	Justitiekanslern
JO	Justitieombudsmannen
Ju	Justitiedepartementet
kommissionen	Europeiska kommissionen
nya dataskyddsdirektivet	Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF
OSL	offentlighets- och sekretesslagen (2009:400)
prop.	regeringens proposition
PDL	polisdatalagen (2010:361)
PDF	polisdataförordningen (2010:1155)
PUF	personuppgiftsförordningen (1998:1191)
PUL	personuppgiftslagen (1998:204)
RF	regeringsformen
RB	rättegångsbalken
SOU	Statens offentliga utredningar
TBL	tullbrottsdatalagen (2017:000), som träder i kraft den 1 juli 2017
TF	tryckfrihetsförordningen

Sammanfattning

PNR-direktivet

Den 27 april 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (nedan kallat PNR-direktivet).

PNR är en förkortning av den engelska benämningen Passenger Name Record. Det som åsyftas är uppgifter som passagerare lämnar vid beställning och bokning av flygresor samt vid incheckning. Uppgifterna kan till exempel avse namn, resedatum, resväg, bagageinformation och betalnings sätt. Lufttrafikföretagen samlar redan i dag in och behandlar sådana uppgifter om sina passagerare för sina egna operativa och kommersiella syften. PNR-uppgifter är också av intresse i det brottsbekämpande arbetet. Uppgifterna kan t.ex. användas för att sälla ut tidigare okända passagerare som skulle kunna vara intressanta för myndigheterna att kontrollera. PNR-uppgifterna kan även användas i samband med brottsutredningar eller för att analysera och fastställa misstänkta rese- och beteendemönster.

Myndigheter världen över har i allt större utsträckning börjat samla in PNR-uppgifter från lufttrafikföretag och analysera dem i syfte att bekämpa terrorism och grov brottslighet. För Sveriges del kan Polismyndigheten, Säkerhetspolisen och Tullverket redan i dag begära in vissa PNR-uppgifter från lufttrafikföretag och använda dessa för brottsbekämpande ändamål.

PNR-direktivet utgör ett unionsgemensamt regelverk för insamling och användning av PNR-uppgifter i viss brottsbekämpande verksamhet. Utredningens övergripande uppdrag är att lämna förslag till de lagändringar som krävs för att genomföra PNR-direktivet i svensk rätt.

En ny lag om flygpassageraruppgifter i brottsbekämpningen

Vi föreslår att PNR-direktivet i huvudsak ska genomföras i en ny lag, lagen om flygpassageraruppgifter i brottsbekämpningen. Lagen innehåller bestämmelser om lufttrafikföretags överföring av PNR-uppgifter till enheten för passagerarinformation och om behandlingen av PNR-uppgifter i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Syftet med lagen är att tillgodose behovet av tillgång till PNR-uppgifter i sådan verksamhet och att skydda människor mot att deras personliga integritet kränks vid behandling av uppgifter om dem.

Lagen, liksom det bakomliggande PNR-direktivet, innehåller såväl verksamhetsreglering som dataskyddsreglering. I sistnämnt avseende har vi bedömt det som lämpligast att anpassa författningsförslaget så långt möjligt till den dataskyddsreform som kommer att genomföras under våren 2018. Bestämmelserna i lagen kommer att gälla utöver eller i stället för de generella bestämmelserna i dataskyddsförordningen, den nya ramlag, brottsdatalagen, som föreslås genomföra det nya dataskyddsdirektivet (SOU 2017:29) och annan särreglering för dataskydd som gäller eller kommer att gälla för berörda myndigheter.

Lagen kompletteras med en förordning, som genomför vissa detaljbestämmelser i direktivet.

Otillåten behandling av PNR-information

Lagen innehåller en portalbestämmelse som anger att PNR-uppgifter som överförts från lufttrafikföretag eller resultatet av en enhet för passagerarinformations behandling av sådana uppgifter, dvs. PNR-information, inte får behandlas för andra syften än att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Terroristbrottslighet definieras i lagen som de brott enligt nationell rätt i Sverige eller andra medlemsstater som avses i artiklarna 1–4 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism. Med grov brottslighet avses de brott som anges i en förteckning i bilaga II till PNR-direktivet och för vilka det i nationell rätt i Sverige eller andra medlemsstater är föreskrivet fängelse i tre år eller mer.

Lagen innehåller också ett generellt förbud mot behandling av PNR-uppgifter som utgör känsliga personuppgifter. För det fall enheten för passagerarinformation eller en behörig myndighet mottar sådana uppgifter ska dessa genast raderas.

En enhet för passagerarinformation

Det ska enligt lagen finnas en enhet för passagerarinformation inom Polismyndigheten. Denna enhet har till övergripande uppgift att samla in PNR-uppgifter från lufttrafikföretag, lagra och behandla dessa uppgifter och överföra PNR-information till behöriga svenska myndigheter. Enheten ska också ansvara för utbytet av PNR-information inom EU.

PNR-uppgifter som behandlas av enheten ska inte vara direkt tillgängliga för behöriga myndigheter eller för övriga som arbetar inom Polismyndigheten. Direktåtkomst till PNR-information som behandlas vid enheten ska därför inte tillåtas. Inom enheten ska tillgången till PNR-information begränsas genom särskilda behörighetsbestämmelser.

Lufttrafikföretagens skyldigheter

PNR-uppgifter ska enligt lagen överföras från lufttrafikföretag som har en giltig operativ licens eller motsvarande som ger rätt att mot vederlag utföra lufttransporter av passagerare, och som i sin normala verksamhet samlar och hanterar PNR-uppgifter i reservationssystem. Som utgångspunkt utesluts från överföringsskyldighet flertalet mindre lufttrafikföretag som utför taxiflygningar från mindre flygstationer som saknar system för avgångskontroll av passagerare.

PNR-uppgifterna ska överföras elektroniskt till enheten för passagerarinformation. Vilka PNR-uppgifter som ska överföras framgår av en bilaga till lagen. Även s.k. API-uppgifter (se om dessa slags uppgifter nedan) ingår bland de PNR-uppgifter som ska överföras. Uppgifterna i bilagan ska dock endast överföras i de fall lufttrafikföretagen samlar in dem som en del av sin normala verksamhet. Lagen ålägger alltså inte lufttrafikföretagen att hämta in ytterligare PNR-uppgifter om sina passagerare utan endast att överföra sådana uppgifter som de redan har tillgång till.

PNR-uppgifterna ska normalt överföras vid två tillfällen inför varje flygning ankommande till eller avgående från Sverige. Den första överföringen ska ske 24–48 timmar före flygningens avgång och den andra överföringen omedelbart efter det att gatens dörrar har stängts. Överföringsskyldigheten omfattar såväl flygningar inom EU som flygningar till eller från tredjeland.

Ett lufttrafikföretag som inte har överfört PNR-uppgifter i enlighet med bestämmelserna i lagen eller föreskrifter som utfärdats i anslutning till lagen ska betala en sanktionsavgift. Sanktionsavgiften ska för varje flygning som har utförts utan att lufttrafikföretaget har fullgjort sin överföringsskyldighet bestämmas till minst 20 000 kronor och högst 100 000 kronor. Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Lufttrafikföretag ska informera passagerare om överföringen av PNR-uppgifter till enheten för passagerarinformation och om skälen till överföringen.

Behandling av PNR-uppgifter vid enheten för passagerarinformation

De PNR-uppgifter som har överförts till enheten för passagerarinformation från lufttrafikföretag ska lagras i en särskild databas vid enheten under fem års tid. Därefter ska de raderas. Efter sex månader ska PNR-uppgifterna i databasen maskeras, vilket innebär att tillgängliga uppgifter som direkt kan hänföras till en fysisk person ska göras osynliga för en användare som saknar särskild behörighet för tillgång till uppgifterna.

PNR-uppgifter som har överförts till enheten för passagerarinformation från lufttrafikföretag får endast behandlas för följande ändamål.

- **Förhandsbedömning:** Uppgifterna får behandlas för att enheten ska kunna göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från Sverige, för att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol (användning i realtid). Vid en sådan förhandsbedömning av passagerare får PNR-uppgifterna jämföras dels med uppgifter

i relevanta register eller andra uppgiftssamlingar, dels med på förhand fastställda kriterier.

- Besvara förfrågningar: Lagrade uppgifter får behandlas för att enheten för passagerarinformation ska kunna fullgöra sina uppgifter enligt lagen om att på begäran överföra PNR-information till behöriga mottagare (reaktiv användning).
- Utforma urvalskriterier: Uppgifterna får analyseras för att enheten ska kunna uppdatera eller skapa nya kriterier som ska användas vid förhandsbedömningar av passagerare.

Enheten för passagerarinformation kommer även att få del av PNR-information som har överförts till enheten från motsvarande enheter i andra medlemsstater. Sådan information får endast behandlas för att vidarebefordras till behöriga myndigheter.

Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som utförs vid enheten för passagerarinformation. Polismyndigheten ska utse ett dataskyddsombud för enheten för passagerarinformation. Ombudets uppgifter framgår av lagen.

Överföring av PNR-information från enheten för passagerarinformation

Enheten för passagerarinformation ska fungera som en nod vid vilken massan av PNR-uppgifter som lufttrafikföretagen överför tas emot, lagras och analyseras översiktligt. Endast sådan PNR-information som bedömts vara av intresse för att bekämpa terroristbrottslighet eller grov brottslighet ska därefter nå ut till behöriga myndigheter i det egna landet för vidare analys och åtgärder. Regeringen har utsett Polismyndigheten, Säkerhetspolisen, Tullverket, Ekobrottsmyndigheten och Försvarmakten såsom behöriga att ta emot och begära ut PNR-uppgifter från enheten för passagerarinformation. Ytterligare myndigheter kan komma att utses framöver. Enligt lagen ska enheten i enskilda fall överföra resultatet av sina förhandsbedömningar till en eller flera behöriga myndigheter så att de kan utföra en vidare granskning av PNR-informationen. Enheten ska också överföra PNR-information till behöriga myndigheter som svar på särskilda förfrågningar från en behörig myndighet. Vidare ska enheten vidarebefordra PNR-information som har mottagits från andra med-

lemsstaters enheter för passagerarinformation till behöriga myndigheter. En befattningshavare vid enheten ska alltid ha gjort en bedömning av PNR-informationen innan den lämnas från enheten.

Enheten för passagerarinformation ska enligt lagen även överföra PNR-information till motsvarande enheter i andra medlemsstater. Så ska ske om enheten vid en förhandsbedömning bedömt att viss information även är relevant och nödvändig för en annan medlemsstat. En överföring ska även ske till andra medlemsstater som svar på en begäran från den medlemsstaten. Vidare kan överföringar av PNR-information ske till Europol.

Lagen innehåller också bestämmelser om att enheten för passagerarinformation under vissa förutsättningar får överföra PNR-information till tredjeland.

Överföring av avmaskerade PNR-uppgifter, dvs. fullständiga PNR-uppgifter där personuppgifter tidigare genomgått en maskering, får bara ske om vissa närmare förutsättningar är uppfyllda. Om förundersökning pågår ska en begäran från en behörig myndighet om att få tillgång till avmaskerade PNR-uppgifter ha beslutats av allmän åklagare. I alla andra fall krävs att Polismyndighetens myndighetschef har godkänt utlämnandet. Rikspolischefen ska med vissa begränsningar kunna delegera beslutanderätten.

Behöriga myndigheters behandling av PNR-information

Det finns i lagen särskilda bestämmelser om behandling av PNR-information vid de behöriga myndigheterna. Bland annat anges att ett resultat av enheten för passagerarinformations förhandsbedömning av passagerare genast ska gallras av behöriga myndigheter om det visar sig sakna betydelse för något av de syften som anges i lagens portalbestämmelse. Vidare finns ett undantag från lagens portalbestämmelse om otillåten behandling av PNR-information. Om det har kommit fram uppgifter om annat slags brott än terroristbrottslighet eller grov brottslighet, s.k. överskottsinformation, i samband med en behörig myndighets insats som görs till följd av behandling av PNR-information, får uppgifterna användas för att förhindra, utreda eller lagföra det brottet.

Övriga bestämmelser

Direktivets krav på generella dataskyddsbestämmelser och rättigheter för enskilda omfattas i stor utsträckning av annan tillämplig dataskyddsreglering och behöver, med något undantag, inte särskilt regleras i den nya lagen.

Tillsyn över personuppgiftsbehandling enligt lagen ska utföras av tillsynsmyndigheten enligt den föreslagna brottsdatalagen och i enlighet med bestämmelserna om tillsyn i den lagen.

Sanktionsavgift får tas ut av personuppgiftsansvariga myndigheter vid överträdelse av vissa grundläggande bestämmelser i lagen som har till syfte att skydda enskildas integritet. Vid bestämmande av sanktionsavgiftens storlek och i handlägningsfrågor ska sanktionsavgiftssystemet i den föreslagna brottsdatalagen och den tillhörande förordningen tillämpas.

Sekretess

Befintlig sekretesslagstiftning bedöms ge ett tillfredsställande skydd för PNR-informationen såväl vid enheten för passagerarinformation som vid behöriga myndigheter. Någon ny eller ändrad sekretessreglering är inte motiverad. Inte heller behövs det någon särskild bestämmelse om sekretessgenombrott.

PNR-direktivets förhållande till API-direktivet

API-uppgifter (Advance Passenger Information) avser främst sådan information som finns på passets maskinläsbara del, såsom namn, födelsedatum, nationalitet och passnummer. API-uppgifter anses utgöra verifierbar information och används därför huvudsakligen som ett verktyg för identifiering. I rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare (nedan kallat API-direktivet) regleras transportörers ansvar för att på begäran förse nationella myndigheter med sådana passageraruppgifter inför resor från länder utanför Schengensamarbetet. Direktivet är i Sverige genomfört främst genom vissa bestämmelser i utlänningslagen (2005:716) samt genom lagen (2006:444) om passagerarregister.

Enligt PNR-direktivet ska lufttrafikföretagen överföra såväl PNR- som API-uppgifter till enheterna för passagerarinformation. Skyldigheten att överföra API-uppgifter följer således inte bara av API-direktivet utan även av PNR-direktivet. Det ingår i vårt uppdrag att analysera om och i så fall hur PNR-direktivet påverkar det svenska genomförandet av API-direktivet samt att föreslå hur systemet med flygpassageraruppgifter ska möjliggöra hantering av både PNR-uppgifter och API-uppgifter.

Enligt vår bedömning varken ersätter eller påverkar PNR-direktivet API-direktivet eller dess genomförande i Sverige. Direktiven och deras respektive genomföranden kommer därför att vara parallellt tillämpliga. Vi har vidare funnit att en samordnad hantering av PNR- och API-uppgifter vid enheten för passagerarinformation är möjlig även avseende API-uppgifter som behandlas enligt lagen om passagerarregister. Det kräver dock att API-uppgifter som behandlas enligt lagen om passagerarregister hålls isär från de API-uppgifter som överförs från lufttrafikföretagen enligt den nya lagen, att det alltid står klart för vilket syfte och enligt vilket regelverk API-uppgifter behandlas samt att det säkerställs att regelverkens olikheter i fråga om t.ex. tillgång till uppgifterna följs.

PNR-direktivets betydelse för den nuvarande regleringen

Genomförandet av direktivet får också en effekt på den nuvarande regleringen. Vi föreslår därför att det i polislagen (1984:387), tullagen (2016:253) och lagen (1996:701) om Tullverkets befogenhet vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränslagen) förs in bestämmelser som innebär att transportföretags skyldigheter enligt de lagarna att överföra bokningsuppgifter till Polismyndigheten, Säkerhetspolisen och Tullverket inte ska gälla när lagen om flygpassageraruppgifter i brottsbekämpningen är tillämplig.

Resebyråer och researrangörer

Medlemsstaterna har i en deklaration som antogs samtidigt som PNR-direktivet, angett att de, i enlighet med sin nationella lagstiftning och med förbehåll för parlamentsbehandling i vissa medlemsstater, åtar sig att utvidga insamlingen av PNR-uppgifter till att om-

fatta även aktörer som inte är lufttrafikföretag. Som exempel anges i deklARATIONEN resebyråer och researrangörer som tillhandahåller reserelaterade tjänster. Någon tidsgräns för när detta ska vara genomfört i nationell lagstiftning anges inte i deklARATIONEN. Enligt vår bedömning omfattas resebyråer och researrangörer redan av systemet med insamling av PNR-uppgifter eftersom de överför PNR-uppgifter till lufttrafikföretagen för vidare överföring till enheten för passagerarinformation. Ytterligare utvidgningar av detta system bör enligt vår mening tills vidare anstå. Frågan bör dock bevakas och eventuellt utredas vidare.

Konsekvenser

Förslagen innebär att fler PNR-uppgifter avseende enskilda flygresenärer kommer att samlas in i brottsbekämpande syfte, vilket vi bedömer kommer att få positiva konsekvenser för det brottsbekämpande arbetet. Förslagen innebär också att skyddet för enskildas personliga integritet vid de brottsbekämpande behöriga myndigheternas behandling av uppgifterna säkerställs.

Lufttrafikföretagen kommer att belastas arbets- och kostnads- mässigt av förslagen. Dock bedömer vi inte att deras konkurrensförhållanden kommer att påverkas i någon större omfattning. Vidare medför förslagen ökade kostnader för Polismyndigheten kopplade till inrättandet av en enhet för passagerarinformation och till drivandet av enheten. De ekonomiska konsekvenserna för Polismyndigheten och övriga berörda myndigheter bedöms dock rymmas inom de befintliga ekonomiska ramarna.

Ikraftträdande

Den nya lagen föreslås träda i kraft den 25 maj 2018.

Summary

The PNR Directive

On 27 April 2016, the European Parliament and the Council adopted Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (referred to below as the PNR Directive).

PNR refers to data provided by passengers when booking flights and during check-in. This data can include names, travel dates, route, luggage information and method of payment. Air carriers already collect and process such data about their passengers for their own operational and commercial purposes. PNR data is also of interest for law enforcement purposes. The data can be used, for example, to screen out previously unknown passengers who should be subject to further examinations by the authorities. PNR data can also be used in connection with criminal investigations or to analyse and establish suspicious travel and behavioural patterns.

Authorities all over the world have begun to collect more PNR data from air carriers and to analyse it for the purpose of combating terrorism and serious crime. In Sweden, the Swedish Police Authority, the Swedish Security Service and Swedish Customs are already permitted to request certain PNR data from air carriers and to use it for law enforcement purposes.

The PNR Directive is an EU-wide regulatory framework for the collection and use of PNR data in certain law enforcement activities. The Inquiry's overall remit is to present proposals on the legislative amendments necessary to implement the PNR Directive in Swedish law.

A new Act on air passenger data for law enforcement purposes

We propose that the PNR Directive should mainly be implemented through a new act, the Act on air passenger data for law enforcement purposes. This Act will contain provisions on the transfer by air carriers of PNR data to the passenger information unit and the processing of PNR data in activities for the prevention, detection, investigation and prosecution of terrorist offences or serious crime. The purpose of this Act is to meet the need for access to PNR data in such activities and protection of privacy in the processing of such data.

The Act, like the underlying PNR Directive, will contain regulations on both operations and data protection. Regarding the latter, we consider it most appropriate to adapt the legislative proposal as far as possible to the data protection reform that will be implemented in the first half of 2018. The provisions in the Act will apply in addition to, or instead of, the general provisions in the General Data Protection Regulation, the new framework law – the Criminal Data Act – which has been proposed to implement the new Data Protection Directive (SOU 2017:29), and other special regulations on data protection that apply or will apply to relevant authorities.

The Act will be accompanied by an ordinance implementing certain detailed provisions of the Directive.

Unlawful processing of PNR information

The Act will contain a preamble stating that PNR data transferred by air carriers or the results of a unit for the processing of such passenger information, i.e. PNR information, may not be processed for any purposes other than the prevention, detection, investigation and prosecution of terrorist offences or serious crime. Terrorist offences are defined in the Act as the offences referred to under domestic law in Sweden or other Member States in Articles 1–4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism. Serious crime refers to the offences listed in annex II of the PNR Directive, and for which domestic law in Sweden or other Member States prescribes imprisonment of three years or more.

The Act also contains a general ban on processing PNR data that is sensitive personal data. In the event that the passenger informa-

tion unit or a competent authority receives such data, it must be deleted immediately.

A passenger information unit

Under the Act, there will be a passenger information unit at the Swedish Police Authority. This unit will have responsibility for collecting PNR data from air carriers, storing and processing this data, and transferring PNR information to competent Swedish authorities. The unit will also be responsible for the exchange of PNR information within the EU.

PNR data that is processed by the unit will not be directly available to competent authorities or to others working at the Swedish Police Authority. Direct access to PNR information processed at the unit will therefore not be permitted. In this unit, access to PNR information will be restricted through special authorisation provisions.

Obligations on air carriers

Under the Act, PNR data should be transferred from air carriers with a valid operating licence or equivalent permitting them to carry out, with compensation, carriage of passengers by air, and that collect and process PNR data in reservation systems in their regular activities. One starting point is that the transfer obligation does not apply to the majority of small air carriers conducting taxi flights from small airfields that do not have departure control systems for passengers.

PNR data is to be transferred electronically to the passenger information unit. An annex to the Act specifies the PNR data to be transferred. ‘API’ data (see below for details about this kind of data) is included in the PNR data to be transferred. However, the data referred to in the annex may only be transferred when air carriers collect it as part of their regular activities. Therefore, the Act does not oblige air carriers to collect additional PNR data about their passengers; it simply states that they must transfer data to which they already have access.

PNR data should normally be transferred on two occasions prior to every flight arriving to or departing from Sweden. The first transfer should take place 24–48 hours before the flight departure, and the second transfer should take place immediately after the gate has been closed. The obligation to transfer data applies to flights both within the EU and to or from a third country.

An air carrier that has not transferred PNR data in accordance with the provisions in the Act or provisions issued in connection with the Act must pay a financial penalty. For every flight conducted without the air carrier fulfilling its transfer obligation, the financial penalty is set at a minimum of SEK 20 000 and a maximum of SEK 100 000. The financial penalty may be reduced or waived, in whole or in part, if the infringement is excusable, or if, in view of the circumstances, it would be unreasonable to impose the penalty.

Air carriers must inform passengers about the transfer of PNR data to the passenger information unit and the reasons for this transfer.

Processing of PNR data at the passenger information unit

The PNR data that has been transferred to the passenger information unit from air carriers must be stored in a special database at the unit for a period of five years. It must then be deleted. After six months, the PNR data in the database must be masked, which means that accessible data directly attributable to a natural person must be made invisible to users without special authorisation to access the data.

PNR data that has been transferred to the passenger information unit from air carriers may be processed for the following purposes only.

- Advance assessment: the data may be processed to enable the unit to conduct an assessment of passengers before their estimated arrival to or departure from Sweden so as to select individuals who need to be further investigated by competent authorities or Europol (use in real time). In this kind of advance assessment of passengers, PNR data may be compared with data in relevant databases or other data collections, and with pre-determined criteria.

- Responding to enquiries: stored data may be processed to enable the passenger information unit to fulfil its responsibility under the Act to transfer PNR information to competent recipients upon request (reactive use).
- Devising selection criteria: data may be analysed to enable the unit to update or create new criteria to be used when conducting advance assessments of passengers.

The passenger information unit will also have access to PNR information transferred to the unit from corresponding units in other Member States. This data may only be processed for further transfer to competent authorities.

The Swedish Police Authority is the personal data controller for the processing of personal data conducted at the passenger information unit. The Swedish Police Authority will appoint a data protection officer for the passenger information unit. The officer's duties are stated in the Act.

Transfer of PNR information from the passenger information unit

The passenger information unit will function as a hub at which the mass of PNR data transferred by air carriers is received, stored and superficially analysed. Only PNR information considered to be of interest for combating terrorist offences or serious crime will subsequently be made available to competent domestic authorities for further analysis and action. The Government has appointed the Swedish Police Authority, the Swedish Security Service, Swedish Customs, the Swedish Economic Crime Authority and the Swedish Armed Forces as competent authorities to receive and request PNR data from the passenger information unit. Additional agencies may be appointed in the future. Under the Act, the unit is required, in individual cases, to transfer the results of its advance assessments to one or several competent authorities so that they can conduct an additional examination of the PNR information. The unit should also transfer PNR information to competent authorities in response to special requests from a competent authority. Moreover, the unit should forward PNR information received from other Member States'

passenger information units to competent authorities. An official at the unit is required to have always carried out an assessment of the PNR information before it is disclosed by the unit.

Under the Act, the passenger information unit should also transfer PNR information to corresponding units in other Member States. This is what should be done if, after an advance assessment, the unit considers that certain information is also relevant and necessary for another Member State. Data should also be transferred to other Member States in response to a request from that Member State. Moreover, PNR information should be transferred to Europol.

The Act also contains provisions stating that the passenger information unit may transfer PNR information to a third country under certain conditions.

The transfer of unmasked PNR data, i.e. complete PNR data in which personal data has previously been masked, may only occur if certain more closely defined conditions have been met. If a preliminary investigation is under way, a request from a competent authority on gaining access to unmasked PNR data must have been approved by a public prosecutor. In all other cases, the disclosure must have been approved by the head of the Swedish Police Authority. The National Police Commissioner should be able to delegate the right to decide, subject to certain limitations.

Processing of PNR information by competent authorities

The Act will contain special provisions on the processing of PNR information by the competent authorities. They state, among other things, that the result of an advance assessment of passengers by the passenger information unit must be immediately deleted by competent authorities if it proves to be irrelevant for the purposes stated in the preamble to the Act. In addition, there is an exemption from the Act's preamble on the unlawful processing of PNR information. If information has emerged about some form of offence other than a terrorist offence or serious crime – known as 'excess disclosure' – in connection with a competent authority's actions as a result of having processed PNR information, this information may be used for the prevention, investigation and prosecution of the offence.

Other provisions

The Directive's requirements concerning general data protection provisions and the rights of individuals are largely met by other applicable data protection regulations, and need not – with the occasional exception – be regulated separately in the new Act.

Supervision of personal data processing under the Act should be carried out by the supervisory authority in accordance with the proposed Criminal Data Act and in line with the provisions on supervision in that Act.

A financial penalty may be charged by authorities acting as personal data controllers in the event of a breach of certain fundamental provisions in the Act intended to protect personal privacy. When determining the size of the financial penalty, and in processing issues, the financial penalty system in the proposed Criminal Data Act and the accompanying ordinance should be applied.

Secrecy

Current secrecy legislation is considered to provide sufficient protection for PNR information at both the passenger information unit and competent authorities. There is no need for any new or amended secrecy regulation. Nor is there any need for special provisions on secrecy exemptions.

How does the PNR Directive relate to the API Directive?

API (advance passenger information) data refers primarily to information contained in the machine-readable part of a passport, such as name, date of birth, nationality and passport number. API data is considered to constitute verifiable information and is therefore mainly used as a tool for identification purposes. Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (referred to below as the API Directive) regulates carriers' obligations to provide national authorities, upon request, with such passenger information ahead of travel from countries outside the Schengen area. In Sweden, the Directive has been implemented primarily through certain provisions of the

Aliens Act (2005:716) and through the Passenger Name Record Act (2006:444).

Under the PNR Directive, air carriers should transfer both PNR and API data to the passenger information units. Therefore, the obligation to transfer API data is imposed not only by the API Directive, but also by the PNR Directive. Our remit includes analysing whether and how the PNR Directive affects Sweden's implementation of the API Directive and proposing how the system of flight passenger data can enable processing of both PNR and API data.

In our view, the PNR Directive neither replaces nor affects the API Directive or its implementation in Sweden. The Directives and their implementation will therefore be applicable in parallel. We have also found that the coordinated processing of PNR and API data at the passenger information unit is possible, also with regard to API data processed under the Passenger Name Record Act. However, this requires that API data processed under the Passenger Name Record Act is kept separate from the API data transferred from air carriers under the new Act, that it is always clear which purpose and under which regulatory framework API data is processed, and that it is ensured that the differences in the regulatory frameworks concerning access to data, for example, are monitored.

Significance of the PNR Directive for the existing regulations

Implementation of the Directive will also have an effect on the existing regulations. We therefore propose that the Police Act (1984:387), the Customs Act (2016:253) and the Act on the powers of Swedish Customs at Sweden's borders with other European Union countries (1996:701) (the Internal Borders Act) include provisions requiring that obligations on air carriers under these acts to transfer booking data to the Swedish Police Authority, the Swedish Security Service and Swedish Customs should not apply when the Act on air passenger data in law enforcement is applicable.

Travel agencies and tour operators

In a declaration adopted at the same time as the PNR Directive, the Member States stated that they, in accordance with their national legislation and subject to parliamentary processing in certain Member States, undertake to expand the collection of PNR data to also apply to actors that are not air carriers. Examples given in the declaration include travel agencies and tour operators that offer travel-related services. The declaration gives no time limit for when this should be implemented in national legislation. In our view, travel agencies and tour operators are already covered by the system for collecting PNR data as they transfer PNR data to air carriers for further transfer to the passenger information unit. We consider that further expansions of this system should be deferred until further notice. However, the issue should be monitored and possibly investigated further.

Impact

The proposals would mean more PNR data concerning individual air passengers being collected for law enforcement purposes, which we consider would have a positive impact on law enforcement efforts. The proposals also mean that protection of personal privacy would be guaranteed in the competent law enforcement authorities' processing of data.

The proposals will add a burden in terms of work and costs for air carriers. However, we do not consider that their competitiveness will be affected to any great extent. In addition, the proposals would mean increased costs for the Swedish Police Authority linked to the establishment of a passenger information unit and the running of such a unit. However, the economic consequences for the Swedish Police Authority and other relevant authorities are deemed to fall within the existing economic framework.

Entry into force

It is proposed that the new Act enter into force on 25 May 2018.

1 Författningsförslag

1.1 Förslag till lag (2018:000) om flygpassageraruppgifter i brottsbekämpningen

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens innehåll

1 § Denna lag innehåller bestämmelser om lufttrafikföretags överföring av PNR-uppgifter till enheten för passagerarinformation och om behandlingen av PNR-uppgifter i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Genom denna lag genomförs Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (PNR-direktivet).

Lagens syfte

2 § Syftet med lagen är att tillgodose behovet av tillgång till PNR-uppgifter i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet och att skydda människor mot att deras personliga integritet kränks vid behandling av uppgifter om dem.

Definitioner

3 § I denna lag används följande uttryck med nedan angiven betydelse.

<i>Uttryck</i>	<i>Betydelse</i>
Avmaskerade PNR-uppgifter	Fullständiga flygpassageraruppgifter (PNR-uppgifter) där personuppgifter tidigare genomgått en maskering.
Behörig mottagare	En behörig myndighet, en enhet för passagerarinformation i en annan medlemsstat, en myndighet som har utsetts som behörig i en annan medlemsstat eller Europol.
Behörig myndighet	En sådan av regeringen utsedd myndighet som har behörighet att behandla PNR-information i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.
Flygpassageraruppgifter eller PNR-uppgifter	En sammanställning av uppgifter om varje enskild passagerare som gör det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen.
Grov brottslighet	De brott som anges i bilaga II till PNR-direktivet och för vilka det i nationell rätt i Sverige eller andra medlemsstater är föreskrivet fängelse i tre år eller mer.
Lufttrafikföretag	Ett lufttrafikföretag med giltig operativ licens eller motsvarande som ger rätt att mot vederlag utföra lufttransporter av passagerare, och som i sin normala

	verksamhet samlar och hanterar PNR-uppgifter i reservations-system.
Maskerade PNR-uppgifter	Personuppgifter som genomgått en maskering.
Maskering	Åtgärd som innebär att tillgängliga uppgifter som direkt kan hänföras till en fysisk person görs osynliga för en användare av ett informationssystem som saknar särskild behörighet för tillgång till uppgifterna.
Medlemsstat	En stat som är medlem i EU, med undantag för Danmark.
Passagerare	Alla personer, förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan och som finns upptagna i passagerarförteckningen.
PNR-information	PNR-uppgifter och resultatet av en enhet för passagerarinformations behandling av sådana uppgifter.
Reservationssystem	System där PNR-uppgifter samlas för hantering av reservationer.
Terroristbrottslighet	De brott enligt nationell rätt i Sverige eller andra medlemsstater som avses i artiklarna 1–4 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism.
Tredjeland	En stat som inte är en medlemsstat.

Enhet för passagerarinformation

4 § Det ska hos Polismyndigheten finnas en enhet för passagerarinformation. Enheten ska ansvara för att

1. samla in PNR-uppgifter från lufttrafikföretag, lagra och behandla dessa uppgifter och överföra PNR-information till behöriga myndigheter, och
2. utbyta PNR-information med andra behöriga mottagare.

Otillåten behandling av PNR-information

5 § PNR-uppgifter som har överförts från lufttrafikföretag enligt denna lag eller föreskrifter som meddelats i anslutning till lagen och resultatet av enheten för passagerarinformations behandling av sådana uppgifter får inte behandlas för andra syften än att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet, om inte annat anges i denna lag. Detsamma ska gälla PNR-information som har mottagits från en annan medlemsstat och som där samlats in och behandlats av en enhet för passagerarinformation enligt den nationella reglering som genomfört PNR-direktivet.

Förbud mot behandling av känsliga personuppgifter

6 § PNR-uppgifter som utgör sådana personuppgifter som avses i 2 kap. 11 § brottsdatalagen (2018:000)¹ får inte behandlas enligt denna lag.

2 kap. Lufttrafikföretagens skyldigheter

Överföring av PNR-uppgifter till enheten för passagerarinformation

1 § Lufttrafikföretag ska inför varje flygning ankommande till eller avgående från Sverige överföra samtliga de PNR-uppgifter som anges i bilagan till denna lag till enheten för passagerarinformation. PNR-

¹ Med hänvisningen avses förslaget till ramlag i SOU 2017:29.

uppgifterna ska dock endast överföras i de fall lufttrafikföretagen samlar in uppgifterna som en del av sin normala verksamhet.

Om flygningens linjebeteckning delas med ett eller flera andra lufttrafikföretag, ska det lufttrafikföretag som utför flygningen överföra PNR-uppgifter om samtliga passagerare.

2 § PNR-uppgifterna ska överföras

1. 24–48 timmar före flygningens avgång, och
2. omedelbart efter det att gatens dörrar har stängts.

Överföringar enligt första stycket 2 får begränsas till uppdateringar och kompletteringar av de uppgifter som överförts vid den tidpunkt som avses i första stycket 1.

3 § När det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet, ska lufttrafikföretag på begäran av enheten för passagerarinformation överföra PNR-uppgifter även vid andra tidpunkter än de som anges i 2 §.

4 § Lufttrafikföretagen ska överföra PNR-uppgifterna i elektronisk form. Enheten för passagerarinformation får inte medges direktåtkomst till lufttrafikföretagens uppgiftssamlingar med PNR-uppgifter.

5 § Den som är skyldig att överföra uppgifter enligt denna lag får anlita ett personuppgiftsbiträde för att utföra överföringen.

Information till passagerare

6 § Lufttrafikföretag ska informera passagerare om överföringen av PNR-uppgifter till enheten för passagerarinformation och om skälen till överföringen.

Sanktionsavgift för lufttrafikföretag

7 § Ett lufttrafikföretag som inte har överfört PNR-uppgifter enligt bestämmelserna i denna lag eller föreskrifter som utfärdats i anslutning till lagen ska betala en sanktionsavgift.

8 § Sanktionsavgiften ska för varje flygning som har utförts utan att lufttrafikföretaget har fullgjort sin överföringsskyldighet bestämmas till minst 20 000 kronor och högst 100 000 kronor.

Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

9 § Polismyndigheten beslutar om sanktionsavgift för lufttrafikföretag enligt denna lag.

Sanktionsavgiften tillfaller staten.

10 § Sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum.

11 § Polismyndighetens beslut om sanktionsavgift överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Föreskrifter

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om lufttrafikföretagens överföring av PNR-uppgifter till enheten för passagerarinformation samt om handläggningen av beslut om och verkställighet av sanktionsavgifter.

3 kap. Behandling av PNR-information vid enheten för passagerarinformation

PNR-databas

1 § PNR-uppgifter som överförs från lufttrafikföretag ska lagras i en databas vid enheten för passagerarinformation.

Personuppgiftsansvar m.m.

2 § Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som utförs vid enheten för passagerarinformation.

3 § Enheten för passagerarinformations behandling av PNR-uppgifter får inte ske utanför medlemsstaternas territorium.

Tillåtna ändamål

4 § Enheten för passagerarinformation får endast behandla PNR-uppgifter som anges i 1 § för följande ändamål:

1. Göra en förhandsbedömning av passagerare före deras beräknade ankomst till eller avresa från Sverige, för att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att dessa personer kan vara inblandade i terroristbrottslighet eller grov brottslighet.

2. I enskilda fall fullgöra sina uppgifter enligt 4 kap. att överföra PNR-information på eget initiativ eller för att besvara en begäran från en behörig mottagare.

3. Göra analyser för att uppdatera eller skapa nya kriterier som anges i 5 § 2.

Av 6 kap. framgår att PNR-uppgifter i vissa fall även får överföras till mottagare i tredjeland.

5 § Vid förhandsbedömning enligt 4 § första stycket 1 får PNR-uppgifter

1. jämföras med register eller andra uppgiftssamlingar som är relevanta för ett eller flera av de syften som anges i 1 kap. 5 §, eller

2. behandlas enligt på förhand utformade och fastställda kriterier som är riktade, proportionella och avgränsade och som inte grundas på sådana personuppgifter som avses i 2 kap. 11 § brottsdatalagen (2018:000).

6 § PNR-information som enheten för passagerarinformation tagit från motsvarande enheter i andra medlemsstater får endast behandlas för att vidarebefordra uppgifterna till behöriga myndigheter för fortsatt användning för ett eller flera av de syften som anges i 1 kap. 5 §.

Tillgång till PNR-information

7 § Endast den som tjänstgör vid enheten för passagerarinformation får ha tillgång till PNR-information som behandlas vid enheten. Tillgången ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter vid enheten.

Förbud mot direktåtkomst

8 § Direktåtkomst till PNR-information som behandlas vid enheten för passagerarinformation får inte tillåtas.

Bevarande och gallring av PNR-uppgifter

9 § PNR-uppgifter som lagras i databasen för PNR-uppgifter ska bevaras där i fem år från det att de kommit in från ett lufttrafikföretag. Därefter ska de gallras genom att raderas.

10 § PNR-uppgifter som utgör sådana personuppgifter som avses i 2 kap. 11 § brottsdatalagen (2018:000) ska genast gallras genom att raderas, om de kommer in till enheten för passagerarinformation.

Maskering av PNR-uppgifter

11 § Följande PNR-uppgifter ska maskeras i databasen för PNR-uppgifter sex månader efter att de kommit in från lufttrafikföretagen:

1. Alla namn på passagerare.
2. Antal passagerare som reser tillsammans.
3. Adress och kontaktuppgifter.
4. Alla former av betalningsinformation, inklusive faktureringsadress, om informationen innehåller uppgifter som kan användas för att direkt identifiera en person.
5. Uppgifter om bonusprogram.
6. Allmänna anmärkningar, om dessa innehåller uppgifter som kan användas för att direkt identifiera en passagerare.
7. Alla API-uppgifter.

Dataskyddsbud

12 § Polismyndigheten ska utse ett dataskyddsbud för enheten för passagerarinformation.

Dataskyddsbudet ska ha tillgång till alla uppgifter som behandlas vid enheten.

13 § Utöver de uppgifter som anges i 3 kap. 14 § brottsdatalagen (2018:000) ska dataskyddsbudet vid enheten för passagerarinformation ansvara för genomförandet av relevanta skyddsåtgärder.

Enskilda ska ha rätt att kontakta dataskyddsbudet i egenskap av enda kontaktpunkt i alla frågor som gäller behandling enligt denna lag av PNR-uppgifter om denne.

14 § Om dataskyddsbudet anser att enheten för passagerarinformation bryter mot bestämmelser för behandling av PNR-uppgifter, ska han eller hon anmäla det till tillsynsmyndigheten.

Föreskrifter

15 § Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. utformande av kriterier,
2. tillgång till PNR-information,
3. dataskyddsbudets uppgifter,
4. bevarande och gallring,
5. dokumentation och loggning,
6. information till dataskyddsbud, och
7. enheten för passagerarinformations inhämtande av PNR-information från andra medlemsstater.

4 kap. Överföring av PNR-information från enheten för passagerarinformation

Överföring till behöriga myndigheter

1 § Enheten för passagerarinformation ska i enskilda fall lämna PNR-information till en eller flera behöriga myndigheter för att

1. en vidare granskning ska ske av PNR-information rörande passagerare som valts ut vid en förhandsbedömning enligt 3 kap. 4 § första stycket 1,

2. besvara en motiverad begäran från en behörig myndighet om att tillhandahålla och behandla PNR-uppgifter för ett eller flera av de syften som anges i 1 kap. 5 § och tillhandahålla resultaten av sådan behandling, eller

3. vidarebefordra PNR-information som har mottagits från en motsvarande enhet i en annan medlemsstat.

En befattningshavare vid enheten ska ha gjort en bedömning av PNR-informationen innan den lämnas från enheten.

Överföring till andra medlemsstater

2 § Enheten för passagerarinformation ska till en motsvarande enhet i en annan medlemsstat överföra sådan PNR-information som behandlats för ändamålet förhandsbedömning enligt 3 kap. 4 § första stycket 1 och som bedömts relevant och nödvändig för vidare granskning i den andra medlemsstaten.

3 § Enheten för passagerarinformation ska så snart som möjligt besvara en motiverad begäran från en motsvarande enhet i en annan medlemsstat och överföra lagrade PNR-uppgifter och resultatet av en eventuell behandling enligt 3 kap. 4 § första stycket 1 av dessa uppgifter dit.

4 § Endast när det i ett enskilt brådsökande fall är absolut nödvändigt ska enheten för passagerarinformation besvara en motiverad begäran från en myndighet som har utsetts som behörig i en annan medlemsstat och överföra PNR-uppgifter och resultatet av en eventuell behandling enligt 3 kap. 4 § första stycket 1 av dessa uppgifter direkt till den myndigheten.

5 § När det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet, ska enheten för passagerarinformation på begäran av en motsvarande enhet i en annan medlemsstat inhämta PNR-uppgifter i enlighet med 2 kap. 3 § och överföra dessa till den begärande enheten.

Överföring till Europol

6 § Enheten för passagerarinformation ska besvara en motiverad begäran från Europol och överföra PNR-information dit.

Överföring av avmaskerade PNR-uppgifter

7 § Avmaskerade PNR-uppgifter får lämnas från enheten för passagerarinformation till behöriga mottagare eller till ett tredjeland endast om det rimligen kan antas vara nödvändigt för ändamålet att besvara en sådan begäran som anges i 1 § första stycket 2, 3, 4 eller 6 §§ detta kapitel eller 6 kap. 1 §. Dessutom krävs sådant beslut eller tillstånd som anges i 8 eller 9 §.

8 § Om förundersökning pågår ska en begäran från en behörig myndighet om att få tillgång till avmaskerade PNR-uppgifter ha beslutats av allmän åklagare.

9 § I de fall som inte omfattas av 8 § krävs att tillstånd till överföringen har lämnats av Polismyndigheten.

Myndighetschefen får delegera rätten att besluta om tillstånd till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs.

Den som har fått rätten att fatta beslut får inte arbeta vid enheten för passagerarinformation eller fatta beslut om överföring till sådan verksamhet som han eller hon deltar i.

5 kap. Behöriga myndigheters behandling av PNR-information

Gallring av PNR-information

1 § En behörig myndighet som mottagit PNR-information enligt 4 kap. 1 § första stycket 1 ska genast gallra informationen genom att den raderas, om den visar sig sakna betydelse för något av de syften som anges i 1 kap. 5 §.

2 § För det fall en behörig myndighet mottar PNR-uppgifter som utgör sådana personuppgifter som avses i 2 kap. 11 § brottsdatalagen (2018:000) ska de uppgifterna genast gallras genom att raderas.

Annan behandling av PNR-information

3 § Om det har kommit fram uppgifter om annat brott än terroristbrottslighet eller grov brottslighet i samband med en behörig myndighets insats som görs till följd av behandling av PNR-information, får informationen, utöver vad som anges i 1 kap. 5 §, användas för att förhindra, utreda eller lagföra brottet.

Automatiserade beslut

4 § Ett beslut som har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne får inte enbart grundas på en automatiserad behandling av PNR-uppgifter eller uppgifter som avses i 2 kap. 11 § brottsdatalagen (2018:000).

Föreskrifter

5 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela bestämmelser om behöriga myndigheters inhämtande och behandling av PNR-information.

6 kap. Överföring till tredjeland

1 § Enheten för passagerarinformation får överföra PNR-information till en myndighet i ett tredjeland som där är behörig att bedriva verksamhet som motsvarar ett eller flera av de syften som anges i 1 kap. 5 §. PNR-informationen får dock endast överföras om

1. förutsättningarna i 8 kap. 1 § första stycket 3 och 2 § första stycket brottsdatalagen (2018:000), 4 kap. 3 och 7 §§ samt 2 § detta kapitel är uppfyllda,

2. överföringen är nödvändig för ett eller flera av de syften som anges i 1 kap. 5 §, och

3. det tredjelandet godtar att vidareöverföra uppgifterna till ett annat tredjeland endast om det är absolut nödvändigt för ett eller flera av de syften som anges i 1 kap. 5 § och enheten för passagerarinformation har lämnat ett uttryckligt medgivande till vidareöverföringen.

2 § Om medgivande till överföring på grund av tidsbrist inte kan hämtas in i förväg från en medlemsstat som har lämnat PNR-information till enheten för passagerarinformation, får, i stället för vad som anges i 8 kap. 2 § andra stycket brottsdatalagen (2018:000), informationen ändå överföras om det är absolut nödvändigt för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet.

3 § När enheten för passagerarinformation överför PNR-information till ett tredjeland ska vad som anges i 8 kap. 8 § brottsdatalagen (2018:000) inte gälla.

4 § Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. information till annan medlemsstat när personuppgifter överförs utan förhandsmedgivande enligt 2 §, och

2. uppställande av villkor om användningsbegränsning av PNR-information som överförs till ett tredjeland.

7 kap. Övriga bestämmelser

Enskildas rättigheter

1 § Vad som anges i 4 kap. 10 § brottsdatalagen (2018:000) om registrerads rätt till radering eller begränsning av behandling av personuppgifter ska tillämpas vid behandling i strid mot

1. 1 kap. 5 §,
2. 1 kap. 6 §, eller
3. 3 kap. 9 §.

Det framgår av 7 kap. 2 § brottsdatalagen att beslut enligt 4 kap. 10 § brottsdatalagen kan överklagas.

2 § Bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd ska tillämpas på motsvarande sätt vid behandling i strid med bestämmelser till skydd för personuppgifter i denna lag eller förordning som har meddelats i anslutning till den.

Tillsyn

3 § Tillsyn över personuppgiftsbehandling enligt denna lag ska utföras av tillsynsmyndigheten enligt brottsdatalagen (2018:000) och i enlighet med bestämmelserna om tillsyn i den lagen.

Sanktionsavgifter vid överträdelser av enheten för passagerarinformation eller en behörig myndighet

4 § Sanktionsavgift får tas ut av den personuppgiftsansvariga myndigheten vid överträdelse av bestämmelserna i

1. 1 kap. 5 eller 6 §,
2. 3 kap. 3–11 §§,
3. 4 kap. 7–9 §§,
4. 5 kap. 1, 2 eller 4 §§, eller
5. 6 kap. 1 eller 2 §§.

5 § Vad som sägs i 6 kap. 3 § tredje stycket och 4–8 §§ brottsdatalagen (2018:000) ska gälla även vid uttagande av sanktionsavgift enligt 4 §.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Det framgår av 7 kap. 4 § brottsdatalagen att tillsynsmyndighetens beslut om sanktionsavgift kan överklagas.

Bilaga

PNR-uppgifter som enligt 2 kap. 1 § ska föras över från lufttrafikföretag till enheten för passagerarinformation:

1. PNR-uppgifternas lokaliseringskod.
2. Datum för bokning/utfärdande av biljett.
3. Planerat eller planerade resedatum.
4. Namn.
5. Adress och kontaktuppgifter (telefonnummer och e-postadress).
6. All betalningsinformation, inklusive faktureringsadress.
7. Fullständig resplan.
8. Uppgifter om bonusprogram.
9. Resebyrå/reseagent.
10. Passagerarens resestatus, inklusive resebekräftelser, incheckningsstatus, upplysningar om passagerare som inte infinner sig (no show) och passagerare utan bokning (go show).
11. Delade PNR-uppgifter.
12. Allmänna anmärkningar, inklusive alla tillgängliga uppgifter om ensamresande barn under 18 år, såsom namn, kön, ålder, språkkunskaper, namn och kontaktuppgifter för den person som följer barnet till incheckning för avresan och denna persons förhållande till barnet, namn och kontaktuppgifter för den person som hämtar barnet vid ankomsten och denna persons förhållande till barnet samt flygplatspersonal som ledsagar barnet vid avresan respektive ankomsten.
13. Biljettinformation, inklusive biljettnummer, datum för utfärdande av biljetten, enkelbiljetter och automatisk biljettprisuppgift.
14. Platsnummer och annan platsinformation.
15. Information om gemensam linjebeteckning.
16. All bagageinformation.
17. Antal medresenärer i PNR-uppgifterna och deras namn.
18. All eventuell förhandsinformation (API-uppgifter) som har samlats in, inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland, och sista giltighetsdag, nationalitet, efternamn, förnamn, kön, födelsedatum, lufttrafikföretag, flygnummer, utresedatum, ankomstdatum, avreseflygplats, ankomstflygplats, avresetid och ankomsttid.

19. Alla ändringar som har gjorts av de PNR-uppgifter som anges i punkterna 1–18.

Denna lag träder i kraft den 25 maj 2018.

1.2 Förslag till förordning (2018:000) om flygpassageraruppgifter i brottsbekämpningen

Härigenom föreskrivs följande

1 kap. Allmänna bestämmelser

1 § Denna förordning innehåller kompletterande bestämmelser till lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen.

2 § Uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen.

2 kap. Lufttrafikföretagens skyldigheter

Överföring av PNR-uppgifter till enheten för passagerarinformation

1 § Lufttrafikföretagen ska överföra PNR-uppgifter i enlighet med artikel 1 i kommissionens genomförandebeslut (EU) 2017/759 av den 28 april 2017 om gemensamma protokoll och dataformat som ska användas av lufttrafikföretag när PNR-uppgifter överförs till enheterna för passagerarinformation.

Vid eventuella tekniska problem får överföringen ske på annat lämpligt sätt som säkerställer ett tillfredsställande skydd för uppgifterna.

2 § Lufttrafikföretag som har samlat in sådan förhandsinformation om passagerare (API-uppgifter) som anges i punkt 18 i bilagan till lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen, men inte lagrar denna information med hjälp av samma tekniska metoder som för andra PNR-uppgifter, ska överföra även dessa uppgifter till enheten för passagerarinformation. Bestämmelserna i lagen och i denna förordning är tillämpliga även för dessa uppgifter.

Handläggning av sanktionsavgift för lufttrafikföretag

3 § Ett beslut om sanktionsavgift ska delges den som avgiften ska tas ut av.

Verkställighet av sanktionsavgift för lufttrafikföretag

4 § En sanktionsavgift ska betalas till Polismyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

5 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

3 kap. Behandling av PNR-information vid enheten för passagerarinformation

Utformande av kriterier

1 § Enheten för passagerarinformation ska i samarbete med de behöriga myndigheterna fastställa och regelbundet se över de kriterier som avses i 3 kap. 5 § 2 lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen.

Tillgång till PNR-information

2 § Behörighet för tillgång till uppgifter som har maskerats enligt 3 kap. 11 § lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen får endast ges till dataskyddsbudet eller den som har ett särskilt behov av fullständiga uppgifter för att kunna utföra sina arbetsuppgifter vid enheten för passagerarinformation. Behörigheten får bara utnyttjas när det i ett enskilt fall är absolut nödvändigt med tillgång till fullständiga uppgifter.

3 § Polismyndigheten meddelar närmare föreskrifter om tillgång till PNR-information och till övriga personuppgifter som behandlas vid enheten för passagerarinformation.

Elektroniskt utlämnande av personuppgifter

4 § Begränsningen i 2 kap. 20 § första meningen polisdatalagen (2010:361) gäller inte för enheten för passagerarinformations överföring av PNR-information till behöriga mottagare.

Efterhandskontroll

5 § Har överföring av avmaskerade PNR-uppgifter skett efter tillstånd från Polismyndigheten, ska dataskyddsombudet vid enheten för passagerarinformation göra en utvärdering av överföringen i efterhand.

Dataskyddsombudet ska även göra en utvärdering i efterhand av varje överföring till tredjeland som skett utan förhandssamtycke från den medlemsstat som har lämnat uppgifterna till enheten.

Bevarande och gallring

Omedelbar gallring

6 § Om lufttrafikföretagen har sänt in andra PNR-uppgifter än de som anges i bilagan till lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen, ska enheten för passagerarinformation vid mottagandet genast gallra dessa genom att de raderas.

Annan gallring

7 § Resultatet av en sådan behandling av PNR-uppgifter som avses i 3 kap. 4 § första stycket 1 lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen ska gallras så snart det inte längre behövs för att kunna informera behöriga mottagare om resultatet.

Om ett sådant resultat som avses i första stycket utgörs av en träff som inte bedöms behöva granskas vidare, får resultatet bevaras om syftet med bevarandet är att undvika motsvarande felaktiga träffar i framtiden. Gallring måste dock senast ske då de bakomliggande PNR-uppgifterna ska gallras enligt 3 kap. 9 § samma lag.

8 § Resultatet av en sådan behandling av PNR-uppgifter som avses i 3 kap. 4 § första stycket 2 lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen ska gallras så snart det inte längre behöver bevaras för återrapportering från mottagaren.

9 § PNR-information som har mottagits från andra medlemsstaters enheter för passagerarinformation ska gallras så snart resultatet inte längre behövs för att kunna informera behöriga myndigheter samt för att återrapportera till den enhet för passagerarinformation som har sänt in informationen.

Dokumentation och loggning

10 § Dokumentation om behandlingen av PNR-uppgifter vid enheten för passagerarinformation ska bevaras. Dokumentationen ska minst avse

1. uppgifter om vilka register eller andra uppgiftssamlingar och på förhand fastställda kriterier som används inom enheten,

2. namn och kontaktuppgifter för den organisation och personal inom enheten för passagerarinformation som har behörighet att behandla PNR-uppgifter samt personalens olika nivåer av åtkomstbehörighet,

3. varje begäran om att få ta del av PNR-uppgifter som har framställts av en behörig myndighet, en enhet för passagerarinformation i en annan medlemsstat eller en myndighet som har utsetts som behörig i en annan medlemsstat, och

4. varje begäran om att få ta del av PNR-uppgifter från och varje överföring av sådana uppgifter till ett tredjeland.

11 § Sådan loggning som avses i 3 kap. 4 § brottsdataförordningen (2018:000) ska utföras över enheten för passagerarinformations personuppgiftsbehandling. Loggarna ska bevaras i 5 år.

Information till dataskyddsbud

12 § Dataskyddsbudet vid enheten för passagerarinformation ska informeras om

1. varje utlämnande av avmaskerade PNR-uppgifter efter tillstånd från Polismyndigheten, och

2. varje överföring av PNR-uppgifter från enheten för passagerarinformation till tredjeland.

4 kap. Inhämtande av PNR-information från andra medlemsstaters enheter för passagerarinformation

1 § Inhämtande av PNR-information från andra medlemsstater får endast ske för ett eller flera av de syften som anges i 1 kap. 5 § lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen.

2 § En behörig myndighet som önskar ta del av PNR-information som lagras hos en enhet för passagerarinformation i en annan medlemsstat ska framställa begäran till enheten för passagerarinformation vid Polismyndigheten för vidare förmedling till den andra medlemsstaten.

3 § Endast om det i ett enskilt brådsökande fall är absolut nödvändigt får en behörig myndighet vända sig direkt till enheten för passagerarinformation i en annan medlemsstat med en begäran om att ta del av PNR-information som lagras hos den enheten.

Om en behörig myndighet har framställt en begäran enligt första stycket, ska en kopia av begäran skickas till enheten för passagerarinformation vid Polismyndigheten.

4 § Endast när det i ett enskilt fall är nödvändigt för att reagera på en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet, får enheten för passagerarinformation hos en motsvarande enhet i en annan medlemsstat begära att PNR-uppgifter ska hämtas in från lufttrafikföretag i enlighet med artikel 8.5 i PNR-direktivet för vidarebefordran till enheten.

5 kap. Överföring till tredjeland

1 § När enheten för passagerarinformation har överfört PNR-information till ett tredjeland utan förhandsmedgivande ska den utan dröjsmål informera den medlemsstat som har lämnat uppgifterna till enheten om överföringen.

2 § I samband med en överföring av PNR-information till ett tredjeland ska enheten för passagerarinformation uppställa villkor om användningsbegränsning som avses i 8 kap. 10 § brottsdatalagen (2018:000) i syfte att skydda PNR-informationen från användning i strid med PNR-direktivet.

Denna förordning träder i kraft den 25 maj 2018.

1.3 Förslag till lag om ändring i polislagen (1984:387)

Härigenom föreskrivs att 25 § polislagen (1984:387) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

25 §²

Ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige ska på begäran av Polismyndigheten eller Säkerhetspolisen skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter, som företaget har tillgång till. Transportföretaget har endast skyldighet att lämna de uppgifter om passagerare som avser namn, resrutt, bagage och medpassagerare samt sättet för betalning och bokning.

Polismyndigheten får begära uppgifter enligt första stycket endast om uppgifterna kan antas ha betydelse för den brottsbekämpande verksamheten.

Vad som anges i första och andra stycket ska inte gälla när lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen är tillämplig.

Denna lag träder i kraft den 25 maj 2018.

² Senaste lydelse 2014:588.

1.4 Förslag till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen

Härigenom föreskrivs att 15 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

15 §³

Transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige skall på begäran av Tullverket skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter, som företaget har tillgång till. Transportföretag har endast skyldighet att lämna de uppgifter om passagerare som avser namn, resrutt, bagage och medpassagerare samt sättet för betalning och bokning.

Tullverket får begära uppgifter enligt första stycket endast om uppgifterna kan antas ha betydelse för verkets brottsbekämpande verksamhet.

Vad som anges i första och andra stycket ska inte gälla när lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen är tillämplig.

Denna lag träder i kraft den 25 maj 2018.

³ Senaste lydelse 1999:434.

1.5 Förslag till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Härigenom föreskrivs att det i lagen (2007:258) om behandling av personuppgifter i Försvarens försvarsunderrättelseverksamhet och militära säkerhetstjänst ska införas en ny paragraf, 1 kap. 1 a §, med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

1 a §

I lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen finns det särskilda bestämmelser om behandling av personuppgifter. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Denna lag träder i kraft den 25 maj 2018.

1.6 Förslag till lag om ändring i polisdatalagen (2010:361)

Härigenom föreskrivs att det i polisdatalagen (2010:361) ska införas en ny paragraf, 1 kap. 4 a §, med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

4 a §

I lagen (2018:000) om flygpassageraravgifter i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen finns det särskilda bestämmelser om behandling av personuppgifter. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Denna lag träder i kraft den 25 maj 2018.

1.7 Förslag till lag om ändring i tullagen (2016:253)

Härigenom föreskrivs att det i tullagen (2016:253) ska införas en ny paragraf, 4 kap. 6 a §, med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 kap.

6 a §

Vad som anges i 6 § ska inte gälla när lagen (2018:000) om flygpassageraravgifter i brottsbekämpningen är tillämplig.

Denna lag träder i kraft den 25 maj 2018.

1.8 Förslag till lag om ändring i tullbrottsdatalagen (2017:000)

Härigenom föreskrivs att 2 kap. 8 § tullbrottsdatalagen (2017:000) ska ha följande lydelse.

Lydelse enligt prop. 2016/17:91 Föreslagen lydelse

2 kap. 8 §

Personuppgifter som har lämnats till Tullverket från transportföretag enligt 4 kap. 6 § tullagen (2016:253) eller 15 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen får behandlas i den utsträckning det är tillåtet enligt dessa lagar och enbart i den utsträckning det behövs för planering av kontrollverksamheten och urval av kontrollobjekt.

Om det behövs i ett enskilt fall får sådana personuppgifter behandlas för något annat ändamål som anges i 5 § och göras gemensamt tillgängliga.

I lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen finns det särskilda bestämmelser om behandling av personuppgifter. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Denna lag träder i kraft den 25 maj 2018.

2 Inledning

2.1 Uppdraget

Utredningens uppdrag är att lämna förslag till de lagändringar som krävs för att i svensk rätt genomföra Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och för att Sverige ska leva upp till den deklaration som medlemsstaterna har antagit i anledning av direktivet. Direktiven för arbetet finns i *bilaga 1*.

I uppdraget ingår bl.a. att

- föreslå ett system för hur flygpassageraruppgifter ska hanteras i Sverige och hur enheten för passagerarinformation ska organiseras,
- föreslå vilka sanktioner som ska kunna åläggas flygbolag som inte uppfyller sina skyldigheter enligt direktivet,
- föreslå en reglering för personuppgiftsbehandling och sekretess som passar in i den befintliga svenska strukturen och ger en rätts-säker och mer effektiv brottsbekämpning samtidigt som skyddet för den personliga integriteten säkerställs, och
- analysera om och i så fall hur direktivet påverkar det svenska genomförandet av rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare (API-direktivet) samt att föreslå hur systemet med flygpassageraruppgifter ska möjliggöra hanteringen av både PNR-uppgifter och API-uppgifter.

2.2 Arbetets genomförande

Utredningens arbete påbörjades i mitten av april 2016. Arbetet har bedrivits på sedvanligt sätt med regelbundna sammanträden med gruppen av sakkunniga och experter. Utredningen har sammanträtt vid sammanlagt nio tillfällen.

Utredningen har beaktat det arbete som pågår inom Polismyndigheten med att bl.a. inrätta en enhet för passagerarinformation och i övrigt genomföra direktivets tekniska delar. Den 17 juni 2016 genomfördes ett besök vid Polismyndigheten.

Det samråd som utredningen enligt direktiven ska ha med berörda myndigheter har huvudsakligen skett genom experterna. Därutöver har utredningen i vissa delar samrått med Datainspektionen som har lämnat övergripande synpunkter.

Synpunkter har också inhämtats från berörda ekonomiska aktörer. Den 25 oktober 2016 hölls ett dialogmöte med representanter för lufttrafikföretagen. Ett dialogmöte med representanter för resebyråer och researrangörer hölls den 7 november 2016. Ytterligare kontakter med dessa aktörer har förekommit efter mötena.

Enligt utredningens direktiv ska utredaren i den utsträckning det är möjligt beakta det arbete som genomförs av Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06). Utredningarna samrådde den 16 november 2016. Arbetet med genomförandet av det nya dataskyddsdirektivet har därutöver följts under hand. Våra författningsförslag är anpassade till den nämnda utredningens förslag till ny ramlagstiftning, brottsdatalagen med anslutande förordning, varigenom det nya dataskyddsdirektivet föreslås bli genomfört (SOU 2017:29). Skälet för detta något ovanliga anslag redogör vi för i avsnitt 8.5.

Utredningen har vidare deltagit vid ett flertal möten med andra utredningar som utreder frågor om anpassning till EU:s dataskyddsreform. Även arbetet inom andra relevanta utredningar har beaktats.

3 PNR-direktivet och överenskommelser i anledning av direktivet

3.1 Allmänt om direktivet

Den 27 april 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (PNR-direktivet). Direktivet jämte rättelser av detta finns i *bilaga 2 och 3*.

PNR är en förkortning av den engelska benämningen Passenger Name Record. I den svenska versionen av direktivet har detta begrepp översatts som passageraruppgiftssamling eller PNR-uppgifter. Det som åsyftas är uppgifter som passagerare lämnar vid beställning och bokning av flygresor samt vid incheckning. Uppgifterna kan till exempel avse namn, resedatum, resväg, bagageinformation och betalningssätt. Lufttrafikföretagen samlar redan i dag in och behandlar sådana uppgifter om sina passagerare i olika bokningssystem för sina egna operativa och kommersiella syften. Direktivet reglerar skyldigheten för lufttrafikföretag att överföra dessa redan insamlade uppgifter till enheter för passagerarinformation i medlemstaterna. Direktivet anger också för vilka ändamål uppgifterna får behandlas samt hur länge uppgifterna får och ska lagras och under vilka förutsättningar de ska överföras till olika mottagare. Målen för direktivet är bl.a. att trygga säkerheten, skydda personers liv och säkerhet samt att inrätta en rättslig ram till skydd för PNR-uppgifterna vid behöriga myndigheters behandling av dessa.

3.2 Bakgrund

Terroristattentat under senare årtionden har lett till nya initiativ för att förbättra säkerheten. Samtidigt har den internationella organiserade brottsligheten ökat.¹ Organiserad brottslighet och terrorism är företeelser som ofta inbegriper internationella resor. Som en följd av detta har myndigheterna i flera länder i allt större utsträckning börjat samla in och analysera PNR-uppgifter i syfte att bekämpa terrorism och grov brottslighet.

PNR-uppgifter bör skiljas från s.k. API-uppgifter (Advance Passenger Information). API-uppgifter avser främst sådan information som finns på passets maskinläsbara del, såsom namn, födelse-datum, nationalitet och passnummer. I rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare (API-direktivet) regleras transportörers ansvar för att på begäran förse nationella myndigheter med sådana passageraruppgifter inför resor från länder utanför Schengen-området. API-direktivet syftar till att förbättra gränskontrollerna och bekämpa olaglig invandring.

API-uppgifter används huvudsakligen som ett verktyg för identifiering. Uppgifterna kan därmed användas som ett led i gränskontrollerna. API-uppgifterna kan dock även användas av brottsbekämpande myndigheter för att dessa ska kunna identifiera misstänkta och eftersökta personer. Uppgifterna kan även komma till användning i underrättelsearbetet med att exempelvis kartlägga var vissa personer har befunnit sig vid olika tidpunkter.

PNR-uppgifter används snarare som ett verktyg för underrättelseverksamhet än som ett verktyg för identitetskontroll. Uppgifterna används främst för att göra riskbedömningar av passagerare och för att sälla ut personer som skulle kunna vara intressanta att kontrollera vidare men som inte är misstänkta sedan tidigare. Uppgifterna kan även användas för att analysera och fastställa misstänkta rese- och beteendemönster. PNR-uppgifterna kan också användas i samband med brottsutredningar och för lagföringsåtgärder. En närmare beskrivning av hur PNR- och API-uppgifter kan användas i brottsbekämpande verksamhet finns i avsnitt 14.1.

¹ KOM (2010) 492 slutlig av den 21 september 2010, s. 2.

PNR-uppgifter har använts i närmare 60 år, främst av tullmyndigheter men också till viss del av andra brottsbekämpande myndigheter världen över.² I Sverige har uppgifterna använts av Tullverket på Arlanda sedan början av 1990-talet. Inledningsvis förekom endast manuell behandling av PNR-uppgifter. Den senaste tidens tekniska utveckling har möjliggjort tillgång till och analys av PNR-uppgifter på ett sätt som inte tidigare var möjligt.

Ett antal länder utanför Europeiska unionen har i dag särskilda system för inhämtande och analys av PNR-uppgifter. Efter terroristattentaten den 11 september 2001 antog USA lagstiftning som innebär att lufttrafikföretag med trafik till, från eller genom dess territorium ska tillhandahålla de amerikanska myndigheterna PNR-uppgifter. Snart beslutade Kanada och Australien att göra samma sak. Flera länder har följt i deras fotspår.

EU ingick i mitten av 2000-talet avtal som reglerar överföringen av PNR-uppgifter från lufttrafikföretag till USA, Australien och Kanada. Avtalen har därefter omförhandlats. De senaste avtalen med USA och Australien har godkänts av Europaparlamentet och trädde i kraft år 2012. Vad gäller det planerade nya avtalet med Kanada har Europaparlamentet ännu inte tagit ställning. Parlamentet har begärt ett yttrande från EU-domstolen bl.a. i frågan om avtalet är förenligt med fördraget om Europeiska unionen och Europeiska unionens stadga om de grundläggande rättigheterna vad gäller fysiska personers rätt till skydd av personuppgifter. Generaladvokaten har lämnat ett förslag till yttrande där det anges att vissa förtydliganden måste göras i avtalet och/eller vissa av bestämmelserna utgå för att avtalet ska vara förenligt med stadgan och inte gå utöver vad som är strängt nödvändigt för att uppnå målsättningen att skydda den allmänna säkerheten. Något yttrande från EU-domstolen har dock ännu inte kommit. Under 2015 antog Europeiska unionens råd ett beslut som godkänner att förhandlingar inleds om ett avtal med Mexiko.

De brottsbekämpande myndigheterna i EU-länderna har i olika utsträckning möjlighet att tillgå och behandla PNR-uppgifter. För Sveriges del kan bl.a. Polismyndigheten och Tullverket redan i dag begära in och använda vissa PNR-uppgifter för brottsbekämpande ändamål. Detta beskrivs närmare i kapitel 5. Uppgifterna kan också sparas i enskilda utredningar med stöd av polisdatalagen (2010:361)

² A.a. s. 4.

och lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet³. Något nationellt system för insamling av uppgifterna finns dock inte. Uppgifterna sparas inte heller i någon central databas.

Ett unionsgemensamt regelverk för insamling och användning av PNR-uppgifter i brottsbekämpande verksamhet har diskuterats under flera år. År 2007 överlämnade Europeiska kommissionen ett förslag till rådets rambeslut om användande av PNR-uppgifter i brottsbekämpningssyfte. Förslaget förhandlades under två år men blev inaktuellt när Lissabonfördraget trädde i kraft år 2009. År 2011 lade kommissionen fram ett förslag till direktiv om användning av PNR-uppgifter för bekämpande av terroristbrott och allvarliga brott. Förslaget syftade till att enhetligt reglera insamling, sparande och behandling av flygpassageraruppgifter. I huvudsak fanns det två skäl till förslaget. Det första var att bidra till medlemsstaternas möjligheter att bekämpa och skydda medborgarna från allvarliga brott, inklusive terroristbrottslighet. Det andra var att undvika utvecklandet av olika PNR-system inom EU vilket skulle kunna leda till rättsosäkerhet, ökade kostnader och risk för bristande skydd för den personliga integriteten.

Rådet var tidigt positivt till förslaget. Europaparlamentet dröjde längre med att ta ställning bl.a. eftersom det ansågs behövas ett starkare skydd för den personliga integriteten. Efter år av förhandlingar och sedan ett antal terroristattentat genomförts i Europa, kom rådet och parlamentet i december 2015 överens om ett gemensamt förslag till reglering. Förslaget innebar bl.a. att vissa frågor lämnades utanför direktivet och i stället hanteras i frivilliga överenskommelser mellan medlemsstaterna.

3.3 Direktivets innehåll i korthet

Direktivet är indelat i fyra kapitel och innehåller sammanlagt 22 artiklar. Artiklarna presenteras starkt förkortat i det följande. Det närmare innehållet i artiklarna och de skäl som hänför sig till dessa kommer att redovisas i anslutning till våra överväganden om artiklarnas implementering.

³ Ersätts den 1 juli 2017 av tullbrottsdatalagen (2017:000).

Av *artikel 1* framgår att direktivet innehåller bestämmelser om lufttrafikföretags överföring av PNR-uppgifter på flygningar utanför EU. I artikeln anges att de PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

Direktivet avser således endast flygningar utanför EU. I *artikel 2* ges dock möjlighet för en medlemsstat att tillämpa direktivets bestämmelser även för flygningar inom EU.

I *artikel 3* definieras centrala begrepp i direktivet. Med *lufttrafikföretag* avses exempelvis ett sådant företag med giltig operativ licens eller motsvarande som ger rätt att bedriva passagerarflygtrafik. Med *flygningar utanför EU* menas varje flygning som utförs av ett sådant lufttrafikföretag, med avgång från ett tredjeland och planerad landning på en medlemsstats territorium eller flygning från en medlemsstats territorium med planerad landning i ett tredjeland, i båda fallen inklusive eventuella mellanlandningar på territorier i medlemsstater eller tredjeländer. *Passagerare* är alla personer, förutom besättningsmedlemmar, som transporteras med eller ska transporteras med ett flygplan med lufttrafikföretagets godkännande. Godkännandet framgår av att personen står med i passagerarförteckningen.

I *artikel 4* anges att varje medlemsstat ska inrätta eller utse en myndighet eller del av en myndighet med behörighet att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet som ska fungera som medlemsstatens enhet för passagerarinformation. Enheten ska ansvara för att samla in PNR-uppgifter från lufttrafikföretagen, lagra och behandla dessa uppgifter och överföra dessa uppgifter eller resultatet av behandlingen av dem till behöriga myndigheter. Enheten ska även ansvara för att utbyta uppgifterna och resultatet av behandlingen av uppgifterna med andra medlemsstaters motsvarande enheter och med Europol.

Av *artikel 5* framgår att enheten för passagerarinformation ska utse ett dataskyddsombud, som bl.a. ska ansvara för övervakningen av behandlingen av PNR-uppgifter och för genomförandet av relevanta skyddsåtgärder.

I *artikel 6* anges hur de överförda PNR-uppgifterna får behandlas vid enheten för passagerarinformation och för vilka ändamål. Enligt bestämmelsen får PNR-uppgifterna användas för att göra bedömningar av passagerare före deras planerade ankomst till eller avresa från en medlemsstat. Uppgifterna får även användas för att besvara

motiverade frågor från exempelvis de behöriga myndigheterna. Vidare får uppgifterna behandlas för att uppdatera och skapa nya riskkriterier som kan användas vid förhandsbedömningar av passagerare. I artikel 6 regleras vidare överföring av PNR-uppgifter och resultatet av behandlingen av uppgifterna till behöriga myndigheter i samma medlemsstat.

Varje medlemsstat ska enligt *artikel 7* fastställa en förteckning över de myndigheter som har befogenhet att begära eller motta PNR-uppgifter eller resultatet av behandlingen av dessa uppgifter från enheten för passagerarinformation. Artikeln innehåller också vissa bestämmelser om dessa myndigheters vidare behandling av PNR-uppgifter.

Lufttrafikföretagens skyldigheter vad gäller överföring av PNR-uppgifter framgår av *artikel 8*. Överföringen ska ske genom att uppgifterna skickas från lufttrafikföretagen till enheten för passagerarinformation i den medlemsstat på vars territorium flygningen kommer att ankomma eller från det territorium flygningen kommer att avgå. I bilaga I till direktivet anges vilka PNR-uppgifter som ska överföras, i den mån dessa uppgifter redan samlas in av företaget som en del av dess normala verksamhet. Direktivet ålägger alltså inte lufttrafikföretagen att samla in ytterligare uppgifter om sina passagerare. Lufttrafikföretagen ska normalt överföra uppgifterna elektroniskt 24–48 timmar före flygningens planerade avgång samt omedelbart efter det att gaten har stängts.

Formerna för utbyte av PNR-uppgifter eller resultatet av en eventuell behandling av dessa uppgifter mellan medlemsstaterna framgår av *artikel 9*, exempelvis när det ska ske självmant och när det ska ske på begäran. Villkoren för Europols åtkomst till PNR-uppgifter anges i *artikel 10*. En medlemsstat får endast under de förutsättningar som anges i *artikel 11* överföra PNR-uppgifter och resultatet av behandlingen av sådana uppgifter till ett tredjeland.

I *artikel 12* behandlas frågor om lagringstid för uppgifter och avidentifiering. PNR-uppgifter som lämnas av lufttrafikföretag ska lagras i en databas vid enheten för passagerarinformation under en period av fem år efter överföringen till enheten och ska sedan raderas. Sex månader efter överföringen ska uppgifterna avidentifieras genom maskering av vissa uppgifter som kan användas för att omedelbart identifiera de passagerare som PNR-uppgifterna avser. Efter utgången av sexmånadersperioden ska utlämnande av fullständiga

PNR-uppgifter endast tillåtas om vissa särskilda förutsättningar är uppfyllda.

Artikel 13 innehåller bestämmelser om skydd av personuppgifter. Medlemsstaterna ska bl.a. föreskriva att den behandling av personuppgifter som sker vid den nationella enheten för passagerarinformation och vid behöriga myndigheter ska omfattas av vissa nationella dataskyddsbestämmelser som överensstämmer med rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet). Med hänvisningen till dataskyddsrambeslutet ska förstås såväl nuvarande lagstiftning som de framtida bestämmelser som kommer att ersätta detta. Vidare finns i artikel 13 dataskyddsbestämmelser om bl.a. förbud mot behandling av känsliga personuppgifter, regler om loggning, informationssäkerhet m.m.

Medlemsstaterna ska enligt *artikel 14* införa effektiva, proportionella och avskräckande sanktioner för överträdelser av nationella bestämmelser som genomför direktivet. Sanktioner ska särskilt riktas mot lufttrafikföretag som inte överför PNR-uppgifter.

Enligt *artikel 15* ska den nationella tillsynsmyndighet som anges i artikel 25 i dataskyddsrambeslutet ansvara för att ge riktlinjer för och övervaka tillämpningen av de bestämmelser som medlemsstaterna antar i enlighet med direktivet. Tillsynsmyndigheten ska vidare hantera klagomål från registrerade, kontrollera att uppgiftsbehandlingen är laglig samt på begäran ge registrerade råd om hur de kan utöva sina rättigheter på området.

I *artikel 16* anges att all överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation ska ske elektroniskt och med tillräcklig grad av informationssäkerhet. Gemensamma protokoll och understödda dataformat för detta ändamål ska antas av kommissionen. Kommissionen ska biträdas av en kommitté i enlighet med *artikel 17*.

Artiklarna 18–22 innehåller bestämmelser om införlivande, översyn, statistik, förhållande till andra bilaterala eller multilaterala avtal eller andra instrument samt ikraftträdande. Direktivet ska vara genomfört i medlemsstaterna senast den 25 maj 2018.

Danmark deltar inte i antagandet av direktivet, som därför inte är bindande för eller tillämpligt på Danmark.

3.4 Överenskommelser i anledning av direktivet

Genom PNR-direktivet åläggs lufttrafikföretag att överföra PNR-uppgifter om samtliga passagerare på flygningar som anländer från eller avgår till ett land utanför EU. De medlemsstater som så önskar får enligt artikel 2 i direktivet på frivillig grund tillämpa det även på flygningar inom EU. I en deklARATION som antogs av rådet i samband med antagandet av PNR-direktivet har Sverige och övriga medlemsstater förklarat att de, mot bakgrund av det aktuella säkerhetsläget i Europa, fullt ut kommer att utnyttja denna möjlighet. Enligt deklARATIONEN ska detta ske senast det datum då direktivet ska införlivas i nationell rätt. DeklARATIONEN finns i *bilaga 4*.

I deklARATIONEN har medlemsstaterna även förklarat att de, i enlighet med parlamentets önskemål, åtar sig att i enlighet med sin nationella lagstiftning och med förbehåll för parlamentsbehandling i vissa medlemsstater, utvidga insamlingen av PNR-uppgifter till att omfatta även aktörer som inte är lufttrafikföretag, t.ex. resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, för vilka sådana uppgifter samlas in och behandlas. Någon tidsgräns för när detta ska vara genomfört i nationell lagstiftning är inte angivet.

4 Transportörsansvaret och API-direktivet

4.1 Inledning

Brottsbekämpande myndigheter hanterar redan i dag information från transportföretag, inklusive flygbolag, för brottsbekämpande ändamål. För flygbolagens del innebär det en skyldighet att överlämna uppgifter om sina passagerare till vissa brottsbekämpande myndigheter. Ett sådant ansvar kan sägas vara en vidareutveckling av det s.k. transportörsansvaret i vid mening. PNR-uppgifter och PNR-direktivet har således en koppling till transportörsansvaret, varför detta kommer att beskrivas översiktligt i det följande. Transportörsansvaret handlar dock huvudsakligen inte om brottsbekämpning utan har sin grund i utlänningsrätten och bestämmelser om en reglerad invandring.

Med transportörsansvar menas att transportörer har vissa skyldigheter beträffande de personer som de transporterar till ett lands gräns. De kan också åläggas sanktioner om de inte uppfyller sina skyldigheter. Sverige har alltsedan anslutningen till den s.k. Chicago-konventionen på 1940-talet haft internationella åtaganden när det gäller transportörsansvaret. De svenska reglerna härom bygger huvudsakligen på dessa internationella åtaganden.

I detta avsnitt kommer inledningsvis de internationella åtaganden som Sverige har på området att behandlas. Därefter kommer bestämmelser om transportörsansvar i EU-rätten och i den nationella rätten att översiktligt beskrivas. Slutligen behandlas det s.k. API-direktivet och dess genomförande i svensk rätt.

4.2 Internationella åtaganden på området

4.2.1 Chicagokonventionen

Sverige har anslutit sig till 1944 års konvention angående internationell civil luftfart, den så kallade Chicagokonventionen, också kallad Icao-konventionen (SÖ 1946:2). Denna konvention reglerar internationell civil luftfart och syftar till att upprätthålla säkerhet under internationell lufttrafik och att underlätta och främja luftfarten. Så gott som alla länder har anslutit sig till konventionen. Den svenska luftfartslagstiftningen bygger i stora delar på konventionen.

I Chicagokonventionen förbinder sig de fördragsslutande staterna till samarbete för att, i alla sådana hänseenden där likformighet kan underlätta och befrämja luftfarten, säkerställa största möjliga likformighet i fråga om författningar, normer, tillämpningsförfaranden och organisation avseende luftfartyg, besättning, luftfartslinjer och markorganisation. I detta syfte antar det permanenta rådet av FN:s fackorgan International Civil Aviation Organization (Icao) olika internationella normer och rekommendationer, vilka tas in i s.k. Annex till konventionen.

I det nu gällande Annex 9 finns bl.a. internationella normer om transportörsansvar och behandlingen av API- och PNR-uppgifter.

Artikel 3.35 i Annex 9 ålägger flygtrafikföretagen att kontrollera att passagerare vid ombordstigningen innehar pass och tillstånd för transit och inresa. Enligt artikel 3.33 ska de fördragsslutande staterna och transportörerna samarbeta för att fastställa att de resedokument som visas upp är äkta och giltiga. Myndigheterna ska enligt artikel 5.3 och 5.4 utan dröjsmål informera transportören när en person inte tillåts inresa och rådgöra med transportören angående möjligheter till återförande. Transportören ska därefter enligt artikel 5.11 återföra passageraren till den plats där han eller hon påbörjade sin resa eller till någon annan plats där han eller hon kan tas emot. Enligt artikel 5.10 får transportören inte hindras från att ta ut transportkostnaden från den avvisade personen. Återförandeplikten upphör enligt artikel 3.47 när personen tillåts resa in i landet.

I artikel 3.48 finns bestämmelser hänförliga till API-uppgifter (se närmare i avsnitt 4.5). Här anges att varje fördragsslutande stat som inför ett API-system ska använda sig av internationellt erkända standarder för överföring av API-uppgifter. Utgångspunkten är att de fördragsslutande länderna ska använda sig av den standard

UN/EDIFACT PAXLST som har utarbetats gemensamt av World Customs Organization (WCO), International Air Transport Association (Iata) och Icao. Det anges vidare att de fördragsslutande staterna så långt det är möjligt ska försöka minimera de operativa och administrativa bördorna för flygtrafikföretagen. Antalet överföringar av API-uppgifter per flygning bör minimeras. De fördragsslutande staterna bör inte använda sig av sanktioner mot flygtrafikföretagen på grund av tekniska överföringsfel. De stater som kräver elektronisk överföring av API-uppgifter ska inte därutöver kräva uppgifterna i pappersform. Det rekommenderas även att API-systemet används dygnet runt samt att olika rutiner för att undvika tekniska avbrott i systemet införs.

Enligt artikel 3.49 bör fördragsslutande stater som kräver tillgång till PNR-uppgifter anpassa sin behandling av uppgifterna och sina tekniska krav till vissa angivna riktlinjer. De riktlinjer som anges är Icao:s dokument 9944, Guidelines on Passenger Name Record (PNR) Data, samt instruktioner för implementering av standardformatet PNRGOV. Riktlinjerna rörande PNRGOV publiceras av WCO under godkännande av Icao och Iata. Vidare rekommenderas de fördragsslutande staterna att överväga att använda sig av standardformatet PNRGOV för överföringen av PNR-uppgifter.

4.2.2 FN:s resolution 2178

Den 24 september 2014 antog FN:s säkerhetsråd resolution 2178 (2014). Resolutionen är antagen i enlighet med kapitel VII i FN-stadgan och är därmed folkrättsligt bindande för alla medlemsstater.

I resolutionen anges att terrorism i alla dess former är ett hot mot internationell fred och säkerhet. Vidare uttrycks en allvarlig oro över det akuta och växande hot som de personer utgör som reser till ett annat land för att delta i terroristhandlingar eller terroristträning, även när detta sker inom ramen för en väpnad konflikt. De bidrar enligt resolutionen till intensiteten och varaktigheten i konflikter och till att de blir mer svårlösta. Personerna uppges även kunna utgöra ett allvarligt hot mot bl.a. sina ursprungsländer, länderna de reser igenom och länderna de reser till.

I resolutionens paragraf 2 bekräftas att alla stater ska begränsa möjligheten för terrorister eller terroristgrupper att röra sig fritt över

gränserna bl.a. genom effektiva gränskontroller och medlemsstaterna uppmanas att införa vissa säkerhetsåtgärder i detta avseende. Medlemsstaterna uppmanas således att använda sig av evidensbaserad riskbedömning och kontrollförfaranden för resande, inklusive insamling och analys av resedata. Det påpekas dock att profilering utifrån stereotyper grundade på diskriminering är förbjudet enligt folkrätten.

I resolutionens paragraf 9 uppmanas medlemsstaterna att kräva att lufttrafikföretag som är verksamma inom deras territorier i förväg lämnar ut uppgifter om passagerare till behöriga nationella myndigheter för att upptäcka avresa från deras territorier eller försök till inresa till eller transitering genom deras territorier med civila luftfartyg.

4.3 Vissa EU-rättsliga åtaganden

4.3.1 Schengenkonventionen och direktivet om transportörsansvar

Sverige har EU-rättsliga åtaganden om transportörsansvar. Hit kan även räknas API-direktivet, som behandlas nedan i avsnitt 4.5.1.

Artikel 26 i Schengenkonventionen¹ och rådets direktiv om komplettering av bestämmelserna i den artikeln (direktivet om transportörsansvar²) behandlar transportörsansvaret. I artikel 26 i Schengenkonventionen föreskrivs att de avtalsslutande parterna – om inte annat följer av förpliktelser i samband med anslutning till Genèvekonventionen angående flyktingars rättsliga ställning, ändrad genom New York-protokollet – ska införa vissa bestämmelser på området. Dessa bestämmelser gäller en skyldighet för en transportör att kontrollera inresehandlingar och ett ansvar för denne att ordna återresa för utlänningar som vägras inresa i en Schengenstat samt sanktioner mot den som befordrar utlänningar utan nödvändiga resehandlingar. Med transportör avses i Schengenkonventionen varje fysisk eller juridisk person som bedriver yrkesmässig persontrafik luft-, sjö- eller landvägen.

¹ Konventionen om tillämpning av Schengenavtalet av den 14 juni 1985.

² Rådets direktiv 2001/51/EG av den 28 juni 2001 om komplettering av bestämmelserna i artikel 26 i konventionen om tillämpning av Schengenavtalet av den 14 juni 1985.

Direktivet om transportörsansvar har som syfte att harmonisera medlemsstaternas lagar om ekonomiska sanktioner mot transportörer som försummar sin kontrollskyldighet avseende inresehandlingar.

De förpliktelser som följer av artikel 26 i Schengenkonventionen och direktivet om transportörsansvar har Sverige uppfyllt genom bestämmelser i utlänningslagen (2005:716), se avsnitt 4.4.2.

4.3.2 Kodex om Schengengränserna

I den så kallade kodexen om Schengengränserna³, även kallad gränskodexen, behandlas en unionskodex om gränspassager för personer. I bilaga VI till kodexen upptas särskilda bestämmelser om de olika transportmedel som används för passage av de yttre gränserna. Bl.a. anges att befälhavaren vid privata flygningar från eller till tredjeländer före starten ska överlämna uppgifter om passagerarnas identitet till gränskontrolltjänstemännen i destinationsmedlemsstaten och, i förekommande fall, i den medlemsstat där den första inresan äger rum.

4.4 Svenska regler om transportörsansvar

4.4.1 Bakgrund

I svensk rätt har det under lång tid funnits reglering av transportörsansvaret såsom nära knuten till utlänningslagstiftningen. Utan att i detalj gå in på detta kan nämnas att det redan i lagen den 14 september 1914 (nr 196) angående förbud för vissa utlänningar att här i riket vistas fanns en bestämmelse om att en befälhavare på fartyg under vissa förutsättningar var skyldig att, utan ersättning från statsverkets sida, vid avvisning återföra utlänningar till det land varifrån de hade medtagits. Bestämmelser med i huvudsak samma innehåll återkom i flera därpå följande utlänningslagar. Genom en ändring i 1937 års utlänningslag den 1 september 1942 ålades befälhavare på luftfartyg samma skyldighet som befälhavare på fartyg. I 1954 års utlännings-

³ Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna).

lag lades ansvaret för återförandet i stället på innehavaren av fartyget eller luftfartyget.

Regler om transportörsansvaret har funnits kvar i senare versioner av utlänningslagen och har skärpts både i fråga om återförandeplikten och gällande transportörens kostnadsansvar. Den senaste regelskärpningen i utlänningslagen skedde den 1 juli 2004 sedan Sverige operativt inträtt i Schengensamarbetet. Transportörsansvaret i utlänningslagen utvidgades då för att uppfylla de åtaganden som följer av artikel 26 i Schengenkonventionen och direktivet om transportörsansvar. Bl.a. lagreglerades transportörers skyldighet att kontrollera att utläningar har pass och andra tillstånd som krävs för inresa i landet.

På senare tid har transportörer också ålagts en skyldighet att genomföra identitetskontroller vid transporter som utförs med buss, tåg eller passagerarfartyg till Sverige från en annan stat bl.a. med stöd av bestämmelserna i den tillfälliga lagen (2015:1073) om särskilda åtgärder vid allvarlig fara för den allmänna ordningen eller den inre säkerheten i landet.

4.4.2 Utlänningslagens bestämmelser om transportörsansvar

De svenska bestämmelserna om transportörsansvar återfinns alltså främst i utlänningslagen. I 9 kap. 3 § regleras transportörers kontrollskyldighet. Enligt bestämmelserna ska en transportör kontrollera att en utläning, som transportören transporterar till Sverige direkt från en stat som inte omfattas av Schengenkonventionen, innehar pass och de tillstånd som krävs för att resa in i landet. Transportören ska också, om det inte är obehövt på grund av resultatet av denna kontroll, kontrollera att utläningen har medel för sin hemresa.

I 12 kap. 5 § regleras transportörers ansvar att ombesörja utläningars återresa i vissa fall. Med transportör avses här ägare eller brukare av ett fartyg eller ett luftfartyg. En utläning som har kommit till Sverige med ett fartyg eller ett luftfartyg direkt från en stat som inte omfattas av Schengenkonventionen och som har avvisats för att han eller hon saknar pass eller de tillstånd som krävs för att resa in i landet eller medel för sin hemresa, får som utgångspunkt föras tillbaka till fartyget eller luftfartyget eller sättas ombord på ett annat sådant med samma transportör.

I 19 kap. 2 § regleras transportörers kostnadsansvar om utlänningar saknar pass eller de tillstånd som krävs för inresa till Sverige eller medel för hemresan. Transportören är enligt denna bestämmelse normalt skyldig att ersätta staten för kostnader för utlänningens resa från Sverige samt resekostnaden för den bevakningspersonal som följer med.

De transportörer som inte har fullgjort sin kontrollskyldighet beträffande pass och de tillstånd som krävs för inresa till landet kan enligt 19 kap. 5 § bli skyldiga att betala en särskild avgift. Avgiften ska enligt 19 kap. 6 § bestämmas till högst 46 000 kr för varje utlänning.

4.4.3 Befälhavares skyldigheter

Befälhavaren på ett luftfartyg som kommer från en ort utanför Schengenstaterna ska enligt 6 kap. 8 § utlänningsförordningen (2006:97) före ankomst underrätta flygplatschefen om ankomsten. Flygplatschefen ska i sin tur utan dröjsmål underrätta Polismyndigheten om att ett luftfartyg kommer från eller avgår till en ort utanför Schengenstaterna. Underrättelseskyldigheten gäller inte för befälhavaren på ett privatflyg. För en sådan befälhavare finns bestämmelser om underrättelseskyldighet i gränskodexen, se ovan under avsnitt 4.3.2.

4.5 API-direktivet och dess genomförande i svensk rätt

4.5.1 API-direktivet

Den 29 april 2004 antog rådet direktiv 2004/82/EG om skyldighet för transportörer att lämna uppgifter om passagerare (API-direktivet). I direktivet regleras transportörers skyldighet att överföra förhandsinformation om passagerare (API-uppgifter) till behöriga nationella myndigheter. Direktivet syftar till att förbättra gränskontrollerna och bekämpa olaglig invandring. Direktivet är också ett led i kampen mot terrorism (se prop. 2005/06:129 s. 18).

Uppgiftsskyldigheten enligt direktivet omfattar transportörer som luftvägen ska transportera passagerare från länder som inte tillhör

EU och inte heller har slutit avtal om samarbete enligt Schengenkonventionen med konventionsstaterna. Dessa transportörer ska på begäran av en myndighet som ansvarar för personkontrollen vid de yttre gränserna föra över information om de ankommande passagerarna. De uppgifter som ska överföras avser bl.a. passagerarnas namn, födelsedatum, medborgarskap, ort för ombordstigning och gränsövergångsställe för inresa. Sådana uppgifter av personlig karaktär hämtas i normala fall från den maskinläsbara delen av passagerarens pass. Uppgifterna ska vidarebefordras till myndigheterna efter incheckning. Myndigheterna får spara passageraruppgifterna i ett tillfälligt register i 24 timmar och ska därefter radera dem om inte uppgifterna behövs för att de myndigheter som ansvarar för genomförandet av personkontroller vid de yttre gränserna ska kunna utföra sina lagstadgade uppgifter.

Medlemsstaterna ska införa sanktioner mot de transportörer som genom fel eller försummelse underlåter att lämna uppgifter eller som lämnar ofullständiga eller felaktiga uppgifter.

I svensk rätt har direktivet genomförts främst genom nya bestämmelser i utlänningslagen samt genom lagen (2006:444) om passagerarregister.

4.5.2 API-direktivets genomförande i utlänningslagen

API-direktivets bestämmelser om transportörers skyldigheter har i Sverige genomförts genom bestämmelser i 9 och 19 kap. utlänningslagen.

I 9 kap. 3 a § anges att en transportör, som luftvägen ska transportera passagerare till Sverige direkt från en stat som inte tillhör EU och inte heller har slutit avtal om samarbete enligt Schengenkonventionen med konventionsstaterna, på begäran av Polismyndigheten ska överföra uppgifter om de ankommande passagerarna så snart incheckningen avslutats. De uppgifter som ska överföras är

1. nummer på och typ av resehandling som används,
2. medborgarskap,
3. fullständigt namn,
4. födelsedatum,

5. gränsövergångsstället för inresa,
6. transportkod,
7. avgångs- och ankomsttid för transporten,
8. det totala antalet passagerare vid transporten, och
9. ursprunglig ort för ombordstigning.

De insamlade uppgifterna ska enligt 3 b § samlas in av transportören och överföras elektroniskt till Polismyndigheten. Om det inte är möjligt att föra över uppgifterna elektroniskt ska de överföras på annat lämpligt sätt. I 3 c § anges att bestämmelser om behandlingen av de uppgifter som överförts till Polismyndigheten finns i lagen om passagerarregister.

I 3 d § anges att en transportör som har överfört uppgifter enligt 3 a § inom 24 timmar efter det att transportmedlet har anlänt till gränsövergångsstället ska radera de insamlade och överförda uppgifterna.

En transportör som samlar in uppgifter som är avsedda att överföras enligt 3 a § ska enligt 3 e § informera passagerarna enligt bestämmelserna i 23–26 §§ PUL. Informationsskyldigheten enligt de nämnda bestämmelserna omfattar bl.a. den personuppgiftsansvareges identitet, ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen.

I 19 kap. 5 a § framgår att en transportör som inte har fullgjort sin uppgiftsskyldighet kan bli skyldig betala en särskild avgift. Enligt 19 kap. 6 § ska den särskilda avgiften för varje flygning som har gjorts utan att transportören har fullgjort sin uppgiftsskyldighet bestämmas till högst 46 000 kr.

4.5.3 Lagen om passagerarregister

I lagen om passagerarregister finns bestämmelser om behandlingen av de API-uppgifter som har överförts till Polismyndigheten enligt 9 kap. 3 b § utlänningslagen. I 1 § anges att Polismyndigheten med hjälp av automatiserad behandling ska föra ett register över sådana passagerare som avses i 9 kap. 3 a § utlänningslagen. Myndigheten

är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Av 2 § framgår att personuppgiftslagen är tillämplig om inget annat följer av lagen eller föreskrifter som har meddelats med stöd av den. Det framgår också att en registrerad person inte har rätt att motsätta sig sådan behandling som är tillåten enligt lagen. I 3 § definieras vissa begrepp.

I 4 § anges passagerarregistrets ändamål. Registret ska föras för att underlätta verkställandet av personkontroller vid Sveriges gräns mot stater som inte tillhör Europeiska unionen och inte heller har träffat avtal om samarbete enligt Schengenkonventionen med konventionsstaterna.

Registret får enligt 5 § endast innehålla de uppgifter som har inkommit i enlighet med 9 kap. 3 a § utlänningslagen.

Personuppgifter i passagerarregistret ska på begäran lämnas ut till Säkerhetspolisen och Tullverket för sådan verksamhet som avses i 4 §. Personuppgifterna får dock inte lämnas ut på medium för automatiserad behandling. Säkerhetspolisen får dock ha direktåtkomst till personuppgifterna i registret. Regeringen får meddela föreskrifter om utlämnande till och direktåtkomst för fler myndigheter. (Se 6–8 §§.)

I 9 § anges att en uppgift i passagerarregistret ska gallras inom 24 timmar efter överföringen till Polismyndigheten. Om uppgifter i registret behövs för att Polismyndigheten, Säkerhetspolisen eller Tullverket ska kunna verkställa personkontroller enligt 4 §, får uppgifterna i registret dock stå kvar till dess att myndighetens kontroller är slutförda.

Vid behandling av personuppgifter enligt lagen eller enligt föreskrifter som har meddelats med stöd av lagen gäller bestämmelserna i personuppgiftslagen om rättelse och skadestånd (10 §).

Tullverket har nyligen i en framställan till regeringen hemställt om att medges direktåtkomst till passagerarregistret.

5 Dagens reglering och användning av flygpassageraruppgifter i brottsbekämpningen

5.1 Inledning

Brottsbekämpning är ett samlingsbegrepp för alla åtgärder som syftar till att motverka brottslighet. I det brottsbekämpande arbetet innefattas självfallet att utreda begångna brott. Men även åtgärder för att förebygga, förhindra och upptäcka brottslig verksamhet innefattas i begreppet. I svensk lagstiftning brukar man skilja mellan sådan verksamhet som innebär att förebygga, förhindra och upptäcka brottslig verksamhet samt utredning och beivrande av konkreta brott. Åtskillnad görs alltså mellan sådan informations- och underrättelseinhämtning, ”spaning”, som sker innan det finns anledning att anta att ett brott som hör under allmänt åtal har begåtts och sådan utredning som sker sedan en förundersökning enligt 23 kap. 1 § RB har inletts.

I polisens arbetsuppgifter ingår att förebygga och utreda all brottslighet. Även Tullverket har till uppgift att bl.a. bekämpa brott. I den brottsbekämpande verksamheten har Tullverket till uppgift att övervaka och kontrollera trafiken till och från utlandet, så att bestämmelserna om in- och utförsel av varor efterlevs.

Det är Polismyndigheten som ansvarar för personkontrollen vid våra yttre gränser, medan Tullverket svarar för varukontrollen. Även om tullens verksamhet är inriktad på varor får den brottsbekämpande verksamheten indirekt en viss anknytning till personer, eftersom det är personer som för varorna med sig över gränserna och kan dömas för smugglingsbrott. Tullverket och Kustbevakningen är skyldiga att bistå Polismyndigheten vid kontrollen av utlänningars inresa och utresa. Mellan Polismyndigheten och Tullverket har träffats en överenskommelse om samverkan vad gäller person- och tull-

kontroll vid yttre gräns. Tullverket ansvarar emellertid för närvarande inte för personkontroll vid någon flygplats.

Sverige inträdde i EU den 1 januari 1995. Inträdet innebar bl.a. att gränsformaliteter mellan Sverige och de övriga EU-staterna i princip inte längre skulle förekomma. Borttagandet av dessa formaliteter innebar emellertid att tullens kontroll över varuflödet till Sverige minskade och att det således fanns en ökad risk för olaglig införsel av bl.a. narkotika, vapen och dopningsmedel. Som kompensatorisk åtgärd för detta införde Sverige den 1 juli 1996 en möjlighet för tullen att i den brottsbekämpande verksamheten inhämta uppgifter från transportörer i fråga om bl.a. passagerare för att uppnå bättre träffsäkerhet i kontrollerna med mindre störning i den legala trafiken över gränserna. Motsvarande bestämmelser infördes för polisens del den 1 april 1998. I förarbetena till införandet av bestämmelserna för Tullverkets del angavs att uppgiftsskyldigheten innebär att tullen får en möjlighet att förhandsgranska de kommersiella datoriserade bokningssystemen för internationell trafik för att kunna göra en riskbedömning avseende ankommande last och passagerare innan transportmedlet kommer (se prop. 1995/96:166 s. 78). Detsamma gäller för polisens del.

5.2 Tillämpliga bestämmelser

5.2.1 Polismyndigheten och Säkerhetspolisen

Som angetts ovan har polisen sedan år 1998 rätt att få tillgång till uppgifter från transportföretag redan innan misstanke om ett visst konkret brott har uppstått. Detta regleras i 25 och 26 §§ polislagen (1984:387). På begäran av Polismyndigheten eller Säkerhetspolisen ska således ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter som företaget har tillgång till. Uppgifter om passagerare ska avse namn, resrutt, bagage, medpassagerare samt sättet för betalning och bokning. Polisen får begära in uppgifterna endast om de kan antas ha betydelse för den brottsbekämpande verksamheten. Avsikten är dock inte att uppgifterna ska begäras in för att bekämpa rena bagatellbrott. Detta framgår redan av proportionalitetsprincipen i 8 § polislagen (se prop. 1996/97:175 s. 68).

Uppgifterna kan lämnas på så sätt att de görs läsbara genom terminalåtkomst. Härmed avses detsamma som numera normalt benämns direktåtkomst. Polismyndigheten och Säkerhetspolisen får emellertid ta del av uppgifterna på detta sätt endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. De får inte ändra eller på annat sätt bearbeta eller lagra uppgifter som hålls tillgängliga på detta sätt. Uppgifter om enskilda som har lämnats på annat sätt än genom terminalåtkomst ska omedelbart förstöras, om de visar sig sakna betydelse för utredning eller lagföring av brott.

Regleringen är inte avsedd att tillåta någon systematisk kartläggning av resandeströmmar eller något generellt insamlande av uppgifter. Det är inte heller avsett att uppgifter om resande ska registreras, lagras eller bearbetas på ett sådant sätt att nya personregister med uppgifter om resande skapas. Uppgifter som inhämtas genom uppkoppling till databaser via terminal (direktåtkomst) anses således fortfarande tillhöra och förvaras hos transportföretaget. (Jfr prop. 1995/96:166 s. 81 ff.)

För det fall uppgifterna anses ha betydelse för utredning eller lagföring får informationen sparas i enskilda brottsutredningar med stöd av bestämmelserna i polisdatalagen.

5.2.2 Tullverket

Tullverkets befogenhet att inhämta vissa passageraruppgifter från transportföretag om uppgifterna kan antas ha betydelse för dess brottsbekämpande verksamhet infördes år 1996. Bestämmelserna finns numera i 4 kap. 6–8 §§ tullagen (2016:253) samt i 15 och 16 §§ lagen (1996:701) om Tullverkets befogenhet vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränslagen). Bestämmelserna motsvarar de i 25–26 §§ polislagen.

Kompletterande bestämmelser finns i 4 kap. 4–9 §§ tullförordningen (2016:287) och i 3–7 §§ förordningen (1996:702) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen. Bl.a. anges att information om innehållet i de inhämtade bokningsuppgifterna får lämnas till andra tulltjänstemän, andra enheter inom Tullverket, Polismyndigheten och Kustbevakningen om uppgiften behövs i Tullverkets brottsbekämpande verk-

samhet för att klarlägga om brott eller brottslig verksamhet har förekommit, pågår eller planeras. Sådan information får också lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en konvention som Sverige har tillträtt eller en överenskommelse som Sverige har ingått.

Om transportföretag inte lämnar bokningsuppgifter på Tullverkets begäran har Tullverket möjlighet att förelägga transportföretaget att vid vite lämna uppgifterna. Bestämmelser härom finns i 4 kap. 24 § och 7 kap. 5 § tullagen samt i 21 § inregränslagen.

Användningen av passageraruppgifter inom Tullverket regleras i dag i övrigt av lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, främst 13 §. Den lagen ska dock ersättas av en ny lag om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet, tullbrottsdatalagen. Den nya lagen träder i kraft den 1 juli 2017 (se prop. 2016/17:91). I förslaget till tullbrottsdatalag finns bestämmelser om personuppgifter från transportföretag intagna i 2 kap. 8 och 9 §§.

Enligt 2 kap. 8 § TBL får personuppgifter som har lämnats till Tullverket enligt de aktuella bestämmelserna i tullagen eller inregränslagen behandlas i den utsträckning det är tillåtet enligt dessa lagar och enbart i den utsträckning det behövs för planering av kontrollverksamheten och urval av kontrollobjekt. Om det behövs i ett enskilt fall får, enligt andra stycket, personuppgifterna behandlas för något av lagens primära ändamål och göras gemensamt tillgängliga. I 2 kap. 9 § finns bestämmelser om i vilka fall identitetsbeteckningar såsom namn och personnummer får användas som sökbegrepp vid sökning i sådana personuppgifter som lämnats till Tullverket enligt 8 § första stycket. Sådana sökbegrepp får användas bara om uppgifterna avser en person som är eller har varit misstänkt för brott eller kan antas ha samband med brottslig verksamhet eller som övervakas på grund av misstanke om att personen kan komma att utöva brottslig verksamhet. För personuppgifter som har gjorts allmänt tillgängliga gäller lagens bestämmelser om sökning bland sådana uppgifter.

5.3 Dagens användning av PNR-uppgifter

5.3.1 Polismyndigheten

Polismyndigheten arbetar i dag i en mycket begränsad omfattning med PNR- och API-uppgifter för att förhindra grov brottslighet i form av narkotikasmuggling, människosmuggling och penningtvätt. Främst används uppgifterna av gränspolisen i gränskontrollverksamheten.

Passageraruppgifterna används både för att hitta kända personer och för att leta efter mönster som kan indikera att en person är av intresse, s.k. profilering.

Endast ett flygbolag tillhandahåller terminalåtkomst till sitt bokningssystem. De API- och PNR-uppgifter som behandlas utgörs således främst av sådan information som finns tillgänglig på de passagerarlistor som flygbolagen manuellt tillhandahåller vid förfrågan. Vid sådana förfrågningar kan uppgifterna överlämnas i pappersform från flygbolagen över disk. Uppgifterna kan även levereras via fax eller e-post. Kvaliteten på informationen skiljer sig åt då flygbolagen har olika reservations- och incheckningssystem. Uppgifterna från flygbolagen innehåller ofta grundläggande uppgifter. Efterfrågas mer information måste flygbolagen kontaktas igen för komplettering.

Även analysen av de uppgifter som inhämtas sker manuellt då Polismyndigheten saknar tekniskt stöd för hantering av uppgifterna. Varje passagerare hanteras individuellt vilket är ett tidskrävande arbete. Arbetet ställer också höga krav på analytikern då antalet parametrar som ska granskas kan vara stort.

Bristen på IT-stöd hindrar en kontinuerlig bevakning då antalet resenärer är för stort för att uppgifterna ska kunna hanteras manuellt. Analysarbetet blir också extremt krävande med långa handläggningstider och innebär att enbart ett fåtal av alla resenärer kan profileras.

5.3.2 Säkerhetspolisen

Säkerhetspolisen arbetar i dag med insamling av API- och PNR-uppgifter i sitt arbete med kontraterrorism, kontraspionage, författningsskydd och personskydd. PNR-uppgifter används främst för kartläggning.

Vid de tillfällen då PNR-uppgifter behövs tas en direktkontakt med det flygbolag som bedöms kunna ge efterfrågade uppgifter. Denna hantering innebär en osäkerhet i informationshantering, vilket kan medföra att frågor ställs till en större skara än nödvändigt. De uppgifter som levereras från flygbolagen skiljer sig åt och innehåller i flera fall inte tillräcklig information.

Säkerhetspolisen saknar direktåtkomst till system som lagrar PNR-uppgifter eller API-uppgifter. Vissa passageraruppgifter kan komma myndigheten till handa via myndighetssamverkan. All tillgång till passageraruppgifter kräver dock fysisk närvaro av särskilda personer och fysisk tillgång till system på flygplatsen. Detta gör att Säkerhetspolisen inte kan räkna med att information går att få fram just när den behövs.

Säkerhetspolisen saknar tekniskt stöd för hantering av såväl API- som PNR-uppgifter och all hantering sker manuellt. Vid behov kan Säkerhetspolisen använda ett eget analysystem inköpt av en extern leverantör för att analysera de PNR- och API-uppgifter som samlas in manuellt. Underlaget är varierande beroende på vilket flygbolag som har levererat uppgifterna och det krävs ett stort manuellt arbete för att mata in informationen i analysystemen.

5.3.3 Tullverket

Tullverket är den myndighet som i störst utsträckning använder API- och PNR-uppgifter i dag. Uppgifterna används främst för att upptäcka brottslighet i form av smuggling av narkotika, dopningsmedel och cigaretter. Tullverket kan även dela med sig av PNR-uppgifter till övriga brottsbekämpande myndigheter i vissa fall.

Tullverket delar uppgifter med andra länder, främst i Norden. Enbart uppgifter om specifika brottsmisstänkta personer delas för att möjliggöra identifiering och matchning av liknande inkommande händelser.

Tullverket begär in eller hämtar själv in PNR-uppgifter från flygbolagen. Tullen har tillgång till vissa flygbolags bokningssystem och kan på så sätt få del av uppgifterna via direktåtkomst. Uppgifterna skickas även till Tullverket från flygbolagen via e-post eller fax. Informationen inkommer i ett stort antal olika format. För att underlätta en snabb och effektiv sökning för planering och urval av

lämpliga kontrollobjekt får uppgifterna formateras om till ett användarvänligt format och sammanställas elektroniskt. Sammanställningen sker i ett avgränsat system. Tullverket har således visst systemstöd till sin hjälp vid överföringen av uppgifterna. All inhämtning, profilering och analys av uppgifterna hanteras dock manuellt.

Tullverket använder PNR-uppgifter för att profilera sedan tidigare okända personer. En profilering börjar med att Tullverket begär in eller själv hämtar bokningsuppgifterna som behövs för att genomföra profileringen. När bokningsuppgifterna finns tillgängliga analyseras uppgifterna. Efter analys skickas utfallet vidare till det s.k. tullfiltret som agerar på underlaget.

Tullverket har dagligen åtkomst till bokningsuppgifter från 32 flygbolag, antingen via direktåtkomst eller genom att flygbolagen skickar sina uppgifter till Tullverket. Hur stor del av dessa uppgifter som tullen faktiskt tar del varierar. Vissa dagar sker inte någon profilering över huvud taget beroende på personalsituationen. Vissa bolag, vars bokningssystem tullen har direktåtkomst till, anses inte utgöra en risk ur ett tullperspektiv. Dessa bokningsuppgifter granskas därför sällan. Av samtliga ankommande resenärer till statliga och kommunala flygplatser år 2015 kontrollerade Tullverket mindre än 1 procent.

Alla grova narkotikabeslag på Arlanda år 2015 i passagerartrafiken var baserade på tillgång till PNR-uppgifter. Alla gripna kurirer var tidigare okända för svenska myndigheter. Samtliga beslag avsåg flygningar inom EU.

6 Dataskyddsreglering

6.1 Internationella konventioner

6.1.1 Europakonventionen m.m.

Enligt artikel 8 i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får endast göra inskränkningar i dessa rättigheter med stöd av lag och om det är nödvändigt i ett demokratiskt samhälle för vissa i artikeln uppräknade ändamål, bl.a. med hänsyn till den allmänna säkerheten och till förebyggande av oordning och brott. Artikel 8 skyddar bl.a. mot felaktig behandling av personuppgifter.

Europakonventionen gäller som svensk lag. Det framgår av 2 kap. 19 § RF att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Även i FN:s konvention om medborgerliga och politiska rättigheter finns en bestämmelse till skydd för godtyckligt eller olagligt ingripande i någons privat- och familjeliv (artikel 17).

6.1.2 Dataskyddskonventionen

Europarådets ministerkommitté antog år 1981 en konvention till skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen). Konventionen trädde i kraft den 1 oktober 1985. Sverige har, liksom övriga EU-medlemsstater, anslutit sig till konventionen. Ett arbete med att se över konventionen pågår.

Dataskyddskonventionens syfte är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till per-

sonlig integritet i samband med automatiserad behandling av personuppgifter. Konventionens tillämpningsområde är enligt huvudregeln automatiserade personregister och automatisk databehandling av personuppgifter i allmän och enskild verksamhet.

Konventionen innehåller principer för dataskydd som de konventionsanslutna staterna måste iaktta i sin nationella lagstiftning. Bl.a. ska personuppgifter som är föremål för automatiserad behandling samlas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Vidare måste uppgifterna vara relevanta för ändamålen med behandlingen och får inte senare användas på ett sätt som är oförenligt med dessa. Uppgifterna måste också vara riktiga och aktuella och de får inte bevaras längre tid än vad som är nödvändigt för ändamålen.

Vissa kategorier av personuppgifter får enligt konventionen behandlas endast om den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana personuppgifter hör uppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, sexualliv och uppgifter om brott. Vidare föreskrivs att en registrerad bl.a. ska ha möjlighet till insyn i register och till att få uppgifter rättade.

Under vissa förutsättningar får undantag göras från bestämmelserna i konventionen om bl.a. uppgifternas beskaffenhet. Sådana inskränkningar förutsätter stöd i den nationella lagstiftningen och att inskränkningen är nödvändig i ett demokratiskt samhälle för vissa angivna ändamål, t.ex. brottsbekämpning.

Konventionen kompletteras med flera av ministerkommittén antagna rekommendationer om hur personuppgifter bör behandlas inom olika områden. En sådan rekommendation rör polisen.

6.2 Gällande EU-rättslig reglering

6.2.1 EU-stadgan om de grundläggande rättigheterna

I artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna slås fast att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sin korrespondens. I artikel 8 föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har

rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna efterlevs.

I artikel 52 i stadgan anges i vilken utsträckning inskränkningar får göras i de rättigheter som erkänns i stadgan. Utgångspunkten är att sådana inskränkningar endast får göras i lag och ska vara förenliga med det väsentliga innehållet i rättigheterna. Begränsningar får endast göras om de är nödvändiga och svarar mot ett allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

6.2.2 Dataskyddsdirektivet

Den allmänna regleringen av behandling av personuppgifter inom EU finns i dag i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU.

Direktivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204) med tillhörande förordning (se avsnitt 6.3.2). Direktivet gäller inte för behandling av personuppgifter som faller utanför gemenskapsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område.

6.2.3 Dataskyddsrambeslutet

Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) reglerar dataskyddet inom angivna områden. Rambeslutet är föranlett av ett antal EU-instrument rörande utvidgat polisiärt och rättsligt samarbete avseende gränsöverskridande informationsutbyte. Det är tillämpligt på uppgifter som överförs eller görs tillgängliga mellan medlemsstater och EU-organ eller vissa utpekade informationssystem. Dataskydds-

rambeslutet gäller däremot inte för rent nationell personuppgiftsbehandling. Från tillämpningsområdet undantas också personuppgiftsbehandling inom området nationell säkerhet.

Dataskyddsrambeslutet uppfylls redan till stora delar av befintlig lagstiftning. De återstående delarna har genomförts i svensk rätt genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag) med tillhörande förordning (se avsnitt 6.4.5).

6.3 Huvuddragen i den svenska regleringen

6.3.1 Regeringsformen

Grundläggande bestämmelser till skydd för den personliga integriteten finns i regeringsformen. I 1 kap. 2 § första stycket slås det fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och i fjärde stycket anges bl.a. att det allmänna ska värna den enskildes privatliv och familjeliv. Enligt 2 kap. 6 § andra stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar i det grundlagsfästa skyddet kan endast göras genom lag och bara under de förutsättningar som anges i 2 kap.

Andra stycket i 2 kap. 6 § infördes vid 2010 års grundlagsreform. Bestämmelsen omfattar enbart betydande intrång i den enskildes privata sfär. I förarbetena anges att det är naturligt att det läggs stor vikt vid uppgifternas karaktär vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden. Ju känsligare uppgifterna är, desto mer ingripande måste det allmännas hantering av uppgifterna normalt anses vara. Även hantering av ett litet fåtal uppgifter kan innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär. Vid bedömningen av intrångets karaktär är det också naturligt att stor vikt läggs vid ändamålet med behandlingen. En hantering som syftar till att utreda brott kan enligt förarbetena normalt anses vara mer känslig

än t.ex. en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Mängden uppgifter kan också vara en betydelsefull faktor i sammanhanget. (Se prop. 2009/10:80 s. 183.)

6.3.2 Personuppgiftslagen

Lagens syfte och tillämpningsområde

Personuppgiftslagen, genom vilket det nu gällande dataskyddsdirektivet genomfördes i svensk rätt, syftar till att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Kompletterande bestämmelser till lagen finns i personuppgiftsförordningen (1998:1191).

Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Begreppet behandling av personuppgifter omfattar i stort sett allt man kan göra med sådana uppgifter, t.ex. att samla in, söka, bevara eller sprida uppgifterna.

Lagen innehåller generella regler för all behandling av personuppgifter och behandlar även sådan verksamhet som faller utanför unionsrätten. Enligt 2 § gäller särreglering i lag eller förordning framför bestämmelserna i personuppgiftslagen. Sådan särreglering finns framför allt i olika registerförfattningar.

Enligt 5 § ska lagen tillämpas på all helt eller delvis automatiserad behandling av personuppgifter. Dessutom är den tillämplig på manuell behandling av personuppgifter som ingår, eller är avsedda att ingå, i en strukturerad samling av personuppgifter vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Behandling av uppgifter om juridiska personer, som definitionsmässigt inte utgör personuppgifter, omfattas inte av personuppgiftslagen. Sådan behandling som en fysisk person utför i verksamhet av rent privat natur undantas också enligt 6 §.

Grundläggande krav på behandlingen

Vissa grundläggande krav för all behandling av personuppgifter slås fast i 9 § PUL. Där anges att personuppgifter alltid ska behandlas lagligt, på ett korrekt sätt och i enlighet med god sed. Personuppgifter ska samlas in och behandlas bara för särskilda, uttryckligt angivna ändamål. Efter insamlingen får uppgifterna inte behandlas för något annat ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in (den s.k. finalitetsprincipen). De personuppgifter som behandlas ska vidare vara riktiga och relevanta i förhållande till ändamålen med behandlingen och får inte vara fler än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Om det är nödvändigt ska uppgifterna vara aktuella. För det fall personuppgifterna inte uppfyller dessa krav, ska alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna uppgifterna.

Personuppgifter får inte bevaras längre tid än nödvändigt med hänsyn till ändamålen med behandlingen. Därefter ska de avidentifieras eller förstöras. Eftersom personuppgiftslagen är subsidiär till annan lagstiftning får uppgifter inte avidentifieras eller förstöras om det strider mot annan lagstiftning, t.ex. tryckfrihetsförordningens bestämmelser om allmänna handlingar eller arkivlagstiftningen.

Tillåten och otillåten behandling

I 10–12 §§ PUL finns en uttömmande uppräkningslista av de fall där behandling av personuppgifter är tillåten. Den registrerades samtycke är alltid en legitim rättslig grund för behandling. Återkallar personen sitt samtycke får ytterligare uppgifter om honom eller henne inte behandlas.

I vissa fall får personuppgifter behandlas även om den registrerade inte har gett sitt samtycke. En förutsättning i dessa fall är att behandlingen är nödvändig för ändamålen.

Personuppgifter får behandlas i samband med ett avtal med den registrerade, när det behövs för att fullgöra avtalet eller när det behövs för att på den registrerades begäran vidta åtgärder innan avtalet träffas. Som exempel på behandling som kan vara nödvändig för att fullgöra ett avtal kan nämnas fakturering och förande av kundregister. Vidare får behandling utföras om den är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig

skyldighet. Dessutom får personuppgifter behandlas för att skydda vitala intressen för den registrerade. Likaså får personuppgifter behandlas om det är nödvändigt för att den personuppgiftsansvarige, eller en tredje man till vilken personuppgifter lämnas ut, ska kunna utföra en arbetsuppgift i samband med myndighetsutövning. Slutligen får personuppgifter behandlas om en avvägning ger vid handen att den personuppgiftsansvariges berättigade intresse av behandling väger tyngre än den registrerades intresse av skydd.

Behandling av känsliga personuppgifter

I 13 § PUL förbjuds behandling av känsliga personuppgifter. Med detta avses uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv.

Från förbudet mot behandling av känsliga uppgifter gäller ett flertal undantag som närmare regleras i 15–19 §§ PUL.

Regeringen, eller den myndighet regeringen bestämmer, får enligt 20 § föreskriva ytterligare undantag från förbudet i 13 §, om det behövs med hänsyn till ett viktigt allmänt intresse.

Information till den registrerade

Personuppgiftslagen innehåller ett flertal bestämmelser som syftar till att genom information trygga den enskildes rätt att kontrollera om behandling av personuppgifter om honom eller henne pågår. Om uppgifter om en person samlas in från personen själv, ska den personuppgiftsansvarige enligt 23 § självant lämna den registrerade information om behandlingen av uppgifterna. Har uppgifterna samlats in från en annan källa, ska den personuppgiftsansvarige enligt 24 § självant informera den registrerade när uppgifterna noteras, eller om avsikten med behandlingen är att lämna ut dem till tredje man, när uppgifterna lämnas ut första gången. Informationen behöver dock inte lämnas om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i lag eller annan författning. Information behöver heller inte lämnas om det skulle vara omöjligt eller kräva en oproporionerligt stor arbetsinsats.

Informationen ska enligt 25 § omfatta uppgift om vem som är personuppgiftsansvarig, ändamålen med behandlingen och all övrig information som den registrerade behöver för att kunna ta till vara sina rättigheter i samband med behandlingen. Information behöver inte lämnas om sådant som den registrerade redan känner till.

Enligt 26 § är den personuppgiftsansvarige vidare skyldig att på ansökan, en gång per år, gratis informera om uppgifter om sökanden behandlas eller inte, ändamålen med behandlingen, vilka uppgifter som behandlas, varifrån dessa kommer och till vem de lämnas ut. Någon information behöver dock inte lämnas om personuppgifter som endast behandlas i löpande text som ännu inte fått sin slutliga utformning eller utgör minnesanteckning, utom i de fall där uppgifterna har lämnats till tredje man eller – i fråga om behandling i löpande text – har behandlats under längre tid än ett år.

Informationsskyldigheten gäller enligt 27 § inte om uppgifterna omfattas av sekretess eller tystnadsplikt.

Rättelse

Personuppgifter som är felaktiga eller ofullständiga eller som annars inte har behandlats i enlighet med personuppgiftslagen, ska enligt 28 § på begäran av den registrerade rättas, blockeras eller utplånas av den personuppgiftsansvarige. Om felaktiga personuppgifter har lämnats till tredje man, ska denne i vissa fall informeras om korrigeringen.

Säkerhet vid behandlingen

I 30 och 31 §§ PUL finns allmänna bestämmelser om säkerheten vid behandling av personuppgifter. Bestämmelserna avser att trygga både den tekniska säkerheten och att de personer som behandlar uppgifterna har tillräckliga instruktioner för att behandla uppgifterna på ett korrekt sätt. Den personuppgiftsansvarige ansvarar för säkerheten.

Överföring av personuppgifter till tredjeland

Enligt 33 § PUL är det förbjudet att till tredjeland föra över personuppgifter under behandling om landet i fråga inte har en adekvat nivå för skydd av personuppgifter. Förbudet gäller också överföring av personuppgifter för behandling i tredjeland. Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredjelandet.

I 34 § anges vissa undantag från förbudet i 33 §. Ett viktigt undantag är att det är tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen. I 35 § PUL finns vissa bemyndiganden som ger möjlighet att besluta om ytterligare undantag i förbudet i 33 §. I bilagor till personuppgiftsförordningen anges vilka stater som enligt särskilda beslut av kommissionen anses ha en adekvat skyddsnivå för behandlingen av personuppgifter vid överföring till vissa i besluten specificerade mottagare.

I 13 a § PUF finns en specialbestämmelse som reglerar transportörens överföring av flygpassageraruppgifter till tredjeland. Enligt bestämmelsen får en transportör som luftvägen transporterar passagerare till eller från ett tredjeland, till det landet föra över personuppgifter som finns i transportörens passagerarförteckning, om det sker enligt villkor som framgår av en överenskommelse mellan tredjelandet och EU avseende behandling och överföring av uppgifter rörande flygpassagerare. I en bilaga till förordningen anges att sådana överenskommelser gäller mellan EU och USA respektive Australien.

Tillsyn

Datainspektionen är enligt 2 § PUF tillsynsmyndighet enligt personuppgiftslagen. Inspektionen är som regel också tillsynsmyndighet för sådan behandling av personuppgifter som regleras i särskilda registerförfattningar. Datainspektionen har till uppgift att bl.a. verka för att människor skyddas mot att den personliga integriteten kränks genom behandling av personuppgifter. Inspektionen informerar bl.a. om gällande regler, utövar tillsyn över att reglerna efterlevs och ger

råd och hjälp åt personuppgiftsombud. I 43–47 §§ PUL finns närmare bestämmelser om tillsynsmyndighetens befogenheter, t.ex. om rätt att meddela vite och möjligheten att förbjuda viss behandling.

Sanktioner

I 48 § PUL regleras den registrerades rätt till skadestånd för den kränkning som en behandling av personuppgifter i strid med lagen har orsakat. Lagen innehåller också en straffbestämmelse. Enligt 49 § kan den som uppsåtligt eller av grov oaktsamhet överträder vissa bestämmelser i lagen dömas för brott mot personuppgiftslagen.

6.4 Aktuella särregleringar

6.4.1 Polisdatalagen

Syfte och tillämpningsområde

Polisdatalagen (2010:361) är tillämplig vid behandling av personuppgifter i brottsbekämpande verksamhet vid Polismyndigheten och Säkerhetspolisen. Lagen gäller även för den polisiära verksamheten vid Ekobrottsmyndigheten. Kompletterande bestämmelser finns i polisdataförordningen (2010:1155).

Syftet med lagen är att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och att skydda enskilda mot att deras personliga integritet kränks vid sådan behandling.

Lagen är tillämplig endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Enligt 1 kap. 6 § tillämpas lagen även i viss utsträckning på behandling av uppgifter om juridiska personer.

Lagen är generellt utformad. Det finns dock även andra författningar som reglerar personuppgiftsbehandling i polisens brottsbekämpande verksamhet, framför allt lagstiftning som reglerar behandling i särskilda register. I 1 kap. 3 § undantas från lagens tillämpningsområde behandling av personuppgifter enligt bl.a. lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen

(2000:344) om Schengens informationssystem och lagen (2006:444) om passagerarregister.

Förhållande till personuppgiftslagen

Polisdatalagen gäller enligt 2 kap. 1 § i stället för personuppgiftslagen. I 2 kap. 2 § hänvisas dock till ett betydande antal bestämmelser i personuppgiftslagen som gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter, information till den registrerade, tillsyn och sanktioner.

Ändamål för behandling och utlämnande av uppgifter

I 2 kap. PDL anges för vilka ändamål personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Enligt 2 kap. 7 § får personuppgifter behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott, eller fullgöra förpliktelser som följer av internationella åtaganden. Bestämmelsen innehåller de primära ändamål för vilka personuppgifter enligt lagen får behandlas.

I 2 kap. 8 § anges de sekundära ändamålen för vilka personuppgifter får behandlas enligt lagen. De ändamålen aktualiseras när personuppgifter som behandlas i polisens brottsbekämpande verksamhet lämnas ut till andra myndigheter eller organisationer för deras behov. Enligt bestämmelsen får personuppgifter behandlas genom sådant utlämnande när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket eller hos utländsk myndighet eller mellanfolklig organisation. Personuppgifter får också behandlas för att lämnas ut för vissa andra i paragrafen specificerade ändamål eller för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen).

Enligt 2 kap. 9 § får personuppgifter också behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till

Polismyndigheten eller Ekobrottsmyndigheten i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I 2 kap. 15 § finns sekretessbrytande bestämmelser som anger i vilken utsträckning personuppgifter får lämnas ut till bl.a. Interpol och Europol, utländsk underrättelse- eller säkerhetstjänst och annan utländsk myndighet eller mellanfolklig organisation. Sekretessbrytande bestämmelser som gäller i förhållande till vissa andra myndigheter finns i 2 kap. 16–18 §§.

Behandling av känsliga personuppgifter

För behandling av känsliga personuppgifter finns särskilda begränsningar i 2 kap. 10 § PDL. Enligt bestämmelsen får uppgifter om en person inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter om det är absolut nödvändigt för syftet med behandlingen.

Register som regleras särskilt i polisdatalagen

Några register regleras särskilt i 4 kap. PDL. Dessa är register över dna-profiler, dvs. dna-registret, utredningsregistret och spårregistret, fingeravtrycks- och signalementsregister, penningtvättsregister och det internationella registret. För dessa register finns särskilda bestämmelser om ändamål, gallring och direktåtkomst.

Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet

I 6 kap. PDL finns bestämmelser om behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. Bestämmelserna reglerar framför allt ändamålen för Säkerhetspolisens personuppgiftsbehandling, som delvis avviker från regleringen för Polismyndigheten. Det finns även särskilda bestämmelser om bevarande och gallring. När det gäller utlämnande av personuppgifter och uppgifts-

skyldighet gäller i huvudsak samma bestämmelser som för Polismyndigheten.

6.4.2 Tullbrottsdatalag

En ny lag för Tullverkets personuppgiftsbehandling

Lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet gäller för närvarande för Tullverkets personuppgiftsbehandling i denna verksamhet. Lagen kommer att ersättas av en ny lag, tullbrottsdatalagen (prop. 2016/17:91) den 1 juli 2017. Mot den bakgrunden redovisas här enbart förslaget till tullbrottsdatalag.

Lagens tillämpningsområde

Tullbrottsdatalagen har utformats i nära anslutning till andra dataskyddslagar på det brottsbekämpande området, t.ex. polisdatalagen. Lagen ska reglera all behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. Enligt 1 kap. 2 § ska lagen endast gälla om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Lagen ska enligt 1 kap. 4 § i viss utsträckning även tillämpas på behandling av uppgifter om juridiska personer.

Förhållandet till personuppgiftslagen

Tullbrottsdatalagen ska gälla i stället för personuppgiftslagen, men hänvisningar görs i 2 kap. 2 § till vissa bestämmelser i personuppgiftslagen som ändå ska tillämpas. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter, information till den registrerade, tillsyn och skadestånd.

Ändamål för behandling och utlämnande av uppgifter

De ändamål för vilka personuppgifter ska få behandlas i Tullverkets brottsbekämpande verksamhet är uppdelade i primära och sekundära ändamål. Personuppgifter ska enligt 2 kap. 5 § TBL få behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, för att utreda eller beivra brott eller för att fullgöra förpliktelser som följer av internationella åtaganden. Personuppgifter som behandlas enligt den paragrafen ska också få behandlas när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Skatteverket eller en utländsk myndighet eller mellanfolklig organisation. Personuppgiftsbehandling genom utlämnande ska också enligt 2 kap. 6 § vara tillåten om den är nödvändig för att tillhandahålla information som behövs i verksamhet hos Kriminalvården för att förebygga brott och upprätthålla säkerheten och i annan verksamhet som Tullverket ansvarar för, om det finns särskilda skäl för att tillhandahålla informationen. Likaså får personuppgifter i ett enskilt fall behandlas för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen). Särskilda regler föreslås gälla för behandling av vissa personuppgifter från transportföretag, se avsnitt 5.2.2.

Personuppgifter ska enligt 2 kap. 7 § också få behandlas om det är nödvändigt för diarieföring, eller om uppgifterna har lämnats till Tullverket i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I 2 kap. 12 § finns en sekretessbrytande bestämmelse som anger i vilken utsträckning personuppgifter får lämnas ut till bl.a. Interpol och Europol, utländsk polismyndighet eller åklagarmyndighet och tullmyndighet eller kustbevakning inom Europeiska ekonomiska samarbetsområdet (EES). En sekretessbrytande bestämmelse som gäller i förhållande till vissa myndigheter finns i 2 kap. 13 §.

Behandling av känsliga personuppgifter

Känsliga personuppgifter, dvs. uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv, ska enligt 2 kap. 10 § TBL inte få behandlas enbart på grund av vad som är känt om en persons sådana förhållanden. Om uppgifter om en person behandlas på annan grund ska de dock få kompletteras med känsliga personuppgifter när det är absolut nödvändigt för syftet med behandlingen.

6.4.3 Lagen om internationellt polisiärt samarbete

Lagen (2000:343) om internationellt polisiärt samarbete tillämpas på polisiärt samarbete mellan Sverige och andra medlemsstater i EU och mellan Sverige och Island, Norge, Schweiz och Liechtenstein i den utsträckning som följer av internationella överenskommelser. Enligt 1 a § gäller polisdatalagen för polisens behandling av personuppgifter vid sådant internationellt polisiärt samarbete som regleras i lagen, om den inte innehåller särskilda regler.

Lagen innehåller bestämmelser om informationsutbyte enligt Prüm-rådsbeslutet¹, CBE-direktivet² och VIS-rådsbeslutet³. Lagen innehåller också vissa bestämmelser rörande Schengensamarbetet.

Den nuvarande lagen om internationellt polisiärt samarbete kommer att upphävas den 2 juli 2017 och ersättas av en ny lag i samma ämne. Lagen kommer att delas in i kapitel. Det införs också fem kapitel som reglerar olika former av personuppgiftsbehandling vid polisiärt samarbete med andra stater inom och utanför EU. Några ändringar i sak ska dock inte ske när det gäller regleringen av behandling av personuppgifter. (Se prop. 2016/17:139.)

¹ Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet.

² Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott.

³ Rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott.

6.4.4 Lagen om internationellt tullsamarbete

Lagen (2000:1219) om internationellt tullsamarbete tillämpas bl.a. på internationellt tullsamarbete som följer av vissa internationella åtaganden och har till syfte att förhindra, upptäcka, utreda eller beivra överträdelser av tullbestämmelser. I 2 kap. 6–8 §§ finns bestämmelser om utbyte av uppgifter. Enligt 6 § får en behörig svensk myndighet, när det är nödvändigt för genomförande av internationellt tullsamarbete på eget initiativ eller på ansökan lämna ut uppgifter till behörig utländsk myndighet eller mellanfolklig organisation, även om uppgiften är sekretessbelagd enligt offentlighets- och sekretesslagen (2009:400).

6.4.5 2013 års lag

Lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag) genomför dataskyddsrambeslutet. Kompletterande bestämmelser finns i förordningen (2013:343) med i övrigt samma namn. Lagen gäller för behandling av personuppgifter i verksamhet som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder, om uppgifterna inom ramen för polissamarbete eller straffrättsligt samarbete görs eller har gjorts tillgängliga eller överförs eller har överförts mellan en svensk myndighet och en medlemsstat i EU eller mellan en svensk myndighet och Island, Norge, Schweiz eller Liechtenstein eller mellan en svensk myndighet och ett EU-organ eller EU-informationssystem. Lagen är tillämplig endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

Från lagens tillämpningsområde undantas i 4 § dels behandling av personuppgifter som rör nationell säkerhet, dels personuppgifter som görs eller har gjorts tillgängliga eller överförs eller har överförts genom visst informationsutbyte som specificeras i bestämmelsen.

Personuppgifter som en svensk myndighet har erhållit får enligt 5 § endast behandlas för andra ändamål än det som uppgifterna först överfördes eller gjordes tillgängliga för, om syftet med behandlingen är att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda

eller beivra brott, verkställa straffrättsliga påföljder eller att vidta rättsliga eller administrativa åtgärder med direkt anknytning till något av dessa ändamål eller att avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får även behandlas för andra ändamål om den som överfört eller gjort uppgifterna tillgängliga har lämnat sitt medgivande eller den som uppgifterna avser har samtyckt till det.

Särskilda begränsningar gäller för överföring av personuppgifter som en svensk myndighet har erhållit enligt 6 § för överföring till enskilda och enligt 7 § för överföring till tredjeland eller internationella organ.

Lagen reglerar också villkor för användningen av personuppgifter.

Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) har föreslagit att lagen upphävs i samband med genomförandet av det nya dataskyddsdirektivet.

6.5 EU:s dataskyddsreform

6.5.1 Bakgrund till reformen

I januari 2012 presenterade kommissionen ett förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Paketet omfattade en förordning med en generell reglering som skulle ersätta det nu gällande dataskyddsdirektivet samt ett nytt direktiv med särregler för främst den brottsbekämpande sektorn som skulle ersätta dataskyddsrambeslutet men ha ett bredare tillämpningsområde.

Det huvudsakliga syftet med kommissionens förslag var att ytterligare harmonisera och effektivisera skyddet av personuppgifter inom EU för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter.

Efter flera års förhandlingar enades Europaparlamentet och rådet den 27 april 2016 om en ny reglering av skyddet för enskilda vid behandling av personuppgifter. Den består av två rättsliga instrument, en förordning och ett direktiv. Regleringen antogs tillsammans med PNR-direktivet och var en förutsättning för att Europaparlamentet skulle rösta genom det förslaget.

6.5.2 En dataskyddsförordning

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordningen) börjar tillämpas den 25 maj 2018.

Förordningen utgör en ny generell reglering för behandling av personuppgifter inom EU och kommer att ersätta dataskyddsdirektivet från år 1995. Förordningen, som är direkt tillämplig, kommer att utgöra ett ramregelverk för skyddet av personuppgifter inom EU. Den kommer därigenom att gälla t.ex. för lufttrafikföretags behandling av PNR-uppgifter. När förordningen träder i kraft måste personuppgiftslagen upphävas, i vart fall i den omfattning som den annars skulle innehålla en dubbelreglering i förhållande till förordningen. Andra författningar som omfattas av den nya förordningens tillämpningsområde måste upphävas i de delar förordningen innehåller motsvarande föreskrifter och i övrigt anpassas till den.

Förordningen reglerar bl.a. grundläggande principer för behandling av personuppgifter, den registrerades rättigheter, personuppgiftsansvar, tillsyn över personuppgiftsbehandling och rätten för enskilda att få tillgång till rättsmedel och sanktioner mot ansvariga som inte lever upp till förordningens krav.

Från förordningens tillämpningsområde undantas bl.a. personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straff, inkluderande skydd mot samt förebyggande av hot mot den allmänna säkerheten. Personuppgiftsbehandling för dessa syften faller i stället under det nya dataskyddsdirektivets tillämpningsområde.

Dataskyddsutredningen har haft i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till. Utredningen har avgett betänkandet Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39). I betänkandet föreslås att kompletterande bestämmelser till dataskyddsförordningen av generell karaktär ska samlas i en ny lag, dataskyddslagen.

6.5.3 Ett nytt dataskyddsdirektiv

Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och om det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (det nya dataskyddsdirektivet) ska vara genomfört i nationell rätt senast den 6 maj 2018.

Direktivet ska dels skydda fysiska personers grundläggande friheter och rättigheter, särskilt deras rätt till skydd av personuppgifter, dels underlätta det informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätt eller nationell rätt. Direktivet ersätter dataskyddsrambeslutet.

I förhållande till nuvarande svensk reglering innehåller det nya dataskyddsdirektivet en delvis ny eller mer detaljerad reglering om rättigheter för enskilda och om skyldigheter för personuppgiftsansvariga eller biträden när det gäller bl.a. datasäkerhet, dokumentation och loggning, konsekvensanalyser och förhandssamråd med tillsynsmyndighet och regler om underrättelser vid s.k. personuppgiftsincidenter.

Direktivet innehåller också regler som anpassats för rättsaktens tillämpningsområde om överföring av personuppgifter till tredjeland och internationella organisationer. Även när det gäller uppgifter och befogenheter för en tillsynsmyndighet innehåller direktivet särskilt anpassade bestämmelser.

Enligt direktivet har enskilda vissa rättigheter, bl.a. att få vända sig till en tillsynsmyndighet med klagomål, att få tillgång till rättsmedel både mot tillsynsmyndighetens beslut och mot åtgärder av en personuppgiftsansvarig eller biträde samt att få ersättning av ansvariga som inte lever upp till direktivets krav. Direktivet förpliktar även medlemsstater att föreskriva regler om påföljder eller sanktioner vid överträdelser av bestämmelser som genomför direktivet.

Utredningen om 2016 års dataskyddsdirektiv har haft i uppdrag att föreslå hur det nya dataskyddsdirektivet ska genomföras i svensk rätt. Utredningen har i delbetänkandet Brottsdatalagen (SOU 2017:29) föreslagit att direktivet i huvudsak genomförs genom en ny ramlag, brottsdatalagen. Syftet med den föreslagna lagen är både att skydda fysiska personers grundläggande fri- och rättigheter och att säker-

ställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt. Enligt förslaget ska lagen – i likhet med personuppgiftslagen – vara generellt tillämplig inom det område som direktivet reglerar. Lagen ska även vara subsidiär. Den föreslagna lagen ska tillämpas av myndigheter som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder vid behandling av personuppgifter. Lagen ska också gälla för personuppgiftsbehandling vid upprätthållande av allmän ordning och säkerhet. De som har sådana arbetsuppgifter betecknas behöriga myndigheter. Lagen ska även tillämpas av andra aktörer som har fått i uppgift att utöva myndighet för något av de nämnda syftena. De behöriga myndigheternas behandling av personuppgifter kommer dock bara att styras av lagen när de behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Dataskyddsförordningen kommer att bli tillämplig i övrigt, t.ex. när Polismyndigheten behandlar personuppgifter i tillståndsärenden eller när en allmän domstol handlägger ett tvistemål. Det som blir avgörande för om lagen är tillämplig är dels om det är en behörig myndighet som behandlar personuppgifterna, dels syftet med behandlingen.

De närmare bestämmelserna i förslaget till brottsdatalog kommer, i den mån de är av intresse för vår utredning, att behandlas i kommande avsnitt.

De myndigheter som bedriver verksamhet inom den föreslagna lagens tillämpningsområde har i allmänhet särskilda registerförfattningar som reglerar personuppgiftsbehandlingen. Utredningen om 2016 års dataskyddsdirektiv kommer att i slutbetänkandet, som ska redovisas den 30 september 2017, föreslå de anpassningar som krävs i berörda registerförfattningar.

6.5.4 Viss personuppgiftsbehandling faller utanför båda instrumenten

Viss behandling av personuppgifter undantas från både dataskyddsförordningens och dataskyddsdirektivets tillämpningsområden. Det gäller bl.a. personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet. Till

Säkerhetspolisens huvuduppgifter hör att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terrorbrott och att utreda och beivra sådana brott. Säkerhetspolisen ansvarar vidare för personskyddet av den centrala statsledningen. Nu nämnda uppgifter hör till nationell säkerhet.

Utredningen om 2016 års dataskyddsdirektiv har föreslagit att brottsdatalagen inte ska vara tillämplig för Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Inte heller ska lagen vara tillämplig när Polismyndigheten övertagit en uppgift som rör nationell säkerhet från Säkerhetspolisen. Förslaget innebär dock inte att Säkerhetspolisens personuppgiftsbehandling kommer att lämnas oreglerad inom området nationell säkerhet. På samma sätt som Säkerhetspolisen i dag tillämpar polisdatalagen och vissa bestämmelser i personuppgiftslagen i verksamhet som rör nationell säkerhet bör, enligt utredningen, myndigheten i framtiden tillämpa vissa bestämmelser i brottsdatalagen. Vilka bestämmelser det bör vara och hur myndighetens behandling av personuppgifter i övrigt bör regleras kommer utredningen att behandla i slutbetänkandet. (Se SOU 2017:29 s. 175 ff.)

7 Pågående arbeten

7.1 Internationellt arbete

Intresset för att använda sig av PNR-uppgifter i den brottsbekämpande verksamheten är stort över hela världen. Flera länder, t.ex. USA, Australien och Kanada, har redan etablerade PNR-system. Även Storbritannien har ett fungerande system i bruk. Exempelvis Frankrike och Ungern har också legat långt fram i arbetet med att driftsätta egna PNR-system.

Som angetts i avsnitt 3.2 ingick EU i mitten av 2000-talet avtal som reglerar överföringen av PNR-uppgifter från flygbolag till USA, Australien och Kanada. Avtalen har därefter omförhandlats. De nya avtalen med USA och Australien har godkänts av Europaparlamentet och har trätt i kraft. Vad gäller det planerade avtalet med Kanada har Europaparlamentet ännu inte tagit ställning. Parlamentet har begärt ett yttrande från EU-domstolen bl.a. i frågan om avtalet är förenligt med EU-fördraget och EU-stadgan vad gäller fysiska personers rätt till skydd av personuppgifter. Generaladvokaten har lämnat ett förslag till yttrande där det anges att vissa förtydliganden måste göras i avtalet och/eller vissa av bestämmelserna utgå för att avtalet ska vara förenligt med stadgan och inte gå utöver vad som är strängt nödvändigt för att uppnå målsättningen att skydda den allmänna säkerheten. Något yttrande från EU-domstolen har dock ännu inte kommit. Under 2015 antog EU:s ministerråd ett beslut som godkänner att förhandlingar inleds om ett avtal med Mexiko.

Fem länder, Storbritannien, USA, Kanada, Australien och Nya Zeeland, har ett underrättelsesamarbete kallat "The Five Eyes" som även behandlar PNR- och API-frågor. Inom ramen för samarbetet utbyter länderna erfarenheter kring användningen av PNR- och API-uppgifter samt även operativ information.

7.1.1 Arbete inom PNRGOV Working Group

Som framgått i avsnitt 4.2.1 rekommenderas i annex 9 till Chicago-konventionen att de fördragsslutande staterna använder sig av standardformatet PNRGOV för överföringen av PNR-uppgifter. I annexet anges även att de fördragsslutande stater som kräver tillgång till PNR-uppgifter bör anpassa sin behandling av uppgifterna och sina tekniska krav till vissa angivna riktlinjer, bl.a. instruktioner för implementering av standardformatet PNRGOV.

PNRGOV har utarbetats gemensamt av stater, lufttrafikföretag och tjänsteleverantörer. Formatet uppdateras ständigt och instruktionerna för dess implementering finns för närvarande i version 16.1. Arbetet relaterat till PNRGOV utförs av en arbetsgrupp bestående av företrädare för såväl industrin som olika stater och leds av Iata. Arbetsgruppen, med namnet PNRGOV Working Group, håller årligen två möten där standardformatet diskuteras och förslag till förändringar tas fram. Vid mötena deltar Iata, Icao, WCO samt företrädare för olika länder, flygbolag och systemleverantörer.

7.1.2 Arbete inom EU

Samtliga berörda medlemsstater arbetar nu med att genomföra PNR-direktivet i nationell rätt och i den operativa verksamheten. Beroende på befintliga system och den nuvarande användningen av PNR-uppgifter i brottsbekämpningen har medlemsstaterna kommit olika långt i detta arbete.

Enligt artikel 4 i PNR-direktivet ska varje medlemsstat inrätta eller utse en myndighet eller del av en myndighet som ska fungera som medlemsstatens enhet för passagerarinformation. Den engelska benämningen för enheten är Passenger Information Unit (PIU). Enheten ska ansvara för att samla in PNR-uppgifter från lufttrafikföretagen, lagra och behandla dessa uppgifter och överföra uppgifterna eller resultatet av behandlingen av dem till behöriga myndigheter. Enheten ska även ansvara för att utbyta uppgifterna med främst andra medlemsstaters motsvarande enheter och med Europol.

Under tiden PNR-direktivet har förhandlats har kommissionen skapat en möjlighet för medlemsstaterna att ansöka om bidrag för att etablera nationella enheter för passagerarinformation och för att bygga upp nödvändiga rutiner och datastöd. 14 medlemsstater, där-

ibland Sverige, har ansökt och erhållit bidrag från den s.k. ISEC-fonden¹. Sedan PNR-direktivet antogs har kommissionen erbjudit juridisk assistans, expertis och ekonomisk support för att tillse att fungerande enheter för passagerarinformation byggs upp inom medlemsstaterna och kommer att vara på plats när direktivet ska vara genomfört i maj 2018. Ytterligare ekonomiskt stöd finns att ansöka om för perioden 2017–2020. Kommissionen har även anordnat möten där frågor kring implementeringen har diskuterats tillsammans med medlemsstaterna. Hitills har fyra sådana möten hållits under kommissionens ledning.

Enligt artikel 8.3 i PNR-direktivet ska all överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation ske på elektronisk väg med användning av gemensamma protokoll och understödda dataformat. Gemensamma protokoll ska användas så att PNR-uppgifternas säkerhet under överföringen tryggas. Understödda dataformat ska säkerställa att de överförda uppgifterna kan läsas av alla berörda parter. Kommissionen har enligt direktivet getts befogenhet att anta en förteckning över de gemensamma protokoll och understödda dataformat som ska användas (artikel 16.2). Kommissionen har i detta arbete biträtt av en kommitté bestående av företrädare för medlemsstaterna. Arbetet är nu slutfört och ett genomförandebeslut har trätt i kraft.²

Inom EU finns även en operativ arbetsgrupp som har till uppgift att säkerställa ett harmoniserat genomförande av PNR-direktivet i medlemsstaterna. Arbetsgruppen utgör ett forum för de framtida enheterna för passagerarinformation och lämnar stöd under arbetet med att implementera direktivet. Gruppen har till syfte att främja största möjliga samarbete och utbyte av information mellan olika enheter för passagerarinformation. Arbetsgruppen är också tänkt att utgöra en grund för ett framtida nätverk mellan enheterna för passagerarinformation. Alla medlemsstater ansvariga för PNR-projekt deltar i arbetsgruppens arbete, som leds av ordförandeskapet.

Inom kommissionens Generaldirektorat för skatter och tullar (Taxud) pågår ett arbete som syftar till att så många tullmyndig-

¹ Program "Prevention of and Fight against Crime" (ISEC).

² Kommissionens genomförandebeslut (EU) 2017/759 av den 28 april 2017 om gemensamma protokoll och dataformat som ska användas av lufttrafikföretag när PNR-uppgifter överförs till enheterna för passagerarinformation.

heter som möjligt ska bli delaktiga i medlemsstaternas enheter för passagerarinformation.

7.2 Arbete i Sverige

7.2.1 Arbete med att upprätta en nationell enhet för passageraruppgifter

Polismyndigheten har till uppgift att förebygga, upptäcka och utreda de flesta av de brott som omfattas av PNR-direktivet. Enligt våra utredningsdirektiv är en utgångspunkt för utredningens uppdrag att den svenska enheten för passagerarinformation ska placeras vid Polismyndigheten.

Polismyndigheten har tillsammans med Tullverket, som framgått ovan, ansökt och erhållit bidrag från en EU-fond. Fondmedlen har avsett att förbereda och sätta upp en it-plattform som kan hämta in PNR-uppgifter från flygbolag och som kan användas för att bearbeta de inhämtade uppgifterna. I ansökan angavs även att en enhet för passagerarinformation skulle etableras. Projektet har tilldelats 1,08 miljoner euro från fonden. Sverige har därefter fått vissa, begränsade, medel för 2017 och kommer att ansöka om ytterligare medel för 2018 och 2019.

Polismyndigheten, Tullverket och Säkerhetspolisen har genomfört en förstudie gällande införandet av en systematiserad hantering av såväl PNR- som API-uppgifter. Projektet startade i november 2014 och redovisades i en rapport daterad den 14 augusti 2015. Enligt rapporten syftar den till att skapa en gemensam bild för såväl Polismyndigheten, Säkerhetspolisen och Tullverket som för berörda departement kring den verksamhet som ska ansvara för hanteringen av PNR- och API-uppgifter. Rapporten syftar också till att tydliggöra verksamhetsnyttan för den brottsbekämpande och brottsförebyggande verksamheten och utgöra ett beslutsunderlag för att starta utvecklingsprojekt för både verksamheten och dess it-stöd.

I förstudierapporten lämnas vissa förslag på hur den nationella enheten för passagerarinformation bör organiseras. Enheten föreslås vara bemannad dygnet runt och bestå av personal som har sin grundanställning inom Polismyndigheten, Säkerhetspolisen eller Tullverket. Tillgång till passageraruppgifterna ska ske via ett it-stöd som uppfyller ställda säkerhetskrav. Förstudien innehåller även bl.a. uppgifter

om de olika roller och kompetenser som kommer att krävas vid enheten, uppgifter om processer och arbetssätt samt ett tekniskt lösningsförslag.

Det bedrivs för närvarande ett projekt vid Polismyndigheten som har till uppgift att etablera en nationell enhet för passagerarinformation med relevant it-stöd. Projektet omfattar såväl sådana uppgifter om passagerare som omfattas av PNR-direktivet, som sådana som omfattas av det tidigare genomförda API-direktivet. En utgångspunkt för projektet är att enheten för passagerarinformation ska behandla såväl sådana uppgifter som hämtas in enligt de nationella bestämmelser som genomför PNR-direktivet som de som genomför API-direktivet. I det senare fallet är planeringen dock att enheten för passagerarinformation endast ska utgöra en stödfunktion, eftersom berörda myndigheter kommer att ha direktåtkomst till uppgifterna i det registret. När det gäller PNR-uppgifter kommer enheten att ansvara för behandlingen av uppgifterna och direktåtkomst till uppgifterna i PNR-databasen kommer inte att vara tillåten.

Vid Polismyndighetens fortsatta arbete med att inrätta en enhet för passagerarinformation har de i förstudien angivna organisationsförslagen vidhållits.

7.2.2 Arbetet med direktivets tekniska bestämmelser

Inom Polismyndigheten pågår således ett arbete med att införa ett automatiserat och strukturerat system för hantering av PNR-uppgifter. Utgångspunkten är att systemet ska ge de behöriga myndigheterna ett effektivt och användarvänligt verktyg för behandlingen av uppgifterna. Tanken är också att enheten för passagerarinformation ska ge likvärdig service till de behöriga myndigheterna. Internationella riktlinjer angående överföring av PNR-uppgifter följs under arbetet.

Analysystemet för PNR-uppgifter kommer att göra automatiska sökningar mot olika databaser. Exempel på sådana databaser är Sis (Schengens informationssystem) och Interpols STLD (Stolen and lost travel documents). En utgångspunkt är att de sökningar som görs vid en normal gränskontroll ska kunna utföras, dock med de begränsningar som följer av PNR-direktivet och datakvalitet. Vidare

kommer systemet att ge möjlighet att jämföra PNR-uppgifter med på förhand fastställda kriterier, s.k. profilering.

De behöriga myndigheterna kommer att få möjlighet att via särskilda sökmallar i ett gemensamt it-system göra förfrågningar hos enheten för passagerarinformation. Stort arbete kommer att läggas på att göra dessa beställningar så lätthanterliga som möjligt. Vidare kommer systemet att utformas så att det inte tillåter vissa beställningar som är oförenliga med PNR-direktivet. Beställningarna kommer att skickas via systemets ärendehantering till en analytiker vid enheten för passagerarinformation, som kontrollerar beställningen och godkänner att den körs i systemet. Systemet genomför därefter en sökning mot den information som finns lagrad. Vid en träff informerar systemet analytikern som analyserar informationen mer i detalj och överför resultatet till behörig myndighet.

Med tanke på de risker som är förknippade med behandlingen och arten av PNR-uppgifterna är det viktigt att systemet håller en hög säkerhetsnivå. Samråd planeras därför ske med Datainspektionen och Säkerhets- och integritetsskyddsnämnden under arbetet med att utforma it-stödet. Såvitt vi erfarit har sådant samråd ännu inte skett.

VÅRA ÖVERVÄGANDEN OCH FÖRSLAG

8 Utgångspunkter och inledande ställningstaganden

8.1 Allmänt om att genomföra EU-direktiv

Vårt övergripande uppdrag är att föreslå de författningsändringar och andra åtgärder som krävs för att genomföra PNR-direktivet i svensk rätt. Ett direktiv har som syfte att harmonisera medlemsstaternas lagstiftning. När ett direktiv genomförs nationellt ska varje medlemsstat besluta de lagar och andra författningar som garanterar att direktivet tillämpas fullt ut på ett tillräckligt klart och precist sätt. Hur själva genomförandet av direktivet i en medlemsstats rättsordning närmare ska gå till överlämnas alltså åt varje stat att själv avgöra. En medlemsstat är följaktligen inte bunden av ett direktivs terminologi eller systematik, om det avsedda resultatet kan uppnås på något annat sätt. EU-direktiv ska således införlivas i nationell rätt genom den lagstiftningsteknik som är ändamålsenlig. Det finns inte heller något absolut krav på att direktiv ska föranleda ny författningsreglering. I den mån befintlig lagstiftning redan uppnår direktivets krav, behövs i princip inte några författningsändringar. Enskilda ska dock ha möjlighet att identifiera sina rättigheter enligt direktivet och kunna göra dessa rättigheter gällande vid domstol (se EU-domstolens domar i t.ex. mål C-131/88, kommissionen mot Tyskland, REG 1991 I-825, och i mål C-361/88, kommissionen mot Tyskland, REG 1991 I-2567).

Det avgörande är således att det i nationell rätt läggs fast en rättslig ram som garanterar att direktivet tillämpas fullt ut på ett tillräckligt klart och precist sätt och som gör det möjligt för enskilda individer att på ett tydligt sätt urskilja vilka rättigheter och skyldigheter de har enligt unionsrätten.

8.2 En samlad ny lag

Vårt förslag: PNR-direktivet ska i huvudsak genomföras genom införandet av en ny samlad lag.

PNR-direktivet innehåller flera nyheter i jämförelse med gällande svensk lagstiftning. Genom direktivet åläggs lufttrafikföretag att överföra PNR-uppgifter inför samtliga flygningar ankommande från eller avgående till ett land utanför EU. Enligt gällande svensk lagstiftning är dessa företag endast skyldiga att *på begäran* lämna över vissa uppgifter om sina passagerare till den efterfrågande myndigheten. Dagens uppgiftsskyldighet omfattar dock färre uppgifter än vad som enligt direktivet framöver ska överföras. PNR-direktivet innehåller vidare för svensk rätt nya företeelser som en databas för PNR-uppgifter och en enhet för passagerarinformation som ska bearbeta uppgifterna. Lagring, analys och utbyte av PNR-uppgifter på det sätt som föreskrivs i direktivet förekommer inte i dag i Sverige.

PNR-direktivet innebär alltså inte, för Sveriges vidkommande, att en redan befintlig verksamhet och reglering ska anpassas till en inom EU utformad harmoniserad reglering för medlemsstaternas pågående verksamheter, så som annars ganska ofta är fallet vid genomförande av direktiv. Genom PNR-direktivet införs i stället en på det hela taget ny verksamhet; ett system för behandling av PNR-uppgifter i en kvantitativ och kvalitativ omfattning som kan sägas innebära ett nytt brottsbekämpningsverktyg i Sverige. Det anförda innebär att en rad helt nya bestämmelser behöver införas för att Sverige ska uppfylla sina skyldigheter enligt direktivet. Frågan är hur regleringen lämpligen bör struktureras rent lagtekniskt.

PNR-direktivet innehåller dels verksamhetsreglering, dels dataskyddsreglering. Till verksamhetsregleringen hör sådana bestämmelser vilka medlemsstaterna måste omvandla till nationell författningsreglering med handlingsdirektiv som anger vad som *ska* göras med PNR-uppgifterna; att de ska sändas från lufttrafikföretagen till nationella enheter för passagerarinformation, att de ska lagras av enheterna viss period och vidareändas i vissa fall till behöriga mottagare m.m. Till dataskyddsregleringen hör sådana bestämmelser som sätter gränser för vad behöriga myndigheter *får* göra med uppgifterna eller som anger vissa rättigheter för enskilda registrerade m.m., dvs. bestämmelser som syftar till att ge skydd för personuppgifter vid den

personuppgiftsbehandling som systemet med användning av PNR-uppgifter inom brottsbekämpningen för med sig. Bestämmelsernas utformning är dock ibland sådan att de olika karaktärerna av reglering är sammanvävda och svåra att särskilja. Direktivet är vidare omfattande och komplext, bl.a. i det att det berör helt olika slags aktörer; såsom kommersiellt verksamma flygbolag och brottsbekämpande myndigheter.

Rent lagtekniskt finns det olika tänkbara sätt att helt eller delvis inarbeta PNR-direktivet i redan gällande lagstiftning. En möjlighet vore således att inarbeta verksamhetsregleringen i t.ex. polislagen (1984:387) och den nya lag om internationellt polisiärt samarbete som ska träda i kraft den 2 juli 2017 (se avsnitt 6.4.3). Dataskyddsregleringen skulle kunna tas in i polisdatalagen och andra registerförfattningar som gäller för myndigheter som kommer att få motta PNR-uppgifter. Regleringen av lufttrafikföretagens skyldigheter skulle vidare kunna tas in i luftfartslagen (2010:500) eller lagen (2010:510) om lufttransporter.

Vår bedömning är dock att en sådan uppsplittrad lagteknisk lösning skulle vara komplicerad, oöverskådlig och kräva korshänvisningar som skulle göra tillämpningen besvärlig. Övervägande skäl talar i stället, enligt vår mening, för att direktivet i huvudsak bör införas i svensk rätt genom en samlad ny lag. Genom en sådan lösning kommer en överskådlig reglering av området för PNR-uppgifter att tillskapas. Dessutom framstår en samlad ny reglering för stunden som den mest praktiska lagtekniska lösningen med tanke på den pågående dataskyddsreformen och därav följande oklarhet om utformningen av den kommande regleringen på området.

8.3 Normgivningsnivå

Vårt förslag: Till den nya lagen ska det införas en anslutande förordning. Centrala bestämmelser i direktivet ska finnas i lagen. Bestämmelser i frågor av mindre vikt för enskilda intressen och närmare bestämmelser rörande hanteringen av PNR-uppgifter m.m. ska tas in i förordningen.

Införandet av PNR-direktivet medför att uppgifter som ett lufttrafikföretag innehar om sina passagerare på flygningar till eller från EU ska överföras till enheten för passagerarinformation i det land dit flygningen kommer att ankomma eller i det land varifrån flygningen kommer att avgå. Enligt den överenskommelse som medlemsstaterna har ingått, och som ska börja gälla senast när direktivet ska vara genomfört i nationell rätt, ska direktivet även tillämpas på flygningar inom EU. Med hänsyn till den stora mängden flygresor som genomförs varje år är det fråga om ett mycket stort antal PNR-uppgifter som ska överföras. Under 2015 uppgick antalet ankommande och avresande utrikespassagerare endast på de svenska flygplatserna till 27 miljoner, varav 20,3 miljoner reste till eller från andra EU-länder. Antalet flygpassagerare ökar ständigt och 2016 var antalet utrikespassagerare på de svenska flygplatserna 28,6 miljoner, varav 22 miljoner reste till eller från andra EU-länder.¹

PNR-uppgifterna ska enligt direktivet lagras vid en nationell enhet för passagerarinformation, analyseras och gallras efter viss tid. Det kan förmodas att endast en mycket liten andel av uppgifterna kommer att bedömas ha samband med sådan brottslighet som faller under direktivet och därför kommer att överföras till behöriga myndigheter eller till andra länders enheter för passagerarinformation eller Europol. Det stora flertalet uppgifter som kommer att lagras vid enheterna avser alltså resenärer som inte på något sätt är inblandade i någon brottslighet.

Enligt 2 kap. 6 § RF är enskilda skyddade gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär kartläggning eller övervakning av personliga förhållanden. Inskränkningar i detta skydd kan enbart ske i lag och bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle (2 kap. 20 och 21 §§ RF). Det har i flera lagstiftningsärenden som rört myndigheters personuppgiftsbehandling framhållits att målsättningen bör vara att myndighetsregister med ett stort antal registrerade och särskilt känsligt innehåll ska regleras särskilt i lag (se t.ex. bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 43).

¹ Enligt Transportstyrelsens statistikuppgifter. Observera dock att alla resande inom EU inte nödvändigtvis har ett EU-land som slutdestination. Statistiken avser första destinationsland efter avgång. Den som t.ex. flyger från Linköping till New York via Köpenhamn räknas i statistiken som resande inom EU.

Det kan diskuteras hur pass integritetskänsliga PNR-uppgifterna kan anses vara sedda var för sig. Emellertid möjliggör systemet, potentiellt sett, en ökad kartläggning av individers flygresor till och från Sverige. Uppgifterna, som från början samlats in av enskilda aktörer för kommersiella syften, görs tillgängliga för användning i viss slags brottsbekämpning trots att det stora flertalet passagerare saknar anknytning till brottslighet. Dessa förhållanden medför enligt vår uppfattning att direktivet huvudsakligen bör införas i svensk rätt genom lag. Vidare innebär direktivet att det måste införas åligganden för enskilda, nämligen lufttrafikföretagen, vilket kräver lagform, se 8 kap. 2 § RF. I den mån det inte finns några normgivningsmässiga eller annars principiella hinder kan dock förordningsform vara att föredra för vissa bestämmelser av för enskilda intressen mindre ingripande karaktär. I och med den relativt detaljerade reglering som ska genomföras enligt direktivet framstår det vidare som en ändamålsenlig ambition att vissa, mer tekniskt inriktade bestämmelser, tas in i en ny, till den nya lagen hörande förordning.

De delar av direktivet som bör införas i svensk rätt genom lag avser bl.a. de grundläggande bestämmelserna om lufttrafikföretagens skyldigheter, tillåten behandling och vidaresändande av PNR-uppgifter. Regleringen av närmare frågor om hanteringen av PNR-uppgifterna m.m., kan dock föras in på förordningsnivå.

8.4 En grundläggande allmän utgångspunkt

Vår utgångspunkt: Utformningen av våra förslag ska ske med beaktande av att det nya systemet för insamling och utbyte av PNR-uppgifter för brottsbekämpande syften är integritetskänsligt. En återhållsam hållning ska därför intas vid utformningen av våra förslag.

Som vi redan framhållit ovan innebär PNR-direktivet att det införs ett i princip nytt verktyg i brottsbekämpningen. Stora nationella databaser över resenärers flygresor kommer att byggas upp i medlemsstaterna. Även om systemet är uppbyggt så att så få uppgifter som möjligt om oskyldiga, vanliga passagerare ska nå ut till den brottsbekämpande verksamheten i Sverige eller utomlands, innebär PNR-systemet en potentiellt sett ökad kartläggning av personers inter-

nationella flygresande. Härigenom företer systemet i viss mån likheter med skyldigheten för teleoperatörerna att utföra en generell datalagring för brottsbekämpande syften, vilket har underkänts av EU-domstolen.² Det rör sig således om en känslig verksamhet när det gäller skyddet för enskildas personliga integritet. Som framgått av avsnitt 7.2 sker vårt arbete med att föreslå direktivets rättsliga genomförande parallellt med arbetet att bygga upp ett organisatoriskt och tekniskt system som lever upp till direktivets krav.

Verksamhetens känsliga karaktär talar, tillsammans med bristande erfarenhet av hur man ska arbeta med PNR-uppgifterna, starkt för att ett återhållsamt förhållningssätt krävs när direktivet nu genomförs. Vår utgångspunkt är därför att våra förslag ska hålla sig nära lydelsen av direktivets bestämmelser samt att, i den mån direktivets bestämmelser öppnar för tolkningar, den tolkning ska väljas som är minst inriparande ur integritetssynpunkt.

Av bl.a. detta skäl vore det lämpligt med en utvärdering och en rättslig översyn efter det att PNR-systemet varit i drift en tid. En sådan utvärdering och översyn torde mycket väl kunna leda till att det identifieras behov av författningsändringar i olika avseenden. Detta kommer vi att beröra i senare avsnitt.

8.5 Den nya lagstiftningens förhållande till relevant dataskyddsreglering

Våra bedömningar: Eftersom PNR-direktivet ska införlivas samtidigt som EU:s dataskyddsreform genomförs, bör våra författningsförslag lämpligen – och så långt möjligt i nuläget – anpassas till den reformen och det förslag om en ny ramlag som lämnats för att genomföra det nya dataskyddsdirektivet.

Övervägande skäl talar för att i lagen inte närmare reglera dess förhållande till mer generell dataskyddsreglering på området. Bestämmelserna i lagen kommer dock att i olika avseenden gälla utöver eller i stället för de generella bestämmelserna i dataskydds-förordningen, den nya ramlag som genomför det nya dataskydds-

² Dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15, Tele2 Sverige och Watson m.fl.

direktivet och annan särreglering för dataskydd som gäller eller kommer att gälla för berörda myndigheter.

Vårt förslag: Det tas i de behöriga myndigheternas allmänna registerförfattningar in bestämmelser om att det i den av oss föreslagna lagen och i föreskrifter som meddelats med stöd av den lagen finns bestämmelser om personuppgiftsbehandling som ska tillämpas i stället för bestämmelserna i aktuell registerförfattning.

Den nya lagen kommer att innehålla bestämmelser som berör flera olika aktörer; främst lufttrafikföretag och olika myndigheter med uppgifter inom det slags brottsbekämpning som avses i PNR-direktivet. Verksamheterna hos dessa aktörer är redan föremål för mer eller mindre ingående författningsreglering. Detta gäller även den personuppgiftsbehandling som sker i verksamheterna. Några grundläggande relationer till annan lagstiftning måste därför redas ut. Det gäller framför allt förhållandena till de nya generella regleringarna på dataskyddsområdet, nämligen dataskyddsförordningen och det förslag till ramlag som genomför det nya dataskyddsdirektivet. Även några andra regleringar kommer att beröras nedan.

EU:s dataskyddsreform

EU:s nya dataskyddsförordning antogs den 27 april 2016. Förordningen, som ska börja tillämpas den 25 maj 2018, utgör en ny generell reglering för personuppgiftsbehandling och kommer att ersätta dataskyddsdirektivet från år 1995. Samtidigt antogs ett nytt dataskyddsdirektiv som ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. I detta ingår även att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Personuppgiftsbehandling som ligger inom direktivets tillämpningsområde är undantagen från dataskyddsförordningens tillämpningsområde. Det nya dataskyddsdirektivet ska vara genomfört i nationell rätt senast den 6 maj 2018. Se en något mera utförlig beskrivning av reformen i avsnitt 6.5.

Förslag till anpassning och genomförandet i Sverige

Två olika utredningar har analyserat den nya förordningen och det nya direktivet.

Dataskyddsutredningen har i betänkandet *Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)* bl.a. lämnat förslag till en ny lag, dataskyddslagen, med kompletterande bestämmelser till dataskyddsförordningen. Till lagen har även föreslagits en anslutande förordning. Enligt förslaget till kompletterande lag ska dataskyddsförordningen, i den ursprungliga lydelsen, i tillämpliga delar gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen. Alla bestämmelser i förordningen gäller dock inte, t.ex. inte de som reglerar skyldigheter för medlemsstaters nationella tillsynsmyndigheter att samarbeta med den svenska tillsynsmyndigheten eller den europeiska tillsynsmyndighetens befogenheter (a. SOU s. 354).

Den till dataskyddsförordningen kompletterande lagen föreslås vara subsidiär till annan lagstiftning (1 kap. 3 §). Avvikande bestämmelser i annan lag eller förordning gäller alltså i stället för lagen.

Utredningen om 2016 års dataskyddsdirektiv har i delbetänkandet *Brottsdatalag (SOU 2017:29)* lämnat förslag till en ny ramlagstiftning med bestämmelser om skydd av personuppgifter inom direktivets tillämpningsområde. I delbetänkandet föreslås en ny ramlag, brottsdatalagen, som ska vara generellt tillämplig vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Ramlagen föreslås också gälla vid behöriga myndigheters personuppgiftsbehandling som utförs i syfte att upprätthålla allmän ordning och säkerhet (1 kap. 2 § förslaget till brottsdatalag). Med behörig myndighet avses en myndighet som har till uppgift att utföra sådan brottsbekämpning m.m. som nyss sagts (1 kap. 6 §). Genom en särskild bestämmelse föreslås dock att Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet inte ska omfattas av lagens tillämpningsområde (1 kap. 4 §). Detsamma ska gälla om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Enligt vad utredningen anger i delbetänkandet som sin uppskatt-

ning ligger Säkerhetspolisens verksamhet i allt väsentligt utanför det nya dataskyddsdirektivets tillämpningsområde, bl.a. dess verksamhet för att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terrorbrott samt att utreda och beivra sådana brott (a. SOU s. 175).

I förslaget föreslås att ramlagen ska vara subsidiär till annan lagstiftning. I 1 kap. 5 § föreskrivs således att om det i en annan lag eller en förordning finns bestämmelser som avviker från ramlagen, ska de bestämmelserna gälla. Om det i en viss myndighets registerförfattning, t.ex. polisdatalagen, finns avvikande bestämmelser gäller alltså de i stället för ramlagen.

I det återstående uppdraget för Utredningen om 2016 års dataskyddsdirektiv innefattas bl.a. att lämna de förslag till författningsändringar som krävs för att anpassa vissa centrala författningar om rättsväsendets behandling av personuppgifter till de nya förutsättningarna. De centrala författningarna avser bl.a. polisdatalagen och lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet³. Vidare ska utredningen överväga om det finns anledning att reglera Säkerhetspolisens personuppgiftsbehandling separat från den lagstiftning som gäller för Polismyndigheten och vid behov lämna författningsförslag. Uppdraget ska slutredovisas senast den 30 september 2017.

Olika regleringsmodeller för registerförfattningar

I nuvarande dataskyddsreglering finns, såsom beskrivits i avsnitt 6.3, personuppgiftslagen varigenom 1995 års dataskyddsdirektiv genomförts. Personuppgiftslagen är generellt tillämplig och gäller även för personuppgiftsbehandling vid brottsbekämpande verksamhet trots att det bakomliggande dataskyddsdirektivet undantar sådan verksamhet från dess tillämpningsområde. Personuppgiftslagen är dock subsidiär till avvikande reglering i annan lag eller förordning (2 § PUL). Inom främst myndighetsområdet finns en mycket stor mängd särregleringar i förhållande till personuppgiftslagen som innehåller just från personuppgiftslagen avvikande regleringar. Det kan handla om författningar som reglerar viss registerföring eller författningar som

³ Ersätts av tullbrottsdatalagen (2017:000) den 1 juli 2017.

mer övergripande reglerar dataskyddsfrågor vid personuppgiftsbehandling vid en viss myndighet eller viss verksamhet. Det gemensamma begreppet för sådan särreglering är registerförfattning.

I dagens registerförfattningar förekommer vanligen bestämmelser som på ett eller annat sätt klargör lagens förhållande till personuppgiftslagen. Olika regleringsmodeller har kommit till användning, huvudsakligen enligt antingen den kompletterande modellen eller den hänvisande modellen men det finns även en heltäckande variant.

De flesta registerförfattningar är i dag utformade i enlighet med den kompletterande modellen. Den tekniken kännetecknas av att särregleringen endast kompletterar eller ersätter huvudregleringen, dvs. personuppgiftslagen, i frågor som är specifika för de verksamheter som omfattas av särlagstiftningen. Den myndighet som berörs måste därmed tillämpa såväl den särskilda registerförfattningen som personuppgiftslagen vid sin behandling av personuppgifter. Personuppgiftslagen ska tillämpas om inte annat följer av registerförfattningen eller av föreskrifter som meddelats med stöd av registerförfattningen. Detta gäller oavsett om registerförfattningen i fråga innehåller eller inte innehåller någon bestämmelse som anger vilket förhållande som gäller mellan författningen och personuppgiftslagen. Frågan om en viss bestämmelse innefattar en avvikelse från vad som ska gälla enligt personuppgiftslagen får göras med tillämpning av sedvanliga metoder för tolkning av författningar (se prop. 1997/98:44 s. 115 f.). Trots att det i teknisk mening alltså inte måste regleras att registerförfattningen och personuppgiftslagen kompletterar varandra på detta sätt, innehåller registerförfattningar ofta bestämmelser som ger uttryck för förhållandet till personuppgiftslagen, dvs. det anges på ett eller annat sätt att personuppgiftslagen gäller utöver registerförfattningen. Ofta anges detta i en paragraf under en särskild rubrik, exempelvis Förhållandet till personuppgiftslagen.

Vid användning av den hänvisande modellen anges i registerförfattningen att den gäller i stället för personuppgiftslagen, om inte annat anges i bestämmelser i registerförfattningen som hänvisar till särskilt utpekade bestämmelser i personuppgiftslagen som ska vara tillämpliga även vid behandling av personuppgifter enligt registerförfattningen i fråga. Även vid den hänvisande modellen måste alltså myndigheten tillämpa såväl den särskilda registerförfattningen som personuppgiftslagen vid sin behandling av personuppgifter. Däremot behöver man inte jämföra bestämmelserna i de båda författningarna

för att komma fram till vad som gäller. Den hänvisande modellen används i flertalet registerförfattningar som gäller för behandling av personuppgifter inom den brottsbekämpande sektorn, exempelvis polisdatalagen och den nya tullbrottsdatalagen som träder i kraft den 1 juli 2017.

För de registerförfattningar som är konstruerade enligt den heltäckande modellen är personuppgiftslagen över huvud taget inte tillämplig beträffande den behandling av personuppgifter som regleras genom författningen. De bestämmelser i personuppgiftslagen som trots detta ska tillämpas i den aktuella verksamheten upprepas i stället i registerförfattningen, vilket i praktiken innebär ett slags dubbelreglering. Fördelen är att tillämparen inte behöver läsa in två olika lagar – registerförfattningen respektive personuppgiftslagen – för att konstatera vilka bestämmelser som reglerar den aktuella personuppgiftsbehandlingen. Registerförfattningen är således heltäckande på så sätt att den helt ersätter personuppgiftslagen. Den heltäckande modellen är ovanlig men används t.ex. i kameraövervakningslagen (2013:460).

Våra bedömningar och förslag

Vårt förslag till lagstiftning för genomförande av PNR-direktivet innehåller bestämmelser som direkt eller indirekt gäller personuppgiftsbehandling hos så pass skilda aktörer som kommersiella lufttrafikföretag och myndigheter som ska använda PNR-uppgifter. Beträffande de sistnämnda har regeringen den 4 maj 2017 utsett Polismyndigheten, Säkerhetspolisen, Tullverket, Ekobrottsmyndigheten och Försvarsmakten såsom behöriga myndigheter enligt artikel 7 i direktivet. Möjligen kommer andra myndigheter att efter hand läggas till. Det är därmed inte möjligt att med en enda bestämmelse klargöra relationen till annan dataskyddsreglering. I det följande behandlar vi frågan i vilken utsträckning det behövs.

Redan här vill vi emellertid framhålla att det mot bakgrund av dataskyddsreformen, som ska genomföras ungefär samtidigt med PNR-direktivet, ter sig mest ändamålsenligt att våra förslag anpassas till reformen i stället för till nu gällande personuppgiftslag. Vi återkommer nedan till detta.

Förhållandet till dataskyddsförordningen

Vissa bestämmelser i den nya lag som vi föreslår kommer att ha lufttrafikföretagen som adressat. Dessa bestämmelser handlar i allt väsentligt om skyldigheter för företagen att leverera PNR-uppgifter till en nationell enhet för passagerarinformation som ska finnas hos Polismyndigheten. Dessa är i och för sig inga dataskyddsbestämmelser men dess fullföljande medför av naturliga skäl en personuppgiftsbehandling i och med översändandet till enheten. Lufttrafikföretagen kommer vid sin personuppgiftsbehandling att omfattas av dataskyddsförordningens bestämmelser. Det innebär bl.a. att förpliktelsen att leverera PNR-uppgifter till de olika enheterna för passagerarinformation i EU, däribland den svenska, kommer att utgöra en sådan laglig grund för behandlingen som avses i artikel 6.1 c om nödvändig behandling för att fullgöra en rättslig förpliktelse. Även den av Dataskyddsutredningen föreslagna kompletterande lagen kommer i princip bli tillämplig, i vart fall i den utsträckning som ett utländskt lufttrafikföretag alls träffas av svensk författningsreglering. De flesta bestämmelser i den lagstiftning vi föreslår kommer emellertid inte att rikta sig till lufttrafikföretagen. På grund därav och på grund av karaktären på de bestämmelser som faktiskt riktar sig till lufttrafikföretagen ser vi inte tillräckliga skäl att ta in en bestämmelse i lagen som mer allmänt upplyser om dess förhållande till dataskyddsförordningen. Förordningen kommer att gälla oavsett. I senare avsnitt kommer vi emellertid, i mån av behov, att ytterligare behandla vad som följer av dataskyddsförordningen.

Förhållandet till den föreslagna ramlagen, brottsdatalagen

Vi kommer i vårt arbete att i stor utsträckning förhålla oss till det förslag till ramlag som lämnats av Utredningen om 2016 års dataskyddsdirektiv såsom om den vore genomförd i enlighet med utredningsförslaget. Av framställningstekniska skäl har vi valt att konsekvent kalla förslaget för brottsdatalagen och även använda förkortningen BDL i anslutning till hänvisningar till föreslagna bestämmelser. Det kan förvisso te sig ovanligt att i så stor utsträckning förhålla sig till ett författningsförslag som ännu inte är antaget av riksdagen och inte heller har föreslagits av regeringen eller ens remissbehandlats. Det är dock fråga om en ovanlig situation där våra för-

fattningsförslag, såsom anförts ovan, bör anpassas till genomförandet av det nya dataskyddsdirektivet som ska genomföras ungefärligen vid samma tidpunkt. I sammanhanget kan nämnas att flera artiklar i PNR-direktivet hänvisar till dataskyddsrambeslutet. Dessa hänvisningar ska enligt skäl 27 i direktivet också ses som hänvisningar till den rättsakt som ersätter rambeslutet, dvs. det nya dataskyddsdirektivet (se avsnitt 6.5.3). Eftersom andra förhållningspunkter saknas har vi i vårt arbete och i utformningen av våra författningsförslag utgått från att brottsdatalagen kommer att genomföras på utsatt datum och på det sätt som föreslagits. Vi är dock medvetna om att i den mån det vidare lagstiftningsarbetet med förslagen i delbetänkandet Brottsdatalag leder till förändringar i författningsförslagen, kan det få följdverkningar på det vidare lagstiftningsarbetet med våra förslag.

Vi bedömer att den personuppgiftsbehandling som kommer att ske hos den nationella enheten för passagerarinformation som en följd av PNR-direktivets bestämmelser faller in under den nya brottsdatalagens tillämpningsområde. Enhetens arbete med PNR-uppgifterna kommer att ingå i Polismyndighetens verksamhet i stort med att förebygga, förhindra, upptäcka, utreda eller lagföra brott, om än bara avseende viss slags brottslighet; terroristbrottslighet och grov brottslighet. I och med att enheten ska finnas hos Polismyndigheten, kommer det föreslagna undantaget i brottsdatalagen för Säkerhetspolisen inte att omfatta enhetens behandling av PNR-uppgifter ens när den avser bekämpning av terroristbrottslighet. Det är alltså vår uppfattning att Polismyndigheten i detta avseende inte kan anses ha övertagit en uppgift rörande nationell säkerhet från Säkerhetspolisen när Polismyndigheten, genom den nationella enheten för passagerarinformation, fullgör sina uppgifter enligt den av oss föreslagna lagen.

Det är vidare vår uppfattning att brottsdatalagen, som förslaget nu är utformat, kommer att i och för sig vara tillämplig på behandlingen av PNR-uppgifter hos sådana svenska myndigheter som ska vara behöriga myndigheter enligt PNR-direktivet och som omfattas av den lagens tillämpningsområde i sin brottsbekämpande verksamhet, nämligen i vart fall Polismyndigheten, Tullverket, och Ekobrottsmyndigheten.

Frågan är om brottsdatalagens tillämplighet bör framgå i lagen genom någon bestämmelse på sätt som i dag vanligen sker när det

gäller befintliga registerförfattningars förhållande till personuppgiftslagen.

Som framgått kommer avvikande bestämmelser i annan lag eller förordning att gälla framför brottsdatalagens bestämmelser alldeles oavsett om detta anges i registerförfattningar eller inte. Omvänt gäller vidare att brottsdatalagens bestämmelser kommer att vara tillämpliga även på en registerförfattnings tillämpningsområde, i den utsträckning som den sistnämnda inte innehåller avvikande bestämmelser och givetvis i övrigt faller under brottsdatalagens tillämpningsområde.

Utredningen om 2016 års dataskyddsdirektiv har aviserat att det kommer att lämnas förslag om en delvis ny regleringsmodell för registerförfattningarna på området. Enligt förslaget ska registerförfattningarna anpassas till brottsdatalagen på så sätt att de ska gälla utöver ramlagen och bara innehålla de bestämmelser som innebär undantag eller avvikelser från bestämmelserna i ramlagen (se SOU 2017:29 s. 141). Utredningen kommer dock, i enlighet med direktiven för arbetet, först i slutbetänkandet lämna förslag till de förändringar som behöver göras i myndigheternas registerförfattningar som en följd av brottsdatalagen.

De redovisade modeller som förekommer bland gällande registerförfattningar är alla förenade med både för- och nackdelar. Vår ambition är att anpassa vår lagkonstruktion till hur de centrala författningarna om personuppgiftsbehandling på det brottsbekämpande området kommer att se ut framöver.

Utredningen om 2016 års dataskyddsdirektiv har alltså redan angett att särförfattningarna ska utformas i enlighet med den kompletterande modellen. Hur detta kommer att närmare utformas är dock på nuvarande stadium inte klart, dvs. om det kommer att föras in bestämmelser i respektive registerförfattning som klargör dess förhållande till brottsdatalagen eller inte.

Vi ser inte skäl att föreslå en annan lagteknisk lösning för vår lag, i den utsträckning den riktar sig till myndigheter som är behöriga myndigheter enligt den nya brottsdatalagen. Även den lagstiftning vi föreslår bör alltså vara kompletterande och gälla utöver brottsdatalagen. Frågan är om det behöver anges på annat sätt än genom den bestämmelse i brottsdatalagen som anger att avvikande bestämmelser i lag eller förordning gäller före den lagen.

Brottsdatalagen är utformad för och kommer att, med visst undantag, att gälla generellt för brottsbekämpande verksamhet vid myndigheter som har till uppgift att bedriva sådan verksamhet. Detta kommer att bli väl inarbetat hos dessa myndigheter. Vi ser därför inte att det finns ett behov av att i en allmän bestämmelse i den lag vi föreslår upplysa om förhållandet till brottsdatalagen, vare sig att brottsdatalagen gäller utöver de regler som finns i den föreslagna lagen eller, motsatsvis, att den föreslagna lagens bestämmelser ersätter eller gäller utöver brottsdatalagens bestämmelser. Det sagda menar vi bör gälla för såväl den reglering som avser personuppgiftsbehandling vid enheten för passagerarinformation vid Polismyndigheten som de bestämmelser som berör den behandling som kommer att ske hos behöriga myndigheter när de mottar PNR-uppgifter och som annars omfattas av brottsdatalagens tillämpningsområde. Till detta kommer att Säkerhetspolisen föreslås stå utanför ramlagens tillämpningsområde när den mottagit PNR-uppgifter i sin verksamhet med att bekämpa terroristbrottslighet. Även Försvarsmakten torde stå utanför brottsdatalagens tillämpningsområde i den verksamhet vari det kan bli aktuellt att motta PNR-uppgifter från enheten för passagerarinformation. För Säkerhetspolisens och Försvarsmaktens del skulle därvid behövas någon specialreglering som inte skulle underlätta begripligheten i lagstiftningen.

Sammantaget är det alltså vår bedömning att övervägande skäl talar för att det är mest ändamålsenligt att inte ta in någon bestämmelse i den av oss föreslagna lagen som upplyser om det som redan gäller vare sig det uttrycks särskilt i lagen eller inte. Med detta åsyftas att brottsdatalagen också gäller vid behandlingen av PNR-uppgifter i tillämpliga delar för sådana myndigheter som också annars har att tillämpa brottsdatalagen, dock inte i den utsträckning den av oss föreslagna lagen kommer att innehålla från brottsdatalagen avvikande bestämmelser. I följande avsnitt kommer vi att i mån av behov närmare beröra vilka bestämmelser i brottsdatalagen som kommer att vara tillämpliga och vilka bestämmelser i den av oss föreslagna lagen som gäller i stället för brottsdatalagen. I övrigt blir det dock en rättstillämpningsfråga att bedöma i vad mån en bestämmelse i vår föreslagna lagstiftning innefattar en avvikelse. Den frågan får avgöras med sedvanliga metoder för tolkning av författningar.

Det är möjligt att de lagtekniska lösningarna för registerförfattningars förhållande till brottsdatalagen som Utredningen om

2016 års dataskyddsdirektiv kommer att föreslå blir andra och att det därför, för att uppnå konsekvensens och ändamålsenlighet på området, finns anledning att i det fortsatta arbetet med genomförandet av PNR-direktivet anpassa våra förslag till dessa kommande, mer generella lösningar.

Registerförfattningar

En ytterligare fråga är hur den av oss föreslagna lagstiftningen ska förhålla sig till sådana registerförfattningar som i dag gäller och som framöver kommer att anpassas till brottsdatalagen.

Utgångspunkten för vårt uppdrag är, enligt våra kommittédirektiv, att den nationella enheten för passagerarinformation ska inrättas vid Polismyndigheten. Vi kommer att behandla detta mer ingående i avsnitt 10. Redan här och i linje med det ovan sagda kan sägas att enhetens arbete kommer att omfattas av tillämpningsområdet för polisdatalagen i dess nuvarande lydelse (1 kap. 2 § första stycket 1 PDL). Det är oklart hur polisdatalagens tillämpningsområde kommer att anges i det anpassade förslag som Utredningen om 2016 års dataskyddsdirektiv ska föreslå. Vi har därför att utgå från den utformning som finns i dag.

Många bestämmelser i den lag vi föreslår kommer att avvika från regleringen i polisdatalagen. Det gäller t.ex. bestämmelser om tillåtna ändamål, behandling av känsliga personuppgifter, gallring, åtkomst m.m. Det skulle tala för att den av oss föreslagna lagen helt skulle ersätta polisdatalagen. Samtidigt kommer emellertid enhetens arbete med PNR-uppgifter att innefatta en hel del annan personuppgiftsbehandling än just den som specifikt rör PNR-uppgifter. Exempelvis ska PNR-uppgifter analyseras och jämföras med uppgifter i relevanta databaser. Detta kommer att beskrivas i avsnitt 13.

I den tämligen omfattande bearbetningen och i det analysarbete som ska ske vid enheten bör enligt vår mening polisdatalagen gälla i den utsträckning som den av oss föreslagna lagen inte innehåller avvikande bestämmelser. Vi föreslår därför detta. Rent lagtekniskt bör detta åstadkommas genom en bestämmelse som utformas med 1 kap. 4 § PDL som modell. Det bör alltså föras in en bestämmelse i polisdatalagen, 1 kap. 4 a §, av vilken framgår att det finns avvikande bestämmelser i den av oss föreslagna lagen som ska tillämpas

i stället för bestämmelserna i polisdatalagen när det gäller personuppgiftsbehandling vid enheten för passagerarinformation.

De behöriga myndigheterna kommer också att behandla PNR-uppgifter när de väl mottagit denna information från enheten för passagerarinformation. Även för den behandlingen kommer det i våra författningsförslag finnas vissa begränsningar som går utöver vad som i dag gäller enligt polisdatalagen och motsvarande regleringar för andra behöriga myndigheter som utsetts eller senare kan komma att utses av regeringen till behöriga myndigheter enligt PNR-direktivet. Även för dessa behöriga myndigheter bör gälla att de avvikande bestämmelserna i vår lag ska gälla framför bestämmelserna i registerförfattningar som annars gäller i deras verksamheter.

I och med att Polismyndigheten och Ekobrottsmyndighetens utsetts som behöriga myndigheter kan den av oss nyss föreslagna bestämmelsen i polisdatalagen göras mer generell så att den omfattar all behandling enligt den av oss föreslagna lagen för dessa myndigheter. Enligt vad vi upplysts om är tanken att det endast är inom Ekobrottsmyndighetens polisiära del som det kommer att bli aktuellt att behandla PNR-information. Det bör därför, enligt vår bedömning, inte föreslås en motsvarande bestämmelse i åklagardatalagen (2015:433).

För Tullverkets del bör en motsvarande bestämmelse tas in i den nya tullbrottsdatalagen, Vi föreslår därför det. Bestämmelsen kan tas in som en nytt tredje stycke i 2 kap. 8 § TBL.

Med tanke på den osäkerhet som råder angående den kommande regleringen för Säkerhetspolisen har vi inte sett det som möjligt att lämna något förslag för den myndigheten. I den mån Säkerhetspolisen även framgent ska omfattas av polisdatalagens tillämpningsområde, kommer emellertid den bestämmelse vi ovan föreslagit i polisdatalagen att även omfatta Säkerhetspolisens personuppgiftsbehandling.

Särskilt om Försvarmakten

Som nämnts ovan utsåg regeringen den 4 maj 2017 Polismyndigheten, Säkerhetspolisen, Tullverket, Ekobrottsmyndigheten och Försvarmakten såsom behöriga myndigheter enligt artikel 7 i direk-

tivet. Vi har av tidsskäl inte haft möjlighet att närmare behandla frågor som gäller Försvarmakten.

Såvitt vi erfarit är tanken att PNR-information ska kunna mottas från eller begäras från enheten för passagerarinformation endast i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Inom den verksamheten gäller lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Regleringen av Försvarmaktens behandling av personuppgifter, inklusive den nu nämnda lagen, kan komma att förändras betydligt till följd av förslag från den utredning som nyligen getts i uppdrag att se över regleringen av behandlingen av personuppgifter inom Försvarmakten och Försvarets radioanstalt (dir. 2017:42). Det uppdraget ska dock redovisas först den 31 maj 2018. Det är därför vår uppfattning att en motsvarande bestämmelse som den vi ovan föreslagit för polisdatalagen och tullbrottsdatalagen bör införas i den nämnda lagen för försvarsunderrättelseverksamheten och militära säkerhetstjänsten i avvaktan på en eventuell ändrad reglering på Försvarmaktens område. Vi föreslår därför detta och att en sådan bestämmelse tas in som en ny paragraf, 1 kap. 1 a §, i den lagen.

9 Den nya lagens inledande bestämmelser

9.1 Den nya lagens namn, innehåll och syfte

Våra förslag: Den nya lagen ska heta lagen om flygpassageraruppgifter i brottsbekämpningen. Lagen ska inledas med bestämmelser som i korthet anger lagens innehåll och att lagen innebär ett genomförande av PNR-direktivet.

Syftet med lagen ska vara att dels tillgodose behovet av tillgång till PNR-uppgifter i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra sådan brottslighet som omfattas av PNR-direktivets tillämpningsområde, dels skydda människor mot att deras personliga integritet kränks vid behandling av uppgifter om dem. Syftet ska uttryckligen anges i lagen.

Lagens namn

Som framgått i avsnitt 8.2 kommer den nya lagen som genomför PNR-direktivet att innehålla såväl verksamhets- som dataskyddsreglering. Med tanke härpå bör lagens namn inte ge intrycket att enbart vara av det ena eller andra slaget av reglering. Flygpassagerardatalag eller lag om behandling av flygpassageraruppgifter eller liknande som för tankarna till dataskyddsreglering bör därför inte väljas. Det är vidare allmänt eftersträvanvärt med korta namn på författningar som dock samtidigt ska ge information om författningens innehåll (se t.ex. Ds 2014:1 s. 17). Vi har övervägt att föreslå namnet PNR-lagen. Vi har dock funnit att det skulle vara alltför svårbegripligt för icke insatta och att det därmed vore olämpligt att använda sig av en sådan förkortning i lagens namn.

Den nya lagen är komplex och riktar sig i större eller mindre utsträckning till flera aktörer. För att i någon mån leva upp till kravet på korta lagrubriker anser vi att benämningen *lagen om flygpassageraruppgifter i brottsbekämpningen* är ändamålsenlig då den fångar kärnan i regleringen, nämligen att sådana uppgifter ska bli tillgängliga för användning inom brottsbekämpande verksamhet.

Lagens innehåll

PNR-direktivets artikel 1 har rubriken syfte och tillämpningsområde. Artikel 1 innehåller dock dels en sammanfattande beskrivning av direktivets innehåll, dels ett initialt klargörande av den mest centrala begränsningen av för vilka ändamål insamlade uppgifter får behandlas enligt direktivet. Vad gäller PNR-direktivets innehåll framgår av punkten a i artikel 1.1 att direktivet innehåller bestämmelser om lufttrafikföretagens överföring av PNR-uppgifter om passagerare på flygningar utanför EU. I punkten b framgår att direktivet också innehåller bestämmelser om behandlingen av de uppgifterna. I den behandling av PNR-uppgifter som omfattas av direktivet inbegrips enligt artikeln medlemsstaternas insamling, användning, lagring och inbördes utbyte av dessa uppgifter.

De PNR-uppgifter som samlas in i enlighet med direktivet får enligt artikel 1.2 endast behandlas på det sätt som anges i direktivets artikel 6.2 a, b och c och endast i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. I direktivet används begreppet brott när det är fråga om såväl att förebygga och upptäcka brott som att utreda brott. I svensk lagstiftning brukar man emellertid skilja mellan å ena sidan underrättelseverksamhet som är ett led i arbetet med att förebygga, förhindra och upptäcka brottslig verksamhet och, å andra sidan, utredning och beivrande av konkreta brott. Vid tidigare genomföranden av såväl Prövrådsbeslutets bestämmelser om automatiserat utbyte av fingeravtrycksuppgifter och VIS-rådsbeslutets bestämmelser om brottsbekämpande myndigheters tillgång till information för viseringar har begreppet brott tolkats så att det omfattar både konkreta brott och sådan brottslig verksamhet som är föremål för underrättelsearbete (se prop. 2010/11:129 s. 110 och prop. 2014/15:82 s. 34). Vi ser ingen anledning att göra någon annan tolkning av begreppets

innebörd i PNR-direktivet. Det innebär att PNR-uppgifter enligt direktivet får behandlas både vid underrättelseverksamhet och vid förundersökning. Vidare får uppgifterna användas av åklagare och i domstol vid en lagföring.

Bestämmelsen i artikel 1 utgör en bra sammanfattning av direktivet. En ny lag om PNR-uppgifter skulle därför kunna inledas med liknande bestämmelser. Således föreslås en inledande bestämmelse som anger att lagen innehåller bestämmelser om lufttrafikföretags överföring av PNR-uppgifter till den nationella enheten för passagerarinformation och om behandlingen av PNR-uppgifter. Det bör av bestämmelsen vidare framgå att sådana uppgifter får användas i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Det kan här anmärkas att vi valt att använda ordet *eller* i uttrycken "utreda eller lagföra" samt "terroristbrottslighet eller grov brottslighet" i stället för ordet *och* som används på motsvarande ställen i den svenska översättningen av PNR-direktivet, vilket torde vara en felöversättning. Det är alltså inte nödvändigt att alla de angivna syftena samtidigt är uppfyllda för att uppgifterna ska få behandlas i ett enskilt fall. Inte heller behöver ett syfte med behandlingen vara att både bekämpa terroristbrottslighet och grov brottslighet, utan det är tillräckligt att den ena sortens brottslighet är aktuell. Vi kommer i det följande att föreslå hur terroristbrottslighet och grov brottslighet ska definieras i lagen. Vi återkommer då till vårt val att använda begreppet terroristbrottslighet i stället för direktivets uttryck terroristbrott.

Upplysning om PNR-direktivet

I författningar som genomför direktiv förekommer ibland och ibland inte en upplysning om att författningen i fråga genomför ett EU-direktiv. En sådan bestämmelse har ingen materiell betydelse som sådan utan innebär enbart just en upplysning. Vi ser ett värde i att upplysa om att lagen genomför PNR-direktivet och föreslår därför att det tas in en sådan upplysningsbestämmelse i lagens inledande paragraf. Härigenom uppfylls vidare kravet enligt artikel 18.1 andra stycket i PNR-direktivet om att hänvisning till direktivet ska göras vid den nationella implementeringen.

Lagens syfte

Direktivets syfte får anses framgå av dess ingress. I skäl 5 anges att målen för direktivet bland annat är att trygga säkerheten, skydda personers liv och säkerhet och att inrätta en rättslig ram till skydd för PNR-uppgifter vid behöriga myndigheters behandling av dessa. I skäl 6 anges att en effektiv behandling av PNR-uppgifter, exempelvis genom att jämföra PNR-uppgifter med uppgifter i olika databaser över eftersökta personer och föremål, är nödvändig för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten. En sådan behandling av PNR-uppgifter anges även vara nödvändig för att samla in bevisning och i förekommande fall för att hitta medbrottslingar och avslöja kriminella nätverk. I skäl 7 anges vidare att bedömningen av PNR-uppgifter gör det möjligt att identifiera personer som tidigare inte har varit misstänkta för delaktighet i terroristbrott eller grov brottslighet och som bör undersökas närmare av de behöriga myndigheterna. Genom att använda PNR-uppgifter är det möjligt att möta hotet från terroristbrott och grov brottslighet från en annan utgångspunkt än vid behandling av andra kategorier av personuppgifter.

Enligt skäl 10 är det av största vikt att alla medlemsstater inför bestämmelser om skyldigheter för lufttrafikföretag som tillhandahåller flygförbindelser utanför EU att överföra de PNR-uppgifter, inklusive API-uppgifter, som de samlar in för att det ska gå att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Av skäl 11 framgår vidare att behandlingen av personuppgifter bör stå i proportion till de särskilda säkerhetsmål som direktivet syftar till att uppfylla.

På grund av rättsliga och tekniska skillnader mellan olika nationella bestämmelser om behandling av personuppgifter, däribland PNR-uppgifter, möts lufttrafikföretagen av olika krav på vilken typ av information som ska översändas och vilka villkor som gäller för översändandet av denna information till de behöriga nationella myndigheterna. Dessa skillnader kan vara till skada för ett effektivt samarbete mellan de behöriga nationella myndigheterna för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. I skäl 35 anges därför som ytterligare syfte bakom

direktivet att det är nödvändigt att på unionsnivå inrätta en gemensam rättslig ram för överföring och behandling av PNR-uppgifter.

Det bör i lagens inledande del finnas en bestämmelse som beskriver lagens syfte. En sådan bestämmelse måste dock utformas på ett mycket övergripande och förenklat sätt men ändå fånga regleringens syfte. Detta är tudelat. Lagen syftar dels till att ge behöriga myndigheter tillgång till information för användning i viss brottsbekämpande verksamhet, dels till att värna de enskildas integritet vid insamlingen och den vidare användningen samt utbytet av uppgifter om dem. PNR-direktivets artiklar avspeglar således en avvägning mellan, å ena sidan, viljan att skapa ett harmoniserat och enhetligt system för informationsanvändning och utbyte inom EU för en effektiv bekämpning av allvarlig brottslighet och, å andra sidan, ett tillgodoseende av berörda passagerares grundläggande rättigheter om respekt för privatlivet och skydd för sina personuppgifter. Detta uttrycks, enligt vår mening, lämpligen med en bestämmelse som anger att syftet med lagen är att tillgodose behovet av tillgång till PNR-uppgifter vid sådan verksamhet som nämnts ovan och att skydda människor mot att deras personliga integritet kränks vid behandlingen av uppgifter om dem.

9.2 Definitioner i lagen

Vårt förslag: Vissa uttryck som används i lagen ska definieras. Definitionerna ska ligga så nära PNR-direktivets definitioner som möjligt.

Vi har i tidigare avsnitt angett att dataskyddsförordningen, brottsdatalagen, polisdatalagen och viss annan dataskyddsreglering för behöriga myndigheter kommer att gälla i mer eller mindre stor utsträckning utöver de bestämmelser som vi föreslår i den nya lagen. Därmed kommer en hel rad dataskyddsrättsliga begrepp att också bli tillämpliga vid behandling av personuppgifter enligt vår lag. Exempel på detta är just orden behandling och personuppgifter, men även begreppen personuppgiftsansvarig, personuppgiftsbiträde, dataskyddsombud, registrerad m.m.

I artikel 3 i PNR-direktivet definieras vissa uttryck som är av grundläggande betydelse både för förståelsen av bestämmelserna i

direktivet och för att ringa in dess närmare tillämpningsområde. Vi menar att huvuddelen av dessa definitioner bör tas in i den nya lagen som genomför direktivet och föreslår därför detta. Vi kommer därvid att förhålla oss nära lydelsen i direktivet. Vilka begreppen är kommer att närmare behandlas eller annars framgå i andra avsnitt i detta betänkande.

Ett par definitioner i direktivet kommer det dock att saknas behov av i vårt förslag enligt vår bedömning. Detta gäller till en början begreppen *flygning utanför EU och flygning inom EU*, eftersom det inte kommer att finnas någon särreglering för det ena eller andra slaget av flygningar. Inte heller finns det behov av att definiera begreppet *sändmetoden*. Detta kommer vi att närmare behandla i avsnitt 11.4.7.

Vidare kommer vi att föreslå definitioner av en del ytterligare begrepp än de som anges i artikel 3 i direktivet. Skälet till detta är närmast att förenkla utformningen av de materiella bestämmelserna i lagen. Inte i något avseende kommer dessa extra definitioner att strida mot direktivet. Vilka dessa definitioner är kommer att framgå i senare avsnitt.

Av avgörande betydelse för PNR-direktivets tillämpningsområde och tillåtna ram för användningen av PNR-uppgifter är emellertid begreppen terroristbrott och grov brottslighet. Genom portalparagrafen i artikel 1.2 slås nämligen fast att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra sådan brottslighet. Nedan behandlar vi i separata avsnitt vad som ska förstås med begreppen terroristbrott och grov brottslighet och hur de bör definieras i den nya lagen.

9.3 Terroristbrott

I artikel 3.8 i PNR-direktivet definieras terroristbrott som de brott enligt nationell rätt som avses i artiklarna 1–4 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism (terrorisrambeslutet). Någon kvalifikation angående straffets svårighet anges inte i direktivet.

9.3.1 Bakgrund

Vad som utgör ett terroristbrott definieras i artikel 1 i terrorismrambeslutet. Med ett sådant brott avses i korthet vissa uppsåtliga handlingar som genom sin art eller sitt sammanhang allvarligt kan skada ett land eller en internationell organisation och som begås i syfte att

- injaga allvarlig fruktan hos en befolkning,
- otillbörligen tvinga offentliga organ eller en internationell organisation att utföra eller att avstå från att utföra en handling, eller
- allvarligt destabilisera eller förstöra de grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturerna i ett land eller i en internationell organisation.

Artiklarna 2–4 i rambeslutet innehåller ytterligare brott med anknytning till terroristbrottslighet, däribland brott som begås av en terroristgrupp och brott med anknytning till terroristverksamhet. Det huvudsakliga genomförandet av terrorismrambeslutet har i svensk rätt skett genom införandet av lagen (2003:148) om straff för terroristbrott. Artiklarna 1–4 i rambeslutet motsvaras i svensk rätt av 2, 4 och 5 §§ i denna lag. Artikel 3 och 4 i terrorismrambeslutet har ändrats genom rambeslutet 2008/919/RIF¹. Ändringarna innebar att ytterligare vissa gärningar med anknytning till terroristbrott skulle vara kriminaliserade. Ändringarna har genomförts i svensk rätt genom lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

Den 15 mars 2017 antog Europaparlamentet och rådet ett direktiv om bekämpande av terrorism² (terrorismdirektivet). Direktivet har trätt i kraft. Avsikten med direktivet är att fastställa minimiregler rörande definitionen av straffbara gärningar samt påföljder och sanktioner på området för terroristbrott, brott med anknytning till en terroristgrupp och brott med anknytning till terroristverksamhet.

¹ Rådets rambeslut 2008/919/RIF av den 28 november 2008 om ändring av rambeslut 2002/475/RIF om bekämpande av terrorism.

² Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF.

Avsikten är vidare att fastställa minimiregler om åtgärder för skydd av och hjälp till offer för terrorism. Direktivet innehåller flera nyheter i förhållande till rambeslutet. Bl.a. föreslås terroristbrottet utökas till att även omfatta vissa angrepp mot informationssystem (i svensk rätt t.ex. grovt dataintrång). Kriminaliseringen av terrorismfinansiering utvidgas också. Artiklarna 3–14 i terrorismdirektivet innehåller de olika straffbara gärningarna på terrorismområdet. Terrorismdirektivet ersätter terrorismrambeslutet, dvs. det rambeslut som anges i PNR-direktivet. I terrorismdirektivets artikel 27 anges att hänvisningar till terrorismrambeslutet ska anses som hänvisningar till terrorismdirektivet. Medlemsstaterna ska senast den 8 september 2018 sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet.

Utredningen om genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism (Ju 2014:26) har fått i uppdrag att analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra det nya terrorismdirektivet. Utredningen ska redovisa detta uppdrag senast den 29 september 2017.

Vidare har en särskild utredare fått i uppdrag att genomföra en översyn av den nationella straffrättsliga lagstiftningen för att bekämpa terrorism. Syftet med översynen är att åstadkomma en ändamålsenlig, effektiv och överskådlig reglering som samtidigt är förenlig med ett väl fungerande skydd för grundläggande fri- och rättigheter. Den föreslagna regleringen bör enligt utredningsdirektivet samlas i ett regelverk (dir. 2017:14). Uppdraget ska redovisas senast den 31 januari 2019.

9.3.2 Våra överväganden och förslag

Vårt förslag: I stället för direktivets benämning terroristbrott ska benämningen terroristbrottslighet användas i lagen. Terroristbrottslighet ska i den nya lagen definieras som de brott enligt nationell rätt i Sverige eller andra medlemsstater som avses i artiklarna 1–4 i terrorismrambeslutet.

PNR-direktivets definition av terroristbrott omfattar samtliga brott som har införts i eller ansetts svara mot befintlig nationell rätt enligt 2002 års rambeslut, med de ändringar som har genomförts genom 2008 års beslut. Att i lag eller förordning ange exakt vilka svenska brott som motsvarar direktivets definition skulle kräva en längre uppräknings och omfatta brott i såväl lagen om terroristbrott som lagen om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet. Redan av detta framgår att benämningen terroristbrott som används i direktivet är för snävt för att passa svenska förhållanden. Vi kommer därför att i lagen använda benämningen terroristbrottslighet både i begreppsdefinitionen och i lagens materiella bestämmelser.

Behovet och nyttan av en uppräknings av olika brottsbenämningar som avser terroristbrottslighet kan ifrågasättas, bl.a. med hänsyn till att det främst är enheten för passagerarinformation som ska tillämpa regleringen. Till detta kommer att terrorismdirektivet har trätt i kraft. Detta direktiv, som ersätter terrorismrambeslutet, innehåller flera förändringar avseende aktuell brottslighet. En möjlig uppräknings av svenska brott i vårt författningsförslag skulle därmed bli inaktuell efter genomförandet av terrorismdirektivet.

Det främsta skälet mot en uppräknings av svenska brottsbenämningar är emellertid att även terroristbrottslighet i andra medlemsstaters nationella rätt, vari 2002 års rambeslut genomförts eller det nya terrorismdirektivet kommer att genomföras, är av betydelse för tillämpningen av den nya lag vi föreslår. Så blir fallet vid utlämnande av PNR-uppgifter från Sverige till andra medlemsstater, eftersom det även då är ett villkor att mottagaren ska använda uppgiften bara för sådan terroristbrottslighet som avses i PNR-direktivet (eller grov brottslighet enligt samma direktiv). Det är därför olämpligt att bara ha svensk lagstiftning i åtanke vid utformningen av den nya lagens definition av begreppet terroristbrottslighet.

I redan befintlig näraliggande lagstiftning rörande brottsbekämpande myndigheters åtkomst till informationssystemet för viseringar (VIS) förekommer en lagteknisk lösning som innebär att begreppet terroristbrott definieras genom en direkt hänvisning till definitionen i artikeln i rådets beslut 2008/633/RIF, se 24 § lagen (2000:343) om internationellt polisiärt samarbete och prop. 2014/15:82 s. 34 f. I artikeln i fråga hänvisas vidare till artiklar i 2002 års rambeslut. Vi har övervägt en motsvarande lösning eftersom det finns uppenbara

fördelar med enhetliga lagtekniska lösningar på näraliggande områden. Enligt vår mening skulle det emellertid innebära en enklare och tydligare reglering att i vår lag föra in en direkt hänvisning till de brott enligt nationell rätt som avses i rambeslutet. Med nationell rätt skulle då kunna avses såväl svensk som annat EU-lands rättsordning. Av tydlighetsskäl anser vi dock att det bör uttryckligen anges att det kan vara fråga om såväl svensk som annan medlemsstats nationella rätt. Definitionen skulle i så fall kunna ha följande lydelse: ”terroristbrottslighet – de brott enligt nationell rätt i Sverige eller andra medlemsstater som avses i artiklarna 1–4 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism”. Även om en hänvisning i vår lag till rambeslutet i stället för omvägen via definitionen i artikel 3.8 PNR-direktivet avviker från det definitionssätt som använts i 2000 års lag, anser vi att fördelarna med en direkt hänvisning överväger. Den föreslagna definitionen blir därmed i princip likalydande med PNR-direktivets definition.

Som nyss angetts har terrorismdirektivet förvisso trätt i kraft. Den av oss föreslagna definitionen kan därför troligen behöva ändras i samband med att terrorismdirektivet genomförs i svensk rätt. Det är ännu inte klart hur detta kommer att genomföras i Sverige och vilka analyser som kommer att göras angående förhållandet mellan befintliga och nya definitioner av aktuell brottslighet. Dessa analyser och ställningstaganden bör lämpligen göras av den utredning som genomför terrorismdirektivet.

9.4 Grov brottslighet

Med grov brottslighet avses enligt PNR-direktivet de brott som förtecknas i bilaga II till direktivet och som kan leda till fängelse eller annan frihetsberövande åtgärd i minst tre år enligt en medlemsstats nationella rätt (se rättelse av direktivet, bilaga 3).

Förteckningen över brott i bilaga II omfattar 26 punkter. Uppräkningen innefattar flera brottsbalksbrott (t.ex. mord, grov miss-handel, rån och bedrägeri) liksom brott och gärningstyper i specialstraffrätten (t.ex. narkotikabrott och miljöbrott). En del punkter avser brott som inte har någon direkt svensk motsvarighet, dock kan det indirekt, helt eller delvis, finnas motsvarigheter.

9.4.1 Bakgrund

De brott som anges i bilaga II till PNR-direktivet omfattas alla, förutom brottet industrispionage (punkten 26), av den uppräkningslista som finns i artikel 2.2 i rambeslutet om en europeisk arresteringsorder³. Den aktuella artikeln i rambeslutet omfattar däremot fler brott än de som upptas i bilaga II till PNR-direktivet. I rambeslutets artikel 2.2 anges de där uppräknade brotten utgöra sådana brott som medför att ett överlämnande på grundval av en europeisk arresteringsorder ska ske utan kontroll av om det föreligger dubbelstraffbarhet för gärningen, förutsatt att brotten, som de definieras i den utfärdande medlemsstatens lagstiftning, kan leda till fängelse eller annan frihetsberövande åtgärd i minst tre år i den utfärdande medlemsstaten. Artikeln har införlivats i svensk rätt genom 2 kap. 2 § andra stycket lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder (arresteringsorderlagen). Av bestämmelsen framgår att den brottslighet som avses är de gärningar som finns angivna i en bilaga till lagen och för vilka det är föreskrivet en frihetsberövande påföljd i tre år eller mer.⁴ Om det i arresteringsordern har angetts att en gärning är sådan som anges i den s.k. listan och gärningen enligt den utfärdande medlemsstatens lagstiftning kan leda till en frihetsberövande påföljd i tre år eller mer, ska således ett överlämnande beviljas utan prövning av om gärningen motsvarar brott enligt svensk lag (se prop. 2003/04:7 s. 76).

Tanken med urvalet av brotten i den s.k. listan enligt artikel 2.2 i rambeslutet är att listan ska omfatta typiskt sett grov, gränsöverskridande brottslighet som kan förekomma mellan medlemsstaterna (se prop. 2001/02:118 s. 8 och prop. 2003/04:7 s. 58.). Vare sig i arresteringsorderlagen eller i dess förarbeten finns angivet vilka svenska brott som motsvarar listbrotten. Detta får anses naturligt eftersom lagen endast gäller överlämnande *från* Sverige enligt en europeisk arresteringsorder och en uppgift från den utfärdande myndigheten om att en gärning omfattas av listan innebär att någon prövning inte ska göras. Frågan om överlämnande *till* Sverige enligt en europeisk arresteringsorder regleras i förordningen (2003:1178)

³ Rådets rambeslut av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan staterna (2002/584/RIF).

⁴ En motsvarande lösning har införts i lagen (2015:650) om erkännande och verkställighet av frivårdspåföljder inom Europeiska unionen.

om överlämnande till Sverige enligt en europeisk arresteringsorder. Enligt förordningen får en arresteringsorder för lagföring utfärdas för brott, för vilket den eftersökte är häktad på sannolika skäl misstänkt för brottet och för vilket är föreskrivet fängelse i ett år eller mer. Inte heller när det gäller överlämnande till Sverige enligt en europeisk arresteringsorder finns det således angivet vilka svenska brott som motsvarar listbrotten. De brott som anges i listan motsvarar dock inte nödvändigtvis brott som i den svenska lagen har samma beteckning (se prop. 2001/02:118 s. 8 och prop. 2003/04:7 s. 57 f.).

För att de brott som anges i bilaga II till PNR-direktivet ska omfattas av direktivets tillämpningsområde krävs, som redan angetts, att de enligt nationell rätt kan leda till minst tre års fängelse. Skrivningen är densamma som i artikel 2.2 i rambeslutet om en europeisk arresteringsorder. Den innebär att det ska ingå tre års fängelse i brottens straffskala för att de ska omfattas, dvs. det ska för de aktuella brotten vara föreskrivet fängelse i tre år eller däröver. Det avgörande är alltså om fängelsestraff av den angivna längden ingår i straffskalan för det brott det gäller. Bedömningen är således hänförlig till straffskalan för ett brott och inte till en straffvärdebedömning.

För Sveriges del innebär kravet på att det ska finnas tre års fängelse i straffskalan för ett brott att det i flera fall krävs att brott bedöms som grova för att de ska omfattas av direktivets användningsområde även om de i och för sig omfattas av listan. Som exempel kan nämnas stöld, bedrägeri, barnpornografibrott och vapenbrott. Narkotikabrott och narkotikasmuggling av normalgraden omfattas dock. Inom tillämpningsområdet faller också t.ex. mord och dråp, grov och synnerligen grov misshandel, människoröv, människohandel, olaga frihetsberövande, våldtäkt, och rån.

9.4.2 Våra överväganden och förslag

Vårt förslag: Begreppet grov brottslighet ska i lagen definieras genom en hänvisning till de brott som anges i bilaga II till PNR-direktivet och för vilka det i nationell rätt i Sverige eller andra medlemsstater är föreskrivet fängelse i tre år eller mer.

Vid genomförandet av EU:s direktiv om underlättande av ett gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott, det s.k. CBE-direktivet, ansåg regeringen det var tillräckligt att i en lagbestämmelse ange att en sökning i en annan stats fordonsregister får göras i syfte att utreda ett sådant trafiksäkerhetsrelaterat brott "som omfattas av artikel 2 i CBE-direktivet" (se prop. 2013/14:65 s. 36 f.). I propositionen hänvisades till att motsvarande författningsteknik använts tidigare i straffrättsliga regleringar som genomfört internationella instrument, bl.a. i 2 § lagen om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott (se prop. 2009/10:78 s. 40 f.).

På samma sätt ansåg regeringen vid genomförandet av VIS-rådsbeslutet, som framgick ovan, att det var tillräckligt att i författningstexten göra en hänvisning till rådsbeslutets definitioner. VIS-rådsbeslutet innehåller samma definitioner av såväl terroristbrott som grov brottslighet som PNR-direktivet, dock med den skillnaden att det för grova brott enligt VIS-rådsbeslutet görs en direkt hänvisning till den s.k. listan i artikel 2.2 i rambeslutet om en europeisk arresteringsorder. I propositionen hänvisade regeringen till att definitionerna är desamma som i den omförhandlade s.k. Eurodacförordningen (EU) nr 603/2013 som bl.a. ger brottsbekämpande myndigheter och Europol rätt att under vissa förutsättningar få tillgång till uppgifter i Eurodac, en EU-gemensam databas med fingeravtryck. Förordningen började tillämpas i juli 2015 och lämnar till tillämparna att avgöra vilka brott som ska anses falla inom definitionerna av terroristbrott och andra grova brott enligt förordningen. Regeringen fann det lämpligt att även beträffande VIS-rådsbeslutet överlämna åt tillämparna att uttolka begreppen. Det angavs också att det ytterst är en fråga för EU-domstolen att avgöra (se prop. 2014/15:82 s. 35 f.). Riksdagen godtog regeringens förslag.

Den hänvisningslösning som har valts vid genomförandet av bl.a. CBE-direktivet och VIS-rådsbeslutet framstår som mest ändamålsenlig. Författningstekniken har därtill använts i flera tidigare lagstiftningsärenden. Metoden att införa en hänvisning till direktivets definition har även den fördelen att regleringen inte kommer att behöva förändras om det i den svenska lagstiftningen skulle införas nya brott med tre års fängelse i straffskalan eller om straffskalan för vissa brott höjs till maximala tre år. Vidare gäller på samma sätt här såsom vi angett ovan angående terroristbrottslighet att inte endast

svensk lagstiftning är av intresse för tillämpningen av den nya lagen. Vid utlämnande av PNR-uppgifter till en behörig mottagare i annan medlemsstat är det således ett villkor att det sker för användning i mottagarlandet vid bekämpning av just sådan grov brottslighet som avses i PNR-direktivet och som i mottagarlandet omfattas av nationell reglering enligt direktivets definition (eller terroristbrottslighet).

Det som talar mot en hänvisning till direktivets definition av grov brottslighet är att en viss otydlighet kan komma att uppstå för tillämparna. Som angivits ovan kommer det dock att vara den nationella enheten för passageraruppgifter som i första hand kommer att behandla PNR-uppgifterna och förfrågningar från behöriga myndigheter m.m. Det kan förutsättas att riktlinjer för enhetens arbete med dessa frågor kommer att utarbetas.

Enligt vår mening framstår lösningen med en direkt hänvisning till direktivets bilaga sammantaget som den både enklaste och lämpligaste lösningen för den nya lagen. Eftersom direktivets definition har rättats bör det av tydlighetsskäl därutöver av lagens definition framgå att brottsligheten ska vara sådan för vilken det i nationell rätt i Sverige eller andra medlemsstater är föreskrivet fängelse i tre år eller mer.

9.5 Otillåten behandling av PNR-information

Vårt förslag: Det ska i lagen föras in en inledande allmän portalbestämmelse som tydliggör att det inte är tillåtet att behandla PNR-uppgifter eller resultatet av en enhet för passagerarinformations behandling av sådana uppgifter i annat syfte än att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Bestämmelsen genomför bl.a. artikel 1.2, 7.4 och 9.2–4. För behöriga myndigheter ska dock gälla ett undantag, som närmare kommer att behandlas i avsnitt 16.2.3.

Vi har redan nämnt att det i artikel 1.2 i direktivet föreskrivs – under artikelns rubrik ”Syfte och tillämpningsområde” – att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet i enlighet med artikel 6.2 a, b och c. (Vi kommer att behandla artikel 6 närmare i avsnitt 13).

Artikeln kan enligt vår mening ses som en portalbestämmelse som talar om vilken behandling av PNR-uppgifter som över huvud taget är tillåten enligt direktivet. Såsom vi tolkar bestämmelsen gäller denna begränsning till bekämpning av terroristbrottslighet och grov brottslighet oavsett om PNR-uppgifterna har samlats in från lufttrafikföretag i Sverige eller har samlats in från lufttrafikföretag i en annan medlemsstat men kommit till Sverige i enlighet med direktivets bestämmelse om utbyte av PNR-uppgifter mellan medlemsstaterna, se artikel 9.2–4. Vidare är begränsningen som huvudregel tillämplig för behöriga myndigheters behandling av mottagna PNR-uppgifter. Det framgår av artikel 7.

Av direktivets olika bestämmelser följer vidare att inte heller resultatet av en enhet för passagerarinformations behandling av PNR-uppgifter får användas för andra syften än att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Vi menar att det är lämpligt att i en allmän portalparagraf slå fast den begränsning för användningen av PNR-uppgifter och resultatet av enheternas behandling av PNR-uppgifter som följer av direktivet. Av tydlighetsskäl bör den formuleras som en förbudsregel som anger att användning för annat slags verksamhet än sådan som avser bekämpning av terroristbrottslighet eller grov brottslighet inte är tillåten. I avsnitt 16.2.3 kommer dock frågan om ett undantag att behandlas (artikel 7.5).

I avsnitt 18.5 kommer vi att föreslå ett mer allmängiltigt förbud som enligt vår mening bör tas in redan i lagens inledande kapitel, nämligen förbudet mot behandling av känsliga personuppgifter. Av framställningstekniska skäl behandlas frågan först i det nämnda senare avsnittet.

10 En enhet för passagerarinformation

10.1 Direktivets bestämmelser

Enligt artikel 4.1 i direktivet ska varje medlemsstat inrätta eller utse en myndighet med behörighet att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet eller en avdelning inom en sådan myndighet vilken ska fungera som medlemsstatens enhet för passagerarinformation. Av skäl 13 framgår att ett syfte med att PNR-uppgifter överförs till en särskilt upprättad enhet är att säkerställa klarhet om vad som gäller och att minska kostnaderna för lufttrafikföretagen. Enheten ska, enligt artikel 4.2, ansvara för att

- a) samla in PNR-uppgifter från lufttrafikföretagen, lagra och behandla dessa uppgifter och överföra dessa uppgifter eller resultatet av behandlingen av dem till behöriga myndigheter,
- b) utbyta både PNR-uppgifter och resultatet av behandlingen av dessa uppgifter med andra medlemsstaters enheter för passagerarinformation och med Europol.

Personal vid enheten för passagerarinformation kan, enligt artikel 4.3, utgöras av tjänstemän som har avdelats från behöriga myndigheter. Vidare anges att medlemsstaterna ska ge enheterna för passagerarinformation tillräckliga resurser för att de ska kunna utföra sina uppgifter. Av artikel 4.4 framgår att två eller flera medlemsstater får inrätta eller utse en och samma myndighet till sin gemensamma enhet för passagerarinformation. Slutligen anges i artikel 4.5 att varje medlemsstat inom en månad från inrättandet eller utseendet av sin enhet för passagerarinformation ska informera kommissionen om detta och får när som helst ändra detta meddelande. Kommissionen ska

offentliggöra meddelandet och eventuella ändringar därav i Europeiska unionens officiella tidning.

10.2 Den svenska enheten för passagerarinformation

Våra förslag: Det ska i lagens inledande bestämmelser tas in en paragraf om att det hos Polismyndigheten ska finnas en enhet för passagerarinformation. I bestämmelsen ska enhetens övergripande uppgifter beskrivas. Dessa är att samla in PNR-uppgifter från lufttrafikföretagen, lagra och behandla dessa uppgifter och överföra PNR-uppgifter och resultaten av behandlingen av dem till behöriga myndigheter samt att utbyta sådan information med andra som är behöriga att motta uppgifterna.

I lagens definitionsparagraf tas in ett samlingsbegrepp för PNR-uppgifter och resultaten av en enhet för passagerarinformations behandling av PNR-uppgifter. Samlingsbegreppet ska benämnas PNR-information.

Det förs även i lagen in en definition av behörig mottagare. Med en behörig mottagare avses en behörig myndighet i Sverige, en enhet för passagerarinformation i en annan medlemsstat, en myndighet som har utsetts som behörig i en annan medlemsstat eller Europol.

Artikel 4 slår alltså fast att varje medlemsstat ska inrätta en egen eller med andra medlemsstater gemensam enhet. Enligt direktivet ska enheten utgöra en egen myndighet med brottsbekämpande uppgifter eller utgöra en avdelning inom en sådan myndighet, Direktivet ger således inte utrymme för att enheten utformas som ett myndighetsgemensamt organ för samverkan mellan flera nationella myndigheter med brottsbekämpande uppgifter. Direktivet slår också fast vad enheten för passagerarinformation ska ha för grundläggande uppgifter.

Enligt våra kommittédirektiv är utgångspunkten för vårt uppdrag att den nationella enheten för passagerarinformation ska placeras vid Polismyndigheten. Det är således inte aktuellt för vår del att överväga en placering hos någon annan myndighet, att en med annan medlemsstat gemensam enhet för passagerarinformation skulle finnas eller att den svenska enheten ska inrättas som en egen myndighet.

Inrättandet och placeringen av den svenska nationella enheten för passagerarinformation bör enligt vår mening komma till klart uttryck genom en bestämmelse som placeras bland den nya lagens inledande bestämmelser. I och med att det redan i lagen framgår att enheten ska finnas och vara placerad vid Polismyndigheten, saknas behov av föreskrifter om enheten i Polismyndighetens instruktion.

Även enhetens övergripande uppgifter bör komma till klart uttryck i bestämmelsen. Dessa uppgifter kan uttryckas på motsvarande sätt som i artikel 4.2 i direktivet. Dock anges i den nämnda artikeln endast att utbyte av PNR-uppgifter och resultatet av behandlingen av dessa uppgifter ska ske med andra medlemsstaters enheter för passagerarinformation och med Europol. Längre fram i direktivet framgår dock att även sådana myndigheter som utsetts som behöriga i andra medlemsstater har rätt att få del av uppgifter från enheten på motsvarande sätt (artikel 9.3). Enligt vår mening bör det redan av denna inledande bestämmelse framgå samtliga aktörer som är behöriga att motta uppgifter från enheten för passagerarinformation. Vi föreslår därför att detta kommer till uttryck i lagen. Vi föreslår även att det i lagens definitionsbestämmelse förs in en definition av behöriga mottagare. Definitionen ska omfatta behöriga svenska myndigheter, enheter för passagerarinformation i andra medlemsstater, myndigheter som har utsetts som behöriga i andra medlemsstater samt Europol. Tredjeländer omfattas inte av definitionen.

Som framgår redan i artikel 4.2 avser enhetens uppgifter inte bara att lagra, analysera och utbyta PNR-uppgifter som mottagits från lufttrafikföretagen. Analyserna m.m. kommer också att leda till så kallade träffar eller andra slags resultat av behandlingen av PNR-uppgifterna. Uttrycket ”PNR-uppgifter eller resultatet av behandlingen av dem” eller motsvarande återkommer ett stort antal tillfällen i direktivet. Det finns därför ett behov av att i den lagstiftning vi föreslår referera till inte bara själva PNR-uppgifterna utan även resultatet av behandlingen av dem. För att förenkla lagstiftningen föreslår vi att det i lagen förs in en definition som omfattar såväl PNR-uppgifter som resultatet av behandlingen av sådana uppgifter. En lämplig samlingsbeteckning är PNR-information, vilket vi alltså föreslår ska tas in i lagens definitionsparagraf.

10.3 Enhetens organisation och utredningens uppdrag

Vår bedömning: Våra författningsförslag ger ett rättsligt ramverk för verksamheten enligt den nya lagen vid enheten för passagerarinformation. Hur enheten närmare ska organiseras, bemannas och administreras m.m. bör överlätas till Polismyndigheten att bestämma, lämpligen i samråd med behöriga myndigheter.

Enligt våra kommittédirektiv ska Polismyndigheten ansvara för genomförandet av direktivets tekniska bestämmelser. I vårt utredningsuppdrag ingår dock att föreslå hur enheten för passagerarinformation ska organiseras.

Inom Polismyndigheten pågår redan ett arbete med att införa en enhet för passagerarinformation. En förstudie gällande införandet av en systematiserad hantering av PNR- och API-uppgifter har, som beskrivits i avsnitt 7.2.1, genomförts av Polismyndigheten tillsammans med Tullverket och Säkerhetspolisen. I förstudien finns förslag på hur enheten för passagerarinformation ska vara organiserad. Polismyndigheten har också, tillsammans med Tullverket, ansökt om och erhållit bidrag från kommissionen för att etablera en enhet för passagerarinformation. Det pågår för närvarande ett arbete med att etablera en sådan enhet med tillhörande it-stöd.

Vi har tolkat utredningsuppdraget så att vi i frågan om hur enheten för passagerarinformation ska vara organiserad bör arbeta i linje med det planeringsarbete som redan pågår. Vi ser det således som vårt uppdrag att se till att det finns ett rättsligt ramverk inom vilket inrättandet och organiseringen kan utvecklas vidare. Vår målsättning är således att ge Polismyndigheten möjlighet att genomföra direktivets tekniska bestämmelser och utarbeta hur enheten för passagerarinformation rent operativt och administrativt ska organiseras. De mer praktiska frågorna kring hur enheten för passagerarinformation rent faktiskt ska arrangeras och bemannas tas lämpligen och bäst om hand av involverade myndigheter själva. Utgångspunkten för vårt arbete är alltså att Polismyndigheten i stor utsträckning ska få bestämma sin egen organisation (jfr 38 § förordning [2014:1102] med instruktion för Polismyndigheten). Med tanke på enhetens uppgifter att bidra till arbetet att bekämpa terroristbrottslighet och

grov brottslighet även vid andra behöriga myndigheter, ter det sig dock lämpligt att det i relevant omfattning sker ett samråd med dessa andra myndigheter när det gäller utformningen av enhetens organisation och arbetssätt m.m. Det är dock inget som vi anser behöver regleras närmare. Endast i den mån det anses nödvändigt kommer vi därför att föreslå att enheten för passagerarinformationsorganisation ska författningsregleras (jfr prop. 2013/14:110 s. 395 f.).

Organisatoriska frågor för utredningen

Vi ser det således som vårt uppdrag att utarbeta ett rättsligt ramverk inom vilket Polismyndigheten kan organisera enheten för passagerarinformation. Den övergripande rättsliga frågan av organisatorisk karaktär som enligt vår mening bör behandlas av utredningen, avser att överväga vilken reglering som krävs för att säkerställa att behandlingen av PNR-information vid enheten för passagerarinformation hålls tillräckligt åtskild från övrig personuppgiftsbehandling inom Polismyndigheten och från behöriga myndigheter i övrigt. PNR-direktivet kan nämligen inte förstås på annat sätt än att de från lufttrafikföretagen insamlade uppgifterna och analysresultaten m.m., dvs. PNR-informationen, ska skyddas inom de nationella enheterna och bara, i bildlig mening, passera enheternas väggar genom de dörrar och under de förutsättningar i övrigt som direktivets regelverk ställer upp. I och med att den svenska enheten inrättas i en befintlig stor myndighet uppstår frågor om hur dessa ”väggar” lämpligen kan åstadkommas. Denna fråga kommer att analyseras i nästföljande avsnitt 10.4. En annan fråga med organisatorisk anknytning är vilka rättsliga konsekvenser m.m. som följer av planerna på att det vid enheten ska tjänstgöra personal som har sin grundanställning vid andra behöriga myndigheter, se avsnitt 7.2.1. Den frågan behandlas nedan i avsnitt 10.5.

10.4 Tillgången till PNR-information bör begränsas

10.4.1 Direktåtkomst

Vårt förslag: Direktåtkomst till PNR-information som behandlas vid enheten för passagerarinformation hos Polismyndigheten ska inte vara tillåten. En bestämmelse som klargör detta tas in i lagen.

Om direktåtkomst

Det finns inte någon legaldefinition av begreppet direktåtkomst. Begreppet har dock använts i lagstiftningssammanhang sedan 1990-talet. Dessförinnan användes begreppet terminalåtkomst. Begreppet direktåtkomst har i senare års dataskyddsreglering främst använts såsom en specialform av elektroniskt utlämnande genom passerande av rättsliga gränser mellan myndigheter eller mellan självständiga verksamhetsgrenar inom myndigheter, s.k. sekretessgränser. Med direktåtkomst avses vanligtvis att någon myndighet har en sådan teknisk tillgång till en annan myndighets upptagningar som avses i 2 kap. 3 § andra stycket TF. En myndighet med direktåtkomst har alltså getts direkt tillgång till någon annan myndighets register eller databas och kan på egen hand söka efter information, normalt utan att kunna påverka innehållet i registret eller databasen (se bl.a. prop. 2009/10:85 s. 168). I begreppet ligger också att den som är personuppgiftsansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av. Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar således inte något beslut om utlämnande av de uppgifter som den som har direktåtkomst tar del av i varje enskilt fall (se bl.a. SOU 2015:39 s. 121). Beslutet att lämna ut uppgifterna tas långt tidigare. Uppgifterna i registret eller databasen är nämligen att betrakta som utlämnade i tryckfrihetsförordningen och sekretesslagstiftningens mening redan då direktåtkomsten tekniskt etableras.

Varken nuvarande personuppgiftslag eller det nya dataskyddsdirektivet reglerar närmare olika sätt att elektroniskt lämna ut personuppgifter. Inte heller brottsdatalagen innehåller bestämmelser av det slaget. Däremot förekommer sådana bestämmelser i polisdatalagen,

tullbrottsdatalagen och flertalet andra registerförfattningar på området. Enligt 2 kap. 21 § PDL är direktåtkomst tillåten bara i den utsträckning som följer av polisdatalagen. Av 3 kap. 8 § PDL följer att bl.a. Säkerhetspolisen, Ekobrottsmyndigheten och Tullverket får medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga i Polismyndighetens brottsbekämpande verksamhet. Med gemensamt tillgängliga avses att fler än ett fåtal personer har rätt att ta del av uppgifterna (3 kap. 1 § PDL). Enligt en förekommande uppfattning innebär tillgång bland en grupp på fler än tio personer att rekvisitet gemensamt tillgängliga är uppfyllt. Inte bara antalet personer med tillgång räknas emellertid. Även sådana faktorer som hur länge uppgifter behandlas kan ha betydelse för att ta bara ett exempel. I 3 kap. 2 § PDL anges vilka personuppgifter som får göras gemensamt tillgängliga.

Det kan också nämnas att lagen (2006:444) om passagerarregister, som tillkommit för att genomföra API-direktivet i svensk rätt, tillåter Säkerhetspolisen att ha direktåtkomst till personuppgifterna i det registret.

Våra överväganden

Av PNR-direktivet följer att behöriga myndigheter, inklusive Polismyndigheten, ska få tillgång till PNR-information först efter det att de har behandlats och vidareförts från enheten för passagerarinformation i enlighet med en viss procedur enligt direktivets bestämmelser. De behöriga myndigheterna kan således inte, såsom i lagen om passagerarregister, tillåtas ha egen åtkomst till PNR-information som behandlas vid enheten.

Som vi redovisat i avsnitt 8.5 kommer polisdatalagen att vara tillämplig vid enhetens behandling av PNR-uppgifter och andra personuppgifter i den utsträckning den nya lagstiftning vi föreslår inte innehåller avvikande bestämmelser. Det är vår bedömning att PNR-uppgifterna, som ska lagras fem år i en databas enligt direktivet, likväl som resultatet av enhetens behandling av PNR-uppgifterna rimligen bör betraktas som sådana personuppgifter som gjort gemensamt tillgängliga inom Polismyndighetens brottsbekämpande verksamhet även om uppgifterna de facto behandlas avgränsat vid enheten. Med tanke på vad 3 kap. 8 § PDL föreskriver om att direktåtkomst

får medges till vissa av de myndigheter som är behöriga myndigheter enligt PNR-direktivet, anser vi att det behövs en uttrycklig bestämmelse i den nya lagen som förbjuder direktåtkomst till PNR-information som behandlas vid enheten. Utan en sådan bestämmelse ger nämligen, logiskt sett, 3 kap. 8 § PDL en rättslig öppning för att medge direktåtkomst till enhetens PNR-information. Vi föreslår därför en sådan förbudsbestämmelse, som kommer att gälla i stället för polisdatalagens reglering av direktåtkomst. Genom en bestämmelse som inte tillåter direktåtkomst säkerställs alltså att andra behöriga myndigheter än Polismyndigheten förhindras att ta direkt del PNR-information som behandlas vid enheten. Med hänsyn till bestämmelsens grundläggande betydelse bör den, enligt vår mening, föras in i vårt förslag till lag.

Vi förutsätter att informationsutbytet enligt direktivet ska kunna ske med användning av modern informationsteknik. Därmed anser vi att det i vår reglering finns behov av ett undantag från den nuvarande bestämmelsen i 2 kap. 20 § första meningen PDL som anger att endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Frågan kan regleras i förordning.

10.4.2 Sekretess inom Polismyndigheten?

Vår bedömning: Det kommer inte att finnas någon sekretessgräns mellan enheten för passagerarinformation och Polismyndighetens övriga brottsbekämpande verksamhet. Det finns inte heller tillräcklig anledning att föreslå en reglering som skulle kunna skapa en sådan sekretessgräns.

Uppgifter inom Polismyndighetens verksamhet omfattas av bestämmelserna om tystnadsplikt och handlingssekretess i offentlighets- och sekretesslagen. Uppgifter som skyddas av sekretess får inte lämnas ut till en enskild eller annan myndighet utan stöd i offentlighets- och sekretesslagen. Sekretess gäller således även mellan myndigheter (8 kap. 1 § OSL). Mellan myndigheter, även med näraliggande uppgifter, finns alltså sekretessgränser.

Enligt 8 kap. 2 § OSL kan det även finnas en sekretessgräns inom en myndighet, nämligen mellan *olika* verksamhetsgrenar om de är att betrakta som *självständiga* i förhållande till varandra. Mellan så-

dana verksamhetsgränser får sekretessbelagda uppgifter inte röjas utan stöd i offentlighet- och sekretesslagen. Bestämmelsen har sin motsvarighet i 2 kap. 8 § TF om när en handling blir allmän när den överlämnats mellan organ inom samma myndighetsorganisation. Det avgörande är även i detta fall att organen uppträder som självständiga i förhållande till varandra. Däremot behöver det inte vara fråga om olika verksamhetsgrenar.

Frågan om när organ eller verksamhetsgrenar inom samma myndighetsorganisation är att betrakta som självständiga i förhållande till varandra kan vara svårbedömd. Frågan har behandlats i ett antal propositioner på senare år, se t.ex. En Kronofogdemyndighet i tiden (prop. 2005/06:200 s. 146 f.) och Patientdatalag m.m. (prop. 2007/08:126 s. 162 f. och 202). I dessa propositioner har, mot bakgrund av uttalandena i förarbetena till den tidigare gällande sekretesslagen, slagits fast att om olika delar av en myndighets verksamhet har att tillämpa olika sekretessbestämmelser, får de anses utgöra olika verksamhetsgrenar i sekretesslagens mening. Först om olika delar av en myndighet utgör olika verksamhetsgrenar i sekretesslagstiftningens mening finns det skäl att även ta ställning till om de också är att betrakta som självständiga i förhållande till varandra.

I motiven till offentlighets- och sekretesslagen anges att det förhållandet att en myndighet har att tillämpa olika sekretessbestämmelser inte med automatik innebär att det också finns olika verksamhetsgrenar inom myndigheten i lagens mening. Att myndigheten har att tillämpa flera olika sekretessbestämmelser kan t.ex. bero på att bestämmelserna visserligen gäller på samma verksamhetsområde men att de finns i olika kapitel därför att de gäller till skydd för olika intressen, t.ex. sekretess till skydd för allmänna intressen i 18 kap. OSL och sekretess till skydd för enskildas intressen i 35 kap. OSL. Sekretessregleringen inom ett verksamhetsområde kan vidare vara uppdelad på flera paragrafer av redaktionella skäl. Först om det finns olika delar av en myndighets verksamhet som har att tillämpa sinsemellan helt olika set av sekretessbestämmelser är det fråga om olika verksamhetsgrenar i sekretesslagstiftningens mening. Om så är fallet behövs det därutöver göras en bedömning av om de olika verksamhetsgrenarna också har organiserats på ett sådant sätt att de förhåller sig självständiga till varandra. Det är bara om båda dessa kriterier är uppfyllda som det uppstår en sekretessgräns inom en myndighet. (Se prop. 2008/09:150 s. 358 ff.).

De tidigare 21 polismyndigheterna, Rikspolisstyrelsen och Statens kriminaltekniska laboratorium slogs den 1 januari 2015 ihop i en ny myndighet, Polismyndigheten. Säkerhetspolisen utgör sedan samma datum en egen myndighet. I propositionen En ny organisation för polisen (prop. 2013/14:110) analyserades om det kommer att finnas enheter inom den nya Polismyndigheten som intar en sådan ställning att de kan anses utgöra självständiga organ i tryckfrihetsförordningens mening. Det ansågs då ännu inte gå att bedöma vilka delar av verksamheten som skulle komma att anses som självständiga organ. Den omständigheten att handläggningen av vissa ärenden koncentreras till en viss enhet inom myndigheten ansågs dock inte innebära att enheten kan anses som ett självständigt organ i den mening som avses i 2 kap. 8 § TF (se a. prop. s. 507 ff.).

I propositionen analyserades vidare om det kommer att finnas sekretessgränser inom Polismyndigheten. Åtta olika verksamhetsgrenar identifierades: den brottsförebyggande och brottsutredande verksamheten (18 kap. 1–3 §§ och 35 kap. 1–5 §§), särskilt personsäkerhetsarbete enligt 2 a § polislagen [1984:387] (18 kap. 7 § och 35 kap. 11 §), handläggningen av vapenärenden (18 kap. 16 § och 35 kap. 23 §), verksamhet enligt lagen om fingerade personuppgifter (22 kap. 2 §), räddningsinsatser enligt lagen om skydd mot olyckor (32 kap. 8 §), verksamhet som avser hjälp och bistånd till enskilda (35 kap. 20 §), verksamhet som avser utlänningskontroll och medborgarskap (37 kap. 1 §) och verksamhet som avser skadereglering (40 kap. 6 §). Bedömningen gjordes att de verksamheter som avser personsäkerhetsarbete och fingerade personuppgifter kunde anses utgöra självständiga verksamhetsgrenar i den tidigare organisationen, men att övriga verksamhetsgrenar tidigare inte hade organiserats så att de kunde anses vara självständiga i förhållande till varandra. Det förutsattes att de både verksamheterna avseende personsäkerhetsarbete och fingerade personuppgifter skulle komma att organiseras skilda från övriga verksamheter så att sekretessgränser uppstår. Huruvida övriga verksamhetsgrenar kommer att kunna anses vara självständiga angavs bero på hur den nya myndigheten organiseras. Det angavs vidare att det vid tillfället inte gick att med säkerhet uttala sig om i vilken utsträckning det kommer att finnas sekretessgränser inom Polismyndigheten, men att det är sannolikt att det i de allra flesta fall inte kommer att finnas sådana gränser. (Se a. prop. s. 508 f.) Angående en följdändring i 2 kap. 18 § PDL, angavs vidare

att ”första stycket har anpassats till att sekretess inte gäller inom Polismyndigheten i dess brottsbekämpande verksamhet, varför polismyndigheter har tagits bort” (a. prop. s. 649).

En närliggande fråga är hur en befattningshavare ska tillämpa sekretessreglerna i förhållande till sina kollegor. Den frågan berörs i viss utsträckning i förarbetena till ändringar i sekretesslagen. Där uttalas att sekretessreglerna inte anses utgöra hinder mot att lämna uppgifter mellan befattningshavare hos en myndighet i den utsträckning som är normal för och behövlig för ett ärendes handläggning eller verksamhetens bedrivande i övrigt (prop. 1990/91:111 s. 24.) Det framhålls dock att det av grunderna för sekretesslagen torde följa att en befattningshavare inte bör anses ha en obegränsad frihet att lämna uppgifter som omfattas av sekretess till andra anställda inom myndigheten. JO har också uttalat att det torde stå klart att en befattningshavare inte har någon obegränsad frihet att lämna uppgifter som omfattas av sekretess till sina arbetskamrater (JO 1983/84 s. 262). JO konstaterar dock att sekretesslagstiftningen inte kan anses utgöra ett hinder mot att en handläggare rådfrågar andra befattningshavare om ett ärende, åtminstone inte om det framstår som objektivt försvarbart. Uppgifter måste också fritt kunna lämnas till den som på ett eller annat sätt deltar i beredningen och avgörande av ett ärende. (Se prop. 2013/14:110 s. 517.)

Vår bedömning

Enheten för passagerarinformation kommer att vara en egen enhet men som sådan utgöra en del av Polismyndighetens brottsbekämpande verksamhet. När det gäller informationsöverföring inom Polismyndigheten synes den rådande uppfattningen vara den att det inte förekommer sekretessgränser (eller sekretessväggar) inom Polismyndighetens brottsförebyggande och brottsutredande verksamhet (se t.ex. a. prop. s. 508 f.). Vi delar den uppfattningen. De sekretessbestämmelser som i första hand blir tillämpliga för PNR-information som behandlas hos enheten finns i 18 kap. 1–2 §§ OSL, till skydd för den brottsbekämpande verksamheten, och 35 kap. 1–2 §§ OSL, till skydd för enskilda. Dessa bestämmelser tillämpas också för annan brottsförebyggande och brottsutredande verksamhet.

Även för det fall särskilda sekretessbestämmelser därutöver skulle införas avseende PNR-information m.m. till skydd för verksamheten vid enheten och för registrerade passagerare (se dock våra bedömningar i den frågan i avsnitt 24) är det knappast motiverat att skapa ett helt eget set av sekretessbestämmelser för verksamheten inom enheten för passagerarinformation. Såvitt kan bedömas är det varken möjligt eller lämpligt att införa någon sekretessreglering i syfte att utforma arbetet inom enheten som en egen verksamhetsgren av annat slag än den brottsförebyggande och brottsutredande verksamheten i övrigt vid Polismyndigheten. Trots att enheten för passagerarinformation kommer att organiseras skild från övrig verksamhet, är det inte heller troligt att den kommer att organiseras så att den blir i tillräcklig grad självständig gentemot övrig brottsbekämpande verksamhet vid Polismyndigheten. Som vi angett ovan bör det överlämnas åt Polismyndigheten att närmare bestämma hur enheten ska organiseras. Sammanfattningsvis är det därför olämpligt att lagstiftningsvägen försöka skapa en ny sekretessgräns inom den brottsbekämpande verksamheten.

Begränsningar i tillgången till PNR-information inom Polismyndigheten med stöd av sekretessbestämmelser synes alltså inte vara en framkomlig väg för att skydda PNR-informationen i förhållande till övrig brottsbekämpande verksamhet inom Polismyndigheten. Det bör dock i sammanhanget påpekas att frånvaron av en sekretessgräns mellan enheten för passagerarinformation och övrig brottsförebyggande och brottsutredande verksamhet inte innebär att det finns en obegränsad rätt att sprida sekretessbelagda uppgifter till kollegor inom myndigheten.

10.4.3 Begränsningar via dataskyddsbestämmelser m.m.

Våra förslag: Det ska föras in en bestämmelse i lagen om att bara den som tjänstgör vid enheten för passagerarinformation får ha tillgång till PNR-information som behandlas vid enheten samt att tillgången till PNR-informationen ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter vid enheten. Närmare bestämmelser om tillgång, behörighetstilldelning m.m. kan meddelas genom föreskrifter av regeringen eller myndighet som regeringen bestämmer.

Nuvarande reglering i polisdatalagstiftningen m.m.

I 2 kap. 11 § PDL slås fast att tillgången till personuppgifter inom Polismyndigheten ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen omfattar såväl direkt tillgång till automatiserade uppgiftssamlingar som tillgång i allmänhet. Polismyndigheten ska således organisera sin verksamhet på ett sådant sätt att obefogad spridning av personuppgifter motverkas. Bestämmelsen riktar sig inte bara till dem som är engagerade i den dagliga verksamheten. Den måste också beaktas av dem som ansvarar för utformningen av nya datasystem liksom av dem som avgör vilken tillgång till personuppgifter respektive tjänsteman behöver för att kunna fullgöra sina uppgifter. (Se prop. 2009/10:85 s. 94 och 326.) I bestämmelsens andra stycke finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela närmare föreskrifter om förutsättningarna för tillgången till personuppgifter. Detaljbestämmelser kan således utformas så att tillgången till personuppgifter begränsas till vad som är nödvändigt för verksamhetens bedrivande. I lagens förarbeten har angetts att det inte är lämpligt att i lagform ange detaljerade riktlinjer för hur tillgången till personuppgifter bör avgränsas. Det har i stället angetts vara Polismyndighetens och övriga berörda myndigheters uppgift att, utifrån respektive myndighets organisation och struktur, säkerställa att åtkomsten till personuppgifter begränsas i enlighet med bestämmelsen (a. prop. s. 95.) Regeringen har i 3 § PDF föreskrivit att Polismyndigheten och Säkerhetspolisen får meddela närmare föreskrifter om tillgången till personuppgifter för sina respektive verksamhetsområden. Vidare anges att för tilldelning av behörigheter för åtkomst till personuppgifter ska det särskilt beaktas att det, utöver behovet av uppgifterna, ställs krav på utbildning och erfarenhet. Enligt 4 § ska de nu nämnda myndigheterna ansvara för att det inom respektive myndighet finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter. Av 4 a § framgår vidare att beträffande penningtvätsregistret som regleras i 4 kap. 18 § PDL och det internationella registret som regleras i 4 kap. 21 § PDL får bara tjänstemän vid särskilda enheter ges tillgång till uppgifter i de registren. I paragrafen anges således att endast tjänstemän vid finansunderrättelseenheten vid Polismyndigheten får ha tillgång till upp-

gifter i penningtvätsregister och att endast tjänstemän vid den nationella funktionen för internationella uppgifter vid Polismyndigheten får ha tillgång till uppgifter i det internationella registret. Av bestämmelsen framgår vidare att det vid Polismyndigheten löpande ska föras en förteckning över de tjänstemän vid myndigheten som behandlar dessa uppgifter.

I förarbetena till polisdatalagen framgår därtill att underrättelseverksamhet bedrivs vid särskilda enheter med särskilt utbildade tjänstemän och att det är en naturlig del av underrättelsearbete att begränsa antalet tjänstemän som tar del av viss information (a. prop. s. 107). I propositionen En ny organisation för polisen (prop. 2013/14:110) anges att det får förutsättas att underrättelsearbetet kommer att bedrivas på samma sätt i den nya polisorganisationen. Polismyndigheten och Säkerhetspolisen ska se till att anställda som arbetar med underrättelseverksamhet inte ges tillgång till fler uppgifter än de har behov av i sitt arbete (a. prop. s. 517).

I de för Tullverket nu gällande bestämmelserna om tillgång till passageraruppgifter finns bestämmelser som reglerar vilka anställda som ska ha behörighet att ta del av bokningsuppgifterna. Således anges i 4 kap. 6 § tullförordningen (2016:287) och i 5 § förordningen (1996:702) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen att chefen för Tullverket, eller en chefstjänsteman som förordnats för uppgiften av chefen, beslutar om vilka anställda som ska ha behörighet att ta del av bokningsuppgifter som lämnats av transportföretag, eller genom terminalåtkomst. Behörighet ska endast ges till den som har nödvändig utbildning och som behöver informationen för sina arbetsuppgifter inom Tullverkets brottsbekämpande verksamhet.

Våra överväganden

Inom en myndighet utan inre sekretessgränser ställer det allmänna dataskyddsrättsliga regelverket krav på att personuppgifter ska skyddas genom att tillgången till uppgifterna avgränsas och begränsas så långt möjligt är för verksamheten. Som framgått ovan finns redan tydliga regler om detta för Polismyndighetens del i polisdatalagstiftningen. Det är snarare regel än undantag att sådana bestämmelser tas in i registerförfattningar som sätter ramar för myndigheternas

informationshantering. Denna dataskyddsreglering sker utifrån intresset att tillgodose enskilda registrerades intresse av att personuppgifter om dem hanteras på ett sätt som ger dem ett tillbörligt skydd för deras personliga integritet.

I stor utsträckning överlappande och likartade krav på att begränsa tillgång till myndigheternas information, särskilt känslig sådan, följer även av annan reglering som motiverats av helt andra intressen än det integritetsintresse som ligger bakom den dataskyddsrättsliga regleringen. Begränsningar av tillgången till en myndighets elektroniska informationssamlingar behövs för att skydda t.ex. verksamhetens effektivitet, samhällsfunktioner och liknande. Det säger sig självt att Polismyndighetens verksamhet är sådan att ett otal begränsningar i polisanställdas tillgång till information måste finnas för att skydda informationen från risken att spridas till nackdel för polisverksamheten som sådan.

Inom enheten för passagerarinformation kommer det att finnas personuppgifter om enskilda som inte bör kunna vara allmänt tillgängliga inom Polismyndigheten för att PNR-direktivets krav på tillfredsställande integritetsskydd ska uppnås (se t.ex. artikel 13.2). En korrekt tillämpning av polisdatalagens och polisdataförordningens bestämmelser skulle emellertid i och för sig kunna anses tillräckliga för att få till konsekvens att endast den som tjänstgör vid enheten för passagerarinformation ges tillgång till PNR-information som behandlas vid enheten. Dock anser vi att frågan om begränsning av tillgången är så pass central för integritetsskyddet att den bör regleras särskilt. Ett tillägg i 4 a § PDF om att endast tjänstemän vid enheten får ha tillgång till PNR-information skulle därvid i och för sig kunna tänkas. I och med att PNR-direktivet genomförs genom en egen avgränsad lagstiftning är det emellertid lämpligare att bestämmelser om begränsningar i tillgången tas in i den lag och förordning som vi föreslår. Vi menar också att en övergripande bestämmelse om att endast den som tjänstgör vid enheten får ha tillgång till PNR-information är av så stor vikt för integritetsskyddet att den bör tas in i lagen.

Det är också av vikt, menar vi, att det inom enheten inte ska få lov att vara full åtkomst till PNR-informationen alldeles oavsett om det är motiverat för verksamhetens effektivitet och ändamålsenlighet eller inte. Även detta bör framgå på lagnivå. Vi föreslår därför att det i lagen också anges att tillgången till PNR-informationen ska

begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter vid enheten. Därmed framgår motsatsvis att onödigt bred åtkomst bland tjänstemännen på enheten inte får förekomma. Närmare bestämmelser om tillgången – inom denna ram – bör dock kunna meddelas i förordningen eller genom föreskrifter av Polismyndigheten. Dessa bestämmelser kommer att gälla i stället för polisdatalagstiftningens reglering. Vi kommer att i senare avsnitt föreslå en bestämmelse i förordningen om att tillgången till vissa slags uppgifter ska begränsas, se avsnitt 13.4.

Därutöver får tillgången till uppgifterna vid enheten för passagerarinformation regleras internt med hjälp av bestämmelser om behörighetstilldelning. Med en sådan ordning kan de uppgifter som behandlas inom enheten på ett enkelt sätt avgränsas och omges av extra integritets- och säkerhetsskydd. Därmed kan tillgången till den information som finns tillgänglig inom enheten för passagerarinformation begränsas till vad varje tjänsteman behöver för att utföra sina arbetsuppgifter. Behörighetsstyrning och principer som avgör tillgången till uppgifter kan utarbetas på förhand. Behörigheterna kan vidare anpassas till olika befattningshavares behov med hänsyn till tjänstenivå och arbetsuppgifter.

Inom enheten kommer emellertid att behandlas inte bara PNR-information som vårt förslag tar sikte på. Enheten kommer exempelvis att kunna göra slagningar i andra databaser som finns tillgängliga i den brottsbekämpande verksamheten. Tillgång och övriga förutsättningar för detta bör, menar vi, lämpligen bedömas och hanteras utifrån polisdatalagstiftningen eller annan tillämplig reglering för detta. Vi föreslår alltså ingen tillkommande dataskyddsrättslig reglering för detta.

Vidare kommer enheten att motta framställningar med förfrågan från behöriga svenska myndigheter, andra länders enheter för passagerarinformation eller Europol. Dessa förfrågningar ska vara motiverade och det kan förmodas att de innehåller information som är känslig både för enskilda personer och för underrättelse- eller utredningsverksamheten vid den begärande myndigheten. Hur dessa ska skyddas från alltför stor tillgänglighet inom enheten eller från spridning ut till övrig verksamhet inom Polismyndigheten bör myndigheten lämpligen själv tillse, på motsvarande sätt som i dag sker beträffande annan information som av andra hänsyn än integritetsintresset inte kan få bli fritt tillgänglig bland myndighetens tiotusen-

tals anställda. Vi föreslår därför ingen reglering av detta. Däremot kommer vi i nästföljande avsnitt att behandla några särskilda frågor som uppkommer med anledning av att personal från andra myndigheter, dvs. andra behöriga myndigheter än Polismyndigheten, kommer att tjänstgöra vid enheten.

Slutligen hänvisar vi till avsnitt 24 där vi allmänt kommer att behandla frågor om det behövs nya eller förändrade sekretessbestämmelser för att skydda PNR-informationen. En ytterligare fråga är om det behövs sekretessbrytande bestämmelser för att möjliggöra de uppgiftsströmmar som PNR-systemet innefattar.

10.5 Personal anställd vid andra myndigheter

Vår bedömning: Det behövs inga särskilda bestämmelser med anledning av att personal med grundanställning vid andra behöriga myndigheter än Polismyndigheten kommer att tjänstgöra vid enheten för passagerarinformation.

Som tidigare angetts kan enligt direktivet personalen vid enheten för passagerarinformation komma att utgöras av tjänstemän som har avdelats från behöriga myndigheter. Således kan personalen vid enheten komma att ha sin grundanställning inte bara vid Polismyndigheten utan även vid exempelvis Tullverket och Säkerhetspolisen. En sådan bemanning ger större möjligheter att ta tillvara den samlade kompetensen som finns inom de behöriga myndigheterna och underlättar för enheten att bedriva sin verksamhet på ett sätt som är till så stor nytta som möjligt för de behöriga myndigheternas bekämpning av terroristbrottslighet och grov brottslighet. Såvitt vi förstått det parallella projektarbetet med att praktiskt och tekniskt organisera enheten för passagerarinformation är tanken att tjänstemännen i sitt arbete vid enheten för passagerarinformation ska representera enheten och inte sina respektive myndigheter. Det är en tanke som är i linje med vad vi angett tidigare om att enheten ska ingå i Polismyndigheten, dvs. inte vara ett samverkansorgan för flera myndigheter.

En följd av detta är att tjänstemän vid enheten som har avdelats från t.ex. Säkerhetspolisen eller Tullverket anses delta i arbetet vid enheten för passagerarinformation och därmed vid Polismyndigheten.

De kommer därmed att i enlighet med 2 kap. 1 § OSL bli bundna av sekretess som gäller för Polismyndighetens arbete vid denna enhet. Det gäller även i förhållande till deras ”hemmamyndigheter”. När personal från Tullverket eller Säkerhetspolisen arbetar inom enheten uppkommer alltså en sekretessgräns mellan dem och dessa myndigheter. Inom enheten kommer det, å andra sidan, inte att finnas sekretessgränser mellan anställda från Polismyndigheten, Säkerhetspolisen eller Tullverket.

En jämförelse kan i detta sammanhang göras med det arbete som sker vid Nationellt centrum för terrorhotbedömning (NCT), som är en permanent myndighetsgemensam arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten vid Försvarmakten (Must) och som nyligen setts över och analyserats från rättslig synvinkel, se Ds 2016:31. Vid NCT arbetar analytiker från de tre NCT-myndigheterna, i gemensamma lokaler hos Säkerhetspolisen. Under sin tid på NCT behåller personalen sin anställning hos den ordinarie myndigheten. Analytikerna vid NCT är, vid sin placering där, alltså fortfarande anställda vid respektive myndighet och företräder också den myndigheten i arbetet vid NCT. Den behandling av personuppgifter som respektive analytiker utför inom ramen för NCT-samarbetet, utför denne som företrädare för den egna myndigheten. I samarbetet finns myndighetsspecifika mappar med information och handläggares personliga mappar, men det finns också en gemensam mapp. Utbytet inom samarbetet av personuppgifter sker med stöd av respektive myndighets registerförfattning. Den information som ligger till grund för NCT:s analyser och bedömningar hämtas in av tjänstemännen främst från deras respektive hemmamyndigheter. Informationen hämtas från bl.a. olika register och databaser. Analytikerna använder sina egna myndigheters IT-system och har inte tillgång till varandras system. Vid sin placering på NCT har analytikernas tillgång till information begränsats genom olika behörigheter och analytikerna kommer endast åt sådan information från hemmamyndigheterna som anses vara relevant för det uppdrag de har vid NCT. I den nyss nämnda utredningen föreslås att det i respektive myndighets registerförfattning införs bestämmelser om att direktåtkomst får medges till de andra samarbetande myndigheterna med anknytande sekretessbrytande bestämmelser. Förslaget bereds för närvarande i Regeringskansliet.

Av redogörelsen för NCT framgår motsatsvis att förutsättningarna kommer att vara helt andra vid enheten för passagerarinformation i och med att avdelade tjänstemän från t.ex. Tullverket kommer att delta i Polismyndighetens arbete när de tjänstgör vid enheten. Den information som hanteras inom enheten, inte bara personuppgifter, kommer vidare att ingå i Polismyndighetens informationsmassa.

Det innebär att en anställd från Tullverket inte kommer att kunna göra slagningar i Tullverkets informationssamlingar med stöd av sin behörighet för tillgång enligt 2 kap. 11 § TBL med anknytande föreskrifter. I stället kommer det att få ske med stöd av den direktåtkomst för Polismyndigheten som kan medges enligt 3 kap. 8 § TBL. När tjänstemannen i fråga t.ex. gör en sökning i informationssamlingar som hör till Polismyndigheten sker det följaktligen inte heller med stöd av direktåtkomst för Tullverket (2 kap. 16–18 §§ PDL) utan på grund av den eventuella behörighet för tillgång som Polismyndigheten kan ha gett i enlighet med de bestämmelser vi ovan redogjort för i 4 § PDF m.m. och de vi föreslagit i den nya lagen med anknytande föreskrifter.

Som vi tidigare påpekat kommer det av allt att döma att förekomma information av olika slag som är mycket känslig, t.ex. om underrättelseoperationer eller som rör rikets säkerhet och liknande, som bara ett fåtal bör känna till och arbeta med. Av den anledningen, samt även ur effektivitetssynpunkt, torde det t.ex. vara lämpligt att bara den som avdelats från Säkerhetspolisen ges rätt att arbeta med att besvara Säkerhetspolisens framställningar om att få ut PNR-information från enheten eller dito framställningar från enheter i andra medlemsstater som uppenbarligen syftar till att vidarebefordras till det landets behöriga säkerhetstjänst. Likaså kan det vara rimligt att den som avdelats från Tullverket ges behörighet att för enhetens, dvs. Polismyndighetens räkning, använda den direktåtkomst till Tullverkets informationssamlingar som Polismyndigheten medgetts. Dessa slags frågeställningar med anknytning till att personal från olika myndigheter arbetar vid enheten bör dock inte regleras i den lagstiftning vi föreslår, utan lämnas bäst över till Polismyndigheten att i samråd med inblandade myndigheter reglera genom föreskrifter, arbetsordning för enheten eller liknande. Vi ser alltså framför oss att det finns behov av en tämligen strikt behörighetstilldelning av

hänsyn till såväl dataskydd och integritet som helt andra skyddshänsyn.

Redan i detta sammanhang vill vi påpeka att det i vårt arbete inte funnits förutsättningar att klarlägga vilka informationssamlingar utöver PNR-uppgifterna som man kommer behöva använda sig av i arbetet vid enheten för passagerarinformation. Det sagda gäller register och andra gemensamt tillgängliga uppgifter hos både Polismyndigheten och hos andra myndigheter. Vi utgår därför från att enheten, när den startar det operativa arbetet, kommer att utnyttja system som den nuvarande registerförfattningsregleringen m.m. ger förutsättningar för genom ramar för ändamålbestämning, direktåtkomst m.m.

11 Lufttrafikföretagens överföring av PNR-uppgifter

11.1 Om lufttrafikföretag

PNR-direktivet ålägger lufttrafikföretag att överföra uppgifter om sina passagerare. Ett lufttrafikföretag definieras i direktivet som ett lufttrafikföretag med giltig operativ licens eller motsvarande som ger rätt att bedriva passagerarflygtrafik (artikel 3.1).

Gemensamma bestämmelser för tillhandahållande av lufttrafik i gemenskapen finns i EU:s lufttrafikförordning¹. Med lufttrafik avses enligt förordningen en flygning eller serie flygningar för befordran av passagerare, gods, och/eller post som utförs mot ersättning och/eller hyra. Ett företag definieras i förordningen som en fysisk eller juridisk person, oavsett om verksamheten bedrivs i vinstsyfte eller inte. Med företag kan enligt förordningen även avses ett officiellt organ, oavsett om det har självständig status som juridisk person eller inte.

11.1.1 Olika former av kommersiell luftfart för befordran av passagerare

Den kommersiella luftfarten för transport av passagerare brukar delas in i reguljärflyg och charterflyg. Med reguljärflygning avses luftfart som regelbundet trafikerar vissa flyglinjer. Vid en reguljärflygning köper passagerarna en plats, flygstol, på ett flygplan i linjetrafik. Med charterflygning avses i stället oregelbunden luftfart. Charterflygningarna går således endast under en viss säsong, beroende på res-

¹ Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen, vanligen benämnd EU:s lufttrafikförordning.

målets karaktär. En charterflygning innebär dessutom vanligtvis att ett helt flygplan hyrs och används som en del av en paketresa, i vilken resa, boende och eventuellt mat m.m. säljs i ett paket. Ett flygplan kan dock chartras även för att utföra en enstaka flygresa.

Traditionellt har researrangörer hyrt flygplan och besättning från ett flygbolag för att utföra en eller flera charterflygningar. Numera äger ofta de stora researrangörerna även flygbolagen som utför charterflygningar. Skillnaden mellan charterflyg och reguljärflyg har också blivit mindre, då researrangörerna sedan ett antal år ofta säljer flygstolar i charterflygningarna. Skillnaden är dock att charterflygningar inte ingår i systemet för flygbokningar direkt hos luftrafikföretagen utan att biljetter säljs via arrangörer och resebyråer.

Det finns även så kallad taxiflygning, som innebär att hela flygplan eller helikoptrar hyrs ut tillfälligtvis för transport av passagerare eller gods på uppdrag av företagsledningar, artister osv. Med taxiflygning avses i detta sammanhang icke regelbunden luftfart med ett mindre luftfartyg, som är typgodkänt för befordran av högst tio passagerare. Vid taxiflygning med passagerare väljs destinationsorten av den som har beställt transporten.

11.1.2 Tillstånd att bedriva passagerarflygtrafik

För att få utföra lufttransporter mot betalning åt allmänheten krävs som huvudregel ett *drifttillstånd* (AOC – air operator certificate). Detta regleras i svensk rätt i 7 kap. 1 § luftfartslagen (2010:500). Grundkravet på drifttillstånd finns även reglerat i den s.k. Easaförordningen² samt i den tillhörande tillämpningsförfordningen, vanligen benämnd Easa-ops³. Drifttillståndet är ett flygsäkerhetsmässigt godkännande som intygar att tillståndsinnehavaren har de yrkesmässiga kunskaper och den organisation som krävs för att på ett betryggande sätt sköta den verksamhet som anges i tillståndet. Ett drifttillstånd gäller för viss typ av luftfart och för vissa luftfartyg.

² Europaparlamentets och rådets förordning (EG) nr 216/2008 av den 20 februari 2008 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av en europeisk byrå för luftfartssäkerhet, och om upphävande av rådets direktiv 91/670/EEG, förordning (EG) nr 1592/2002 och direktiv 2004/36/EG.

³ Kommissionens förordning (EU) nr 965/2012 av den 5 oktober 2012 om tekniska krav och administrativa förfaranden i samband med flygdrift enligt Europaparlamentets och rådets förordning (EG) nr 216/2008.

Kravet på drifttillstånd gäller även för utländska rättssubjekt vid luftfart inom svenskt område och för svenska rättssubjekt vid luftfart utanför Sverige. Drifttillstånd utfärdas i Sverige av Transportstyrelsen och kan erhållas av staten, kommuner och landsting, privatpersoner samt olika former av bolag, föreningar, stiftelser och samfund. I fråga om ett utländskt rättssubjekt som är hemmahörande i ett annat land som är medlem i Internationella civila luftfartsorganisationen (Icao) eller i ett land som Sverige träffat avtal med om rätt till luftfart inom svenskt område, godtas ett drifttillstånd eller en likvärdig handling som har utfärdats av det landet i enlighet med Icao:s normer.

Drifttillstånd krävs således för att få utföra lufttransporter mot betalning åt allmänheten oavsett om det handlar om reguljärflyg, charterflyg eller taxiflyg. Begreppet allmänheten ska tolkas vitt, vilket innebär att i stort sett alla som inte ingår i utövarens närmaste bekantskapskrets innefattas. Vidare är det tillräckligt att det har avtalats om att någon form av betalning ska utgå för att en lufttransport ska vara tillståndspliktig. Det föreligger således inget krav på vinst eller vinstsyfte. Det finns inte heller något krav på att en verksamhet ska ha en viss omfattning för att den ska vara tillståndspliktig, utan en enda flygning kan medföra tillståndsplikt. (Se prop. 2009/10:95 s. 342.)

Beträffande luftfart inom EU krävs det utöver drifttillstånd även en *operativ licens* enligt EU:s lufttrafikförordning. I förordningen anges vilka krav som ska uppfyllas av lufttrafikföretag som bedriver vissa slag av kommersiell flygtrafik inom gemenskapen. Bl.a. krävs att företaget har ett drifttillstånd. Det görs även en prövning av om företaget uppfyller vissa finansiella villkor och försäkringskrav. Ett företag som uppfyller förordningens krav har rätt att få en operativ licens, vilket är ett tillstånd för företaget att mot betalning utföra lufttransport av passagerare, post eller gods som anges i licensen. Inget företag som är etablerat i gemenskapen, dvs. har sitt säte i ett land inom EU, får mot ersättning eller hyra utföra lufttransporter av bl.a. passagerare om de inte har beviljats den nödvändiga operativa licensen. Från kravet på innehav av giltig operativ licens undantas lufttrafik som utförs med icke-motordrivna luftfartyg och/eller ultralätta motordrivna luftfartyg samt lokala flygningar. Licensen har karaktären av ett näringspolitiskt tillstånd. En operativ licens ger inte i sig tillgång till särskilda flyglinjer eller marknader.

En operativ licens enligt EU:s luftrafikförordning utfärdas av nationella tillståndsmyndigheter för företag som är etablerade i gemenskapen. I Sverige är Transportstyrelsen tillståndsmyndighet. För närvarande har totalt 31 operativa licenser utfärdats i Sverige för både svenska och utländska företag. Vissa av dessa är tämligen stora aktörer som flyger i internationell trafik från de stora flygplatserna, t.ex. SAS Sverige AB, genom konsortiet SAS, eller TUIfly Nordic AB. Andra innehavare av svenska operativa licenser är avsevärt mindre. Roslagens Helikopterflyg AB är ett exempel på en mindre aktör och kommunalförbundet Svensk luftambulans ett annat.

När det gäller flygföretag som är etablerade i EU och som enbart flyger på destinationer utanför EU framgår inte uttryckligen av förordningen om dessa behöver ha en operativ licens. Eftersom den operativa licensen inte ger tillträde till marknaden utan är ett grundläggande villkor för verksamheten som flygbolag, synes dock alla medlemsstater acceptera att en operativ licens även är ett krav för att bedriva transporter mellan EU och tredjeland. (Se prop. 2009/10:95 s. 232.) Operativa licenser, eller motsvarande, utfärdas dock även av länder utanför EU.

Frågan om tillträde till flyglinjer inom unionen, för såväl regelbunden som icke regelbunden luftrafik, regleras i kap. II i luftrafikförordningen. Enligt förordningen ska berörda medlemsstater tillåta luftrafikföretag med giltig operativ licens utfärdad av en behörig tillståndsmyndighet inom unionen att utöva trafikrättigheter, däribland befordran av passagerare, på flyglinjer inom EU. Således krävs inte något särskilt trafiktillstånd för tillträde till flyglinjer inom unionen för de luftrafikföretag som har en giltig operativ licens utfärdad inom EU. När det gäller luftfart som inte omfattas av EU:s luftrafikförordning, eftersom den avser inrikestrafik, trafik till tredje länder eller utförs av sådana luftrafikföretag som inte har en giltig operativ licens utfärdad i ett land inom EU, kan det dock utöver ett drifttillstånd även krävas ett *trafiktillstånd* enligt 7 kap. 10 § luftfartslagen för att mot betalning få utföra lufttransporter åt allmänheten. Ett trafiktillstånd är trafikpolitiskt motiverat och ger tillträde till linjer eller marknader. Trafiktillståndet kan ges till såväl svenska som utländska operatörer och kan avse såväl regelbunden som icke regelbunden trafik. Trafiktillstånd lämnas av regeringen eller Transportstyrelsen. I TSFS 2010:168 finns Transportstyrel-

sens föreskrifter om bl.a. trafiktillstånd. När det gäller charter- och taxiflygning finns särskilda föreskrifter i TSFS 2011:104.

11.1.3 Luftrafikföretagens resor till och från Sverige

År 2016 utförde sammanlagt 240 luftrafikföretag flygningar för befordran av passagerare till eller från Sverige antingen i linjefart eller som charterflyg. Av dessa flygbolag utförde 100 stycken fem eller färre sådana resor. Därtill utfördes sådana utlandsresor av upp till 87 olika taxiflygbolag.⁴ Den senare uppgiften är osäker eftersom det inte finns något system som registrerar persontransporter med taxiflyg.⁵

Resorna gick till någon av landets många flygplatser. Det finns i dag 38 flygplatser i landet med reguljär trafik i form av linjefart eller charterflyg. Vid sidan av dessa finns ett betydande antal flygplatser av varierande standard. Taxiflygen behöver inte nödvändigtvis använda sig av flygplatser som är öppna och bemannade.⁶

11.2 Luftrafikföretagens insamlande av PNR-uppgifter

Det finns i dag inte någon uttrycklig författningsreglering om att luftrafikföretag ska inhämta PNR-uppgifter om sina passagerare. Gällande bestämmelser på området ålägger dock luftrafikföretagen att på luftfartygen medföra en passagerarlista med namn på sina passagerare. Alla luftfartyg som utför internationella passagerarflygningar ska således ha med sig en passagerarlista som inkluderar passagerarnas avrese- och destinationsorter. Detta följer av artikel 29 i Chicago-konventionen. Även av Easa-ops följer en skyldighet att medföra passagerarlistor vid kommersiella luftransporter. Enligt förordningen ska flygoperatören också se till att information som är relevant för flygningen och arten av verksamhet bevaras på marken. Det finns dock inte något uttalat krav på att just passagerarlistorna ska bevaras

⁴ Enligt Transportstyrelsens statistikuppgifter.

⁵ Se t.ex. SOU 2016:83 s.143.

⁶ Se a.a. s. 65 f. och 143.

på marken. I förordning (EU) nr 996/2010⁷ behandlas frågor om utredning och förebyggande av flygolyckor. I förordningens artikel 20 anges att unionens flygbolag som ankommer till eller avgår från, och flygbolag från tredjeländer som avgår från, en flygplats belägen på territorierna i de medlemsstater som omfattas av fördragen, ska införa rutiner som gör det möjligt att så snart som möjligt och senast inom två timmar från underrättelsen om att ett luftfartyg har råkat ut för en olycka, ta fram en validerad förteckning, baserad på bästa tillgängliga uppgifter, över alla personer ombord. För att kunna göra en sådan förteckning torde fordras att uppgifter om resenärerna på något sätt finns sparade på marken.

Enligt 15 § TSFS 2011:104 ska vid charterflygningar en förteckning över passagerare förvaras av det företag som utför flygningen och lämnas till Transportstyrelsen på begäran. För taxiflygningarna finns inte någon motsvarande bestämmelse i föreskrifterna om att det ska finnas en förteckning över passagerare.

De luftrafikföretag som utför reguljärflygningar samlar i dag in PNR-uppgifter om sina passagerare. Uppgifterna vidarebefordras ofta från resebyråer eller researrangörer via olika bokningssystem. Uppgifterna kan även lämnas av passagerarna själva när de bokar eller köper flygresor direkt av luftrafikföretaget, exempelvis via en hemsida. Luftrafikföretagen samlar in PNR-uppgifterna för sina egna operativa och kommersiella syften. Därför kan omfattningen av de insamlade uppgifterna samt de insamlade uppgifternas karaktär variera stort mellan luftrafikföretagen och mellan olika passagerare. I vissa fall kan PNR-uppgifterna bestå endast av namn, resväg, viss allmän information och ett biljettnummer. I andra fall kan PNR-uppgifterna även innehålla exempelvis kontakt- och kreditkortsuppgifter samt uppgifter om att någon särskild service kommer att behövas under resan. Bokningssystemen kan tillhandahållas av olika systemleverantörer, som är de som normalt överför uppgifterna till de nationella myndigheter som kräver tillgång till uppgifterna.

De luftrafikföretag som är specialiserade på charterflygningar samlar oftast inte in egna PNR-uppgifter. De uppgifter som behövs för att utföra en flygning, såsom namn och flygnummer, överförs i

⁷ Europaparlamentets och rådets förordning (EU) nr 996/2010 av den 20 oktober 2010 om utredning och förebyggande av olyckor och tillbud inom civil luftfart och om upphävande av direktiv 94/56/EG.

sådant fall till dem från researrangören inför flygresan. Övriga PNR-uppgifter, som passagerarna lämnat i samband med resebokningen, finns kvar hos researrangören. Vid flygningar till tredjeland skickas dock ett API-meddelande till flygbolaget, som i sin tur vidarebefordrar meddelandet till myndigheten i ankomstlandet. Meddelandet innehåller namn, födelsetid, nationalitet på pass och passnummer samt ett bokningsnummer.

De mindre lufttrafikföretag som utför taxifygningar samlar i de flesta fall inte in uppgifter om sina passagerare på ett systematiskt sätt. De insamlade uppgifterna kan i vissa fall bestå av endast en namnuppgift som noteras för hand eller i ett excelformulär.

11.3 Vilka lufttrafikföretag ska åläggas en skyldighet att överföra PNR-uppgifter?

Våra förslag: PNR-uppgifter ska enligt lagen överföras från lufttrafikföretag som har en giltig operativ licens eller motsvarande som ger rätt att mot vederlag utföra lufttransporter av passagerare, och som i sin normala verksamhet samlar och hanterar PNR-uppgifter i reservationssystem.

Reservationssystem ska i lagen definieras som system där PNR-uppgifter samlas för hantering av reservationer.

Direktivets definition av ett lufttrafikföretag, innebärandes ett sådant företag med operativ licens eller motsvarande som ger rätt att bedriva passagerarflygtrafik, innefattar alla företag som utför lufttransport av passagerare mot betalning eller hyra så länge de har den angivna licensen. I begreppet företag innefattas enligt vår bedömning, på samma sätt som enligt lufttrafikförordningen, både fysiska och juridiska personer samt officiella organ. Enligt lufttrafikförordningen undantas från kravet på operativ licens endast lufttrafik som utförs med icke-motordrivna luftfartyg och/eller ultralätta motordrivna luftfartyg samt lokala flygningar. Alla övriga företag som utför lufttransporter mot betalning eller hyra inom unionen ska således ha en operativ licens och träffas därmed av PNR-direktivet. Således omfattas charterflygningarna av direktivets definition, även i de fall charterbolagen äger sina egna flygplan. Även taxifygen omfattas av direktivets definition. Således träffas också taxifygföretagen rent

definitionsmissigt av direktivets överföringsskyldighet när de mot ersättning eller hyra utför lufttransporter med hjälp av mindre flyg eller helikopter över ett lands gränser. Med tillägget ”eller motsvarande” innefattas i definitionen även de luftrafikföretag som inte har en operativ licens utfärdad i ett land inom EU men som har en motsvarande licens från ett tredjeland.

Begreppet luftrafikföretag har definierats på olika sätt i olika svenska författningar. Exempelvis definieras begreppet i TSFS 2010:68 som ett flygföretag med ett giltigt drifttillstånd (AOC). I TSFS 2011:104 definieras däremot ett luftrafikföretag som ett flygföretag med giltigt drifttillstånd och i förekommande fall operativ licens eller motsvarande. Även i de EU-rättsliga förordningarna på området finns det olika definitioner av begreppet. I exempelvis förordning (EG) nr 261/2004⁸ definieras ett luftrafikföretag endast som ett luftrafikföretag med en giltig licens. I luftrafikförordningen är dock definitionen av ett luftrafikföretag ungefärligen densamma som i PNR-direktivet, dvs. ett företag med giltig operativ licens eller motsvarande.

Det saknas således enhetlighet i definitionerna av begreppet luftrafikföretag. Med hänsyn härtill bör, enligt vår mening, PNR-direktivets definition av begreppet införas i den nya lag som vi föreslår. En sådan lösning synes även lämplig eftersom direktivets definition innehåller en upplysning om kravet på en operativ licens. I detta ligger även ett krav på att luftrafikföretaget har ett giltigt drifttillstånd. Definitionen omfattar således såväl ett giltigt operativt tillstånd som ett drifttillstånd. Genom tillägget ”eller motsvarande” innefattas även sådana utländska luftrafikföretag som inte har en operativ licens utfärdad i ett land inom EU men som har en motsvarande licens från ett tredjeland. Av lagens definition bör också framgå att licensen ska ge rätt att bedriva passagerarflygtrafik, dvs. ge rätt att mot betalning eller hyra, dvs. vederlag, utföra lufttransporter av passagerare.

För att direktivets bestämmelser om överföring av PNR-uppgifter ska bli tillämpliga för luftrafikföretagen förutsätts, förutom att företagen träffas av direktivets definition av ett luftrafikföretag, att de

⁸ Europaparlamentets och rådets förordning (EG) nr 261/2004 av den 11 februari 2004 om fastställande av gemensamma regler om kompensation och assistans till passagerare vid nekad ombordstigning och inställda eller kraftigt försenade flygningar och om upphävande av förordning (EEG) nr 295/91.

samlar in PNR-uppgifter som en del av sin normala verksamhet. Denna avgränsning framgår av artikel 8.1. Att uppgifterna ska samlas in som en del av företagets normala verksamhet (på eng. *normal course of their business*) får tolkas som att insamlingen ska ingå som en naturlig del i företagets verksamhet. Insamlingen ska således vara något som företaget redan gör. För det fall företaget inte samlar in PNR-uppgifter i dag, kan överföringsskyldigheten dock inträda i samband med att företaget påbörjar en sådan insamling. Som har angetts ovan ålägger direktivet inte lufttrafikföretagen att inhämta ytterligare uppgifter eller några uppgifter alls om sina passagerare. Vad direktivet handlar om är i stället att redan insamlade uppgifter ska lämnas ut för ny användning i brottsbekämpande syfte. Den grundläggande skyldigheten att överföra PNR-uppgifter enligt direktivet bör därmed inte utsträckas till att avse sådana lufttrafikföretag som inte normalt befattar sig med PNR-uppgifter på det sätt som avses i direktivet.

Definitionen av PNR-uppgifter i artikel 3.5 synes syfta till en systematisk behandling av uppgifter om passagerare via ett reservationssystem, ett avgångskontrollsystem som används för att checka in passagerare på flygningar eller likvärdiga system med liknande uppgifter. Med ett reservationssystem avses enligt artikel 3.6 lufttrafikföretagens interna system, där PNR-uppgifter samlas för hantering av reservationer. Sammanställningen av för resan nödvändiga uppgifter om varje enskild passagerare ska, enligt artikel 3.5, göra det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen för varje resa. Av artikel 8.3 b framgår vidare att lufttrafikföretagen ska ha tillgång till en gate som passagerarna ska passera på vägen till flygplanet, varefter den andra omgången PNR-uppgifter ska överföras. Tanken bakom PNR-direktivet synes således vara att PNR-uppgifterna ska överföras från större aktörer, som normalt samlar in PNR-uppgifter från sina passagerare för operativa och kommersiella ändamål, systematiskt behandlar dem i reservationssystem, avgångskontrollsystem eller likvärdiga system samt själva eller genom en mellanman sköter ombordstigningen på flygplanen genom en gate.

De lufttrafikföretag som utför charterflygningar innehar i många fall endast en mindre mängd PNR-uppgifter. De uppgifter som de innehar behandlas dock oftast systematiskt i företagets datorsystem. Behandlingen av PNR-uppgifter får därmed anses ingå som en normal

del i dessa företags verksamhet. Ombordstigningen på flygplanen sker, i de flesta fall, genom en gate och hanteras elektroniskt på samma sätt som för reguljärflygningarna. Några problem med hänsyn till direktivets överföringstidpunkter föreligger därför i normalfallet inte. Enligt vår bedömning omfattas således, som utgångspunkt, de luftrafikföretag som utför charterflygningar av direktivets överföringsskyldighet.

De luftrafikföretag som utför taxiflygningar saknar emellertid i många fall strukturmässigt system för behandling av PNR-uppgifter i den mening som avses i direktivet. De namnuppgifter som samlas in för att uppfylla kravet på innehav av passagerarlistor antecknas i vissa fall endast manuellt eller med hjälp av excelblad. Någon sådan datoriserad behandling och kontroll av reservationer som avses i direktivet förekommer generellt inte. På mindre flygstationer saknas dessutom gater och incheckningen sker därför manuellt. Den i direktivet angivna skyldigheten att överföra PNR-uppgifter omedelbart efter det att gatens dörrar har stängts synes därmed svår att uppfylla.

Enligt vår bedömning behandlar inte dessa mindre taxiflygföretag PNR-uppgifter på det sätt som avses i direktivet. De bör således inte träffas av överföringsskyldigheten enligt vårt lagförslag. För dessa aktörer får efterfrågade passageraruppgifter i stället begäras in med stöd av de gällande bestämmelserna för transportföretag i polislagen och i tullagstiftningen, som vi därför ser anledning att behålla för sådan luftrafik som utförs av företag som inte kommer att omfattas av skyldigheter enligt den nya lagen för PNR-uppgifter.

För att närmare ringa in de luftrafikföretag som ska åläggas en grundläggande skyldighet att överföra PNR-uppgifter enligt vårt lagförslag bör således ett tillägg göras till definitionen av ett luftrafikföretag. Detta tillägg bör innebära att luftrafikföretaget i sin normala verksamhet ska samla och hantera PNR-uppgifter i reservationssystem. Genom en sådan skrivning faller de luftrafikföretag som strukturmässigt saknar sådana system för behandling av PNR-uppgifter utanför överföringsskyldigheten. En definition av ett reservationssystem bör också föras in i lagen. Definitionen bör utformas på ungefär samma sätt som direktivets definition. För att inte utesluta de luftrafikföretag som låter en tredjepart hantera PNR-uppgifterna bör det dock vara tillräckligt att i definitionen ange att med reservationssystem avses sådana system där PNR-uppgifter samlas för hantering av reservationer.

11.4 Överföring av PNR-uppgifter till enheten för passagerarinformation

11.4.1 Omfattningen av vårt uppdrag

Vårt förslag: Den nationella regleringen ska innehålla bestämmelser om lufttrafikföretagens överföring av PNR-uppgifter bara till den svenska enheten för passagerarinformation.

Av PNR-direktivets artikel 8.1 följer att medlemsstaterna ska anta de åtgärder som är nödvändiga för att se till att lufttrafikföretag överför vissa i direktivet angivna PNR-uppgifter till databasen hos enheten för passagerarinformation i den medlemsstat på vars territorium flygningen kommer att ankomma till eller varifrån flygningen kommer att avgå. Det anges inte uttryckligen vilka delar av direktivet som det åligger varje medlemsstat att lagstifta om. Tanken bakom direktivet är dock att det i samtliga rättsordningar i de EU-länder som är bundna av direktivet ska finnas en harmoniserad skyldighet för lufttrafikföretagen att överföra PNR-uppgifter till såväl avgångslandets som ankomstlandets nationella enhet för passagerarinformation. Med tanke på att varje medlemsstat ska genomföra direktivet i sin rättsordning ser vi det som den enda rimliga lösningen att det svenska genomförandet ska begränsas till passagerartrafik som berör Sverige och svenska flygplatser. Det medför att den av oss föreslagna lagen inte reglerar skyldigheten för ett lufttrafikföretag som flyger mellan Italien och Egypten att överföra PNR-uppgifter till den italienska enheten. Något annat skulle vara orimligt och leda till dubbelreglering många gånger om inom EU.

Vad gäller flygtrafiken inom EU, som också ska omfattas av den nya lagen (se avsnitt 11.4.2), kan man också fråga sig vad den svenska regleringen bör ta sikte på. Enligt direktivet ska ett lufttrafikföretag som ska företa en flygresa från Sverige till exempelvis Frankrike överföra sina PNR-uppgifter dels till den svenska enheten för passagerarinformation, dels till den franska enheten. Likaså ska lufttrafikföretaget inför en resa från Frankrike till Sverige överföra PNR-uppgifterna till både den franska och den svenska enheten för passagerarinformation. Vi ser det som vår uppgift att reglera lufttrafikföretagets skyldighet att överföra PNR-uppgifter till den svenska enheten för passagerarinformation. Lufttrafikföretagets skyl-

dighet att överföra uppgifterna till den franska enheten för passagerarinformation får regleras genom Frankrikes genomförande av direktivet. Även här ser vi detta som en nödvändig begränsning för att undvika framtida tillämpningssvårigheter för luftrafikföretagen. Våra förslag till lag och förordning kommer således att innehålla bestämmelser om luftrafikföretagens överföring till den svenska enheten för passagerarinformation.

11.4.2 Överföring av uppgifter avseende flygresor både inom och utom EU

Våra förslag: Luftrafikföretag ska inför varje flygning ankommande till eller avgående från Sverige överföra PNR-uppgifter till enheten för passagerarinformation.

Om flygningens linjebeteckning delas med ett eller flera andra luftrafikföretag, ska det luftrafikföretag som utför flygningen överföra PNR-uppgifter om samtliga passagerare.

Överföring inför flygningar till och från EU

Enligt artikel 8.1 ska medlemsstaterna anta de åtgärder som är nödvändiga för att se till att luftrafikföretag överför vissa i direktivet angivna PNR-uppgifter i samband med flygningar utanför EU. Med flygning utanför EU avses i direktivet flygningar mellan ett land inom EU och ett land utanför EU (jfr artikel 3.2). Inför sådana flygningar ska enligt bestämmelsen PNR-uppgifter överföras till databasen hos enheten för passagerarinformation i den medlemsstat på vars territorium flygningen kommer att ankomma eller från det territorium varifrån flygningen kommer att avgå. Om flygningens linjebeteckning delas med ett eller flera andra luftrafikföretag ska, enligt bestämmelsen, det företag som utför flygningen ha skyldighet att överföra PNR-uppgifter om samtliga passagerare ombord.

Gemensam linjebeteckning, s.k. code sharing, är en form av samarbete mellan flygbolag. Det innebär att ett flygbolag sätter sin egen bolagskod på en flygning som genomförs av ett annat flygbolag. Detta är ett sätt för flygbolagen att genom samarbete med andra flygbolag utvidga sitt linjenät och marknadsföra sig på linjer de inte själva

flyger. Enligt direktivet vilar i sådant fall ansvaret för att PNR-uppgifterna överförs på det lufttrafikföretag som utför flygningen.

I artikel 8.1 anges vidare att för det fall en flygning utanför EU omfattar en eller flera mellanlandningar på medlemsstaternas flygplatser, ska lufttrafikföretagen överföra PNR-uppgifter för alla passagerare till enheterna för passagerarinformation i alla berörda medlemsstater. Detta gäller även om en flygning inom EU innebär en eller flera mellanlandningar på olika medlemsstaters flygplatser, men endast i fråga om medlemsstater som samlar in PNR-uppgifter från flygningar inom EU. Som angetts i avsnitt 3.3 kommer Danmark inte att tillämpa direktivet, varför detta inte medför någon skyldighet för lufttrafikföretagen att överföra PNR-uppgifter dit. I övrigt ska alltså PNR-uppgifter överföras till samtliga medlemsstater där en flygning startar, landar eller eventuellt mellanlandar.

Överföring även inför flygningar inom EU

Direktivet ålägger således lufttrafikföretagen att överföra PNR-uppgifter om passagerare på flygningar som anländer från eller avgår till ett land utanför EU. Av artikel 2.1 framgår att medlemsstaterna därutöver på frivillig grund kan tillämpa direktivet även på flygningar inom EU. Sverige och övriga medlemsstater som är bundna av direktivet har förklarat att de har för avsikt att tillämpa direktivet även för flygresor inom EU. Sverige kommer att skriftligen meddela kommissionen detta. Kommissionen ska därefter offentliggöra detta meddelande i Europeiska unionens officiella tidning (EUT). När ett sådant meddelande har lämnats, ska, enligt artikel 2.2, alla bestämmelser i direktivet gälla för flygningar inom EU som om de vore flygningar utanför EU och för PNR-uppgifter från flygningar inom EU som om de vore PNR-uppgifter från flygningar utanför EU. Det som ovan angetts om överföring av PNR-uppgifter från lufttrafikföretagen kommer således även gälla flygningar inom EU.

Direktivet ska genomföras i medlemsstaterna senast den 25 maj 2018. Kommissionen har angett att den endast kommer att offentliggöra meddelanden om att en medlemsstat ska tillämpa direktivet även för flygresor inom EU, om staten även har underrättat kommissionen om att den har genomfört direktivets övriga bestämmelser i enlighet med artikel 18.1. Enligt kommissionen kommer således ett

meddelande från en medlemsstat om att den ska tillämpa direktivet även för flygresor inom EU att få rättslig verkan först när hela direktivet är genomfört i medlemsstaten. Vidare har kommissionen angett att det är tillräckligt att direktivet är genomfört i den medlemsstat som PNR-uppgifterna ska överföras till för att ett lufttrafikföretag ska vara skyldigt att överföra PNR-uppgifter dit. Huruvida den medlemsstat där lufttrafikföretaget har sitt säte ännu har genomfört direktivet eller lämnat meddelanden om detta till kommissionen saknar således betydelse för överföringsskyldigheten.⁹

För Sveriges del innebär det ovanstående att lufttrafikföretagen, när direktivet är genomfört här och kommissionen är informerad om detta och om att Sverige ska tillämpa direktivet även på flygningar inom EU, ska överföra PNR-uppgifter till den svenska enheten för passagerarinformation inför alla utrikesresor ankommande till eller avgående från Sverige.

Våra överväganden

En utgångspunkt för vårt uppdrag är att direktivet ska tillämpas även för flygningar inom EU och att detta ska genomföras vid samma tidpunkt som direktivet i övrigt ska vara införlivat i svensk rätt. Det bör därför av vår reglering framgå att överföringar av PNR-uppgifter till enheten för passagerarinformation ska ske såväl inför resor till och från länder utanför EU som inför resor inom EU. Detta kan uttryckas som att överföringar ska ske inför varje flygning ankommande till eller avgående från Sverige. Vidare bör det av regleringen framgå att om flygningens linjebeteckning delas med ett eller flera andra lufttrafikföretag, ska det lufttrafikföretag som utför flygningen överföra PNR-uppgifter om samtliga passagerare. Bestämmelserna, som innebär skyldigheter för enskilda lufttrafikföretag, bör föras in i lag.

⁹ Se Ref. Ares (2017) 68233 – 06/01/2017.

11.4.3 PNR-uppgifter och passagerare

Våra förslag: PNR-uppgifter, eller flygpassageraruppgifter, ska i lagen definieras som en sammanställning av uppgifter om varje enskild passagerare som gör det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen.

Passagerare ska definieras som alla personer, förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan och som finns upptagna i passagerarförteckningen.

Med PNR-uppgifter, eller passageraruppgiftssamling, avses enligt artikel 3.5 en sammanställning av för resan nödvändiga uppgifter om varje enskild passagerare som gör det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen för varje resa som bokas av en person eller för en persons räkning, oavsett om uppgifterna finns i reservationssystemet, i avgångskontrollsystemet som används för att checka in passagerare på flygningar eller i likvärdiga system med motsvarande uppgifter (på eng. *functionalities*). Med passagerare avses enligt artikel 3.4 alla personer, inbegripet personer i transfer eller transit, som transporteras eller ska transporteras med ett flygplan med lufttrafikföretagets godkännande. Detta godkännande ska framgå av att personen står med i passagerarförteckningen. Från begreppet passagerare exkluderas besättningsmedlemmar.

Definitioner av begreppen PNR-uppgifter och passagerare bör föras in i lagen. Definitionerna bör utformas i nära anslutning till direktivets ordalydelse. För att inte i onödan tynga texten bör dock något kortare definitioner användas. Således bör passagerare definieras som alla personer, förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan och som finns upptagna i passagerarförteckningen. PNR-uppgifter bör i lagen definieras som en sammanställning av uppgifter om varje enskild passagerare som gör det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen. Med PNR-uppgifter avses detsamma som flygpassageraruppgifter.

11.4.4 PNR-uppgifter som ska överföras

Våra förslag: Samtliga de PNR-uppgifter som ska överföras ska framgå av en bilaga till lagen. PNR-uppgifterna ska dock endast överföras i de fall lufttrafikföretagen samlar in uppgifterna som en del av sin normala verksamhet.

API-uppgifter ingår bland de uppgifter som ska överföras. I den anslutande förordningen regleras att dessa ska överföras även om de inte lagras eller annars behandlas med hjälp av samma tekniska metoder som andra PNR-uppgifter.

PNR-uppgifter som omfattas av direktivet

En förteckning över de PNR-uppgifter som ska överföras till enheterna för passagerarinformation återfinns i bilaga I till direktivet. Lufttrafikföretagen ska dock enligt artikel 8.1 endast överföra dessa uppgifter för det fall de redan har samlat in dem som en del av sin normala affärsverksamhet. Direktivet ålägger alltså inte lufttrafikföretagen att inhämta ytterligare uppgifter eller några uppgifter alls om sina passagerare och medför inte någon skyldighet för passagerare att tillhandahålla några uppgifter utöver dem som redan tillhandahålls lufttrafikföretagen. Vad direktivet handlar om är således att redan insamlade uppgifter ska lämnas ut för ny användning i brottsbekämpande syfte.

Förteckningen i bilaga I har enligt skäl 15 till syfte att återspegla de offentliga myndigheternas legitima krav på att kunna förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten i EU, samtidigt som grundläggande rättigheter skyddas, särskilt rätten till privatlivet och rätten till skydd av personuppgifter. Vid framtagandet av förteckningen har EU-stadgan, dataskyddskonventionen¹⁰ samt Europakonventionen¹¹ beaktats. Det anges vidare att förteckningen inte är avsedd att grundas på en persons ras eller etniska ursprung, religion eller övertygelse, politiska eller annan åskådning, medlemskap i fack-

¹⁰ Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter.

¹¹ Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

förening, hälsotillstånd, sexualliv eller sexuella läggning. De i förteckningen angivna PNR-uppgifterna ska endast omfatta sådan information om passagerarens bokning och resrutt som gör det möjligt för de behöriga myndigheterna att identifiera flygpassagerare som utgör ett hot mot den inre säkerheten.

Förteckningen över PNR-uppgifter i bilagan omfattar 19 punkter. Uppräkningen innefattar exempelvis datum för bokning/utfärdande av biljett, namn, adress och kontaktuppgifter. *PNR-uppgifternas lokaliseringskod* enligt punkten 1 avser en kod innehållande siffror och bokstäver som är specifik för en särskild resenärs resa. Koderna är detsamma som ett boknings- eller reservationsnummer. Med *delade PNR-uppgifter* enligt punkten 11 avses en uppgift om att det tidigare har funnits ytterligare resenärer med samma lokaliseringskod. När delade PNR-uppgifter finns har alltså inledningsvis två passagerare eller fler haft en gemensam bokning, men en eller flera har gjort ombokningar. Vid en ombokning får de utvalda passagerarna en ny lokaliseringskod.

I punkten 12 i bilagan anges ”Allmänna anmärkningar (inklusive alla tillgängliga uppgifter om ensamkommande barn under 18 år, såsom namn och kön, ålder, språkkunskaper, namn och kontaktuppgifter för den person som följer barnet till incheckning för avresan och denna persons förhållande till barnet, namn och kontaktuppgifter för den person som hämtar barnet vid ankomsten och denna persons förhållande till barnet samt flygplatsanställd som ledsagar barnet vid avresan respektive ankomsten)”. Uppgifterna om barn som reser utan vuxet sällskap är här särskilt angivna eftersom de kan ha betydelse vid utredningar om människosmuggling. *Allmänna anmärkningar* utgör ett fritextsfält för kommunikation mellan t.ex. resebokare och flygbolagspersonal. Bland de allmänna anmärkningarna kan finnas uppgifter om exempelvis cykel med ombord, specialkost, funktionshinder m.m. Användningen av fritextsfältet för allmänna anmärkningar kan innebära att känsliga personuppgifter behandlas. Denna fråga kommer vi att återkomma till i avsnitt 18.5.

Även API-uppgifter omfattas

I punkten 18 i bilagan anges eventuell förhandsinformation (API), som samlats in. Som exempel på API-uppgifter anges typ av identitetshandling, identitetshandlingens nummer, utfärdandeland och sista giltighetsdag, efternamn, förnamn, kön, födelsedatum, luftrafikföretag, flygnummer, utresedatum, ankomstdatum, avresehamn, ankomsthavn, avresetid och ankomsttid. Nationalitet ingår numera även i den svenska exemplifieringen, sedan direktivet rättats på den punkten.

Vissa luftrafikföretag lagrar insamlade API-uppgifter som en del av PNR-uppgifterna, andra gör det inte. Att använda PNR-uppgifter tillsammans med API-uppgifter anges i skäl 10 tillföra ett mervärde, genom att det hjälper medlemsstaterna att kontrollera en individs identitet, vilket ökar PNR-uppgifternas betydelse för brottsbekämpningen och minimerar risken för att man kontrollerar och utreder oskyldiga personer. I artikel 8.2 anges därför att om luftrafikföretagen har samlat in sådana API-uppgifter om passagerare som förtecknas i punkten 18 i bilagan, men inte lagrar denna information med hjälp av samma tekniska metoder som för andra PNR-uppgifter, ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att luftrafikföretagen överför även dessa uppgifter till enheten för passagerarinformation i de medlemsstater som avses i artikel 8.1. Direktivets samtliga bestämmelser ska vara tillämpliga även vid överföring av de uppgifterna.

Våra överväganden

Det bör av lagen framgå vilka PNR-uppgifter som omfattas av luftrafikföretagens överföringsskyldighet. Vidare bör det av lagen framgå att PNR-uppgifterna endast ska överföras i de fall luftrafikföretagen samlar in uppgifterna som en del av sin normala verksamhet.

En förteckning över de PNR-uppgifter som omfattas kan föras in i en bilaga till lagen. En hänvisning endast till den bilaga till direktivet där PNR-uppgifterna framgår har inte bedömts lämplig med hänsyn till att den svenska versionen av bilagan har rättats och i övrigt innehåller vissa oklarheter i översättningen. Vi föreslår således att det till lagen fogas en bilaga som listar de PNR-uppgifter som anges i bilaga I till direktivet, med följande justeringar.

I punkten 7 har vi valt att byta ut uttrycket *hela resrutten för aktuell passageraruppgiftssamling* som används i direktivets bilaga mot det kortare uttrycket *fullständig resplan*.

Enligt punkten 9 i direktivets bilaga ska uppgifter om resebyrå eller resebyråtjänsteman ingå bland de uppgifter som ska överföras från lufttrafikföretagen. Resebyråtjänsteman synes dock vara en felöversättning av det engelska ordet *travelagent*, som bättre bör översättas med reseagent eller researrangör. Med hänsyn härtill föreslår vi att ordet *reseagent* används i stället.

I punkten 12 i direktivets bilaga anges att så kallade allmänna anmärkningar ska ingå bland de uppgifter som ska överföras från lufttrafikföretagen. De allmänna anmärkningarna exemplifieras med tillgängliga uppgifter om *ensamkommande* barn. En bättre översättning är *ensamresande* barn, vilket är den gängse terminologin inom luftfartssektorn. Enligt utredningens mening är också *flygplatspersonal* en bättre översättning än *flygplatsanställd* enligt samma punkt, eftersom det inte torde krävas att en person är anställd av flygplatsen för att omfattas av bestämmelsen. Vi har därför valt att använda dessa uttryck.

Vidare får med eventuella API-uppgifter i punkten 18 i bilagan förstås samtliga API-uppgifter som finns tillgängliga. Således ska lufttrafikföretagen överföra alla API-uppgifter som de har samlat in (på eng. *any advance passenger information data collected*), oavsett om de upptas i exemplifieringen eller inte. Detta framgår därför i bilagan till vårt lagförslag. Vidare är enligt vår mening *avrese- och ankomstflygplats* bättre översättningar än *avrese- och ankomsthamn*. Dessa begrepp används därför i vårt förslag.

I förteckningen över vilka PNR-uppgifter som ska överföras ingår, som framkommit ovan, API-uppgifter. Någon särskild bestämmelse om att även API-uppgifter ska överföras är därför inte nödvändig i den föreslagna lagen. Däremot bör det föras in en bestämmelse om att API-uppgifter ska överföras även om dessa inte lagras eller annars behandlas av företagen med hjälp av samma tekniska metoder som för andra PNR-uppgifter. Detta kan regleras i förordning.

11.4.5 Överföringar ska ske vid två tillfällen

Våra förslag: PNR-uppgifterna ska överföras vid två tillfällen. Det första 24–48 timmar före flygningens avgång, och det andra omedelbart efter det att gatens dörrar har stängts.

Den andra överföringen får begränsas till uppdateringar och kompletteringar av de uppgifter som överfördes vid det första tillfället.

Av artikel 8.3 framgår att luftrafikföretagen ska överföra sina PNR-uppgifter vid två tillfällen. Det första tillfället då en överföring ska ske är 24–48 timmar före flygningens planerade avgång. Det andra tillfället är omedelbart efter det att gatens dörrar har stängts, det vill säga när passagerarna har stigit ombord på planet inför avgång och passagerare inte längre tillåts stiga ombord eller stiga av. Den sista överföringen av uppgifter anses vara av avgörande betydelse för brottsbekämpningen eftersom t.ex. narkotikakurirer ofta bokar sina resor sent alternativt bokar om dem. Enligt artikel 8.4 ska medlemsstaterna tillåta luftrafikföretagen att begränsa den sista överföringen till uppdateringar av de överföringar som har gjorts dessförinnan.

Direktivets bestämmelser om överföringstidpunkter bör föras in i vår lag. Bestämmelsen om att den första överföringen ska ske 24–48 timmar före flygningens planerade avgång kan tolkas som att luftrafikföretagen får välja när, inom denna tidsram, uppgifterna ska överföras. Skrivningen kan dock även tolkas som att det är upp till varje medlemsstat att bestämma när, inom denna tidsram, uppgifterna ska överföras. Som har angetts i avsnitt 4.2.1 framgår av annex 9 till Chicagokonventionen att de fördragsslutande stater som kräver tillgång till PNR-uppgifter bör anpassa sin behandling av uppgifterna och sina tekniska krav till de riktlinjer som anges i Icao:s dokument 9944 och i instruktionerna för implementering av standardformatet PNRGOV. Av artikel 2.8.2 i dokument 9944 framgår att staterna ska förse med PNR-uppgifter vid på förhand fastställda tidpunkter. Även i instruktionerna angående implementering av PNRGOV anges att överföringarna ska ske vid de tidpunkter som bestäms av staterna. Där anges vidare att det är luftrafikföretagen som ansvarar för att överföringarna sker i rätt tid. Staterna bör dock vara medvetna om att tiden det tar för luftrafikföretagen att ta

fram PNR-uppgifterna och överföra dem och för staterna att motta uppgifterna, kan variera. Om denna variation är ett bekymmer för en stat kan ett avtal mellan staten och lufttrafikföretaget behöva ingås för att förtydliga inom vilken tidsperiod som uppgifterna ska mottas.¹²

Enligt vår bedömning bör den tidsram om 24–48 timmar som anges i direktivet bibehållas i den svenska lagstiftningen. Överföringstidpunkten kan regleras närmare i avtal mellan enheten för passagerarinformation och berörda lufttrafikföretag. Har lufttrafikföretagen överfört sina uppgifter inom den i lagen angivna tidsramen har de dock uppfyllt sina lagstadgade skyldigheter och kan inte på denna grund bli föremål för någon sanktionsavgift.

Den andra överföringstidpunkten kan i lagen avgränsas till när gatens dörrar har stängts. Tidpunkten för överföringen torde härigenom vara tillräckligt definierad. Att gatens dörrar har stängts innebär att passagerare inte längre tillåts stiga ombord eller stiga av planet. Vidare bör det av lagen framgå att den andra överföringen får begränsas till såväl uppdateringar som kompletteringar av de uppgifter som överfördes vid det första tillfället. Således ska en andra överföring alltid omfatta även nytillkomna PNR-uppgifter, t.ex. avseende passagerare som bokat flygresan mindre än ett dygn före avgång.

11.4.6 Överföringar vid andra tidpunkter

Vårt förslag: När det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet, ska lufttrafikföretag på begäran av enheten för passagerarinformation överföra PNR-uppgifter även vid andra tidpunkter.

I vissa situationer kan lufttrafikföretagen behöva överföra PNR-uppgifter även vid andra tidpunkter än de som angetts ovan. I artikel 8.5 anges nämligen att i situationer där åtkomst till PNR-uppgifter är nödvändig för att reagera på ett specifikt och faktiskt hot

¹² Air Transport & Travel Industry, Functional and Business Principles, PNRGOV, Version 16.1, s. 6, punkterna 8 och 11.

med anknytning till terroristbrott eller grov brottslighet, ska lufttrafikföretag efter en bedömning i det enskilda fallet på begäran av en enhet för passagerarinformation överföra PNR-uppgifter vid andra tidpunkter än de som anges i punkt 3. En sådan begäran kan exempelvis bli aktuell då omständigheterna medför att tillgång till PNR-uppgifter avseende en viss person eller en viss flygresa är nödvändig för att reagera på en särskild risk för sådan brottslighet som direktivet avser i tiden mellan den första och andra överförings-tidpunkten.

Enligt direktivet ska en sådan ”extra” överföring ske efter en bedömning i det enskilda fallet. En bedömning huruvida det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter bör, enligt vår mening, göras av enheten för passagerarinformation, eventuellt efter framställan av en behörig myndighet. Det är ju enheten för passagerarinformation och de behöriga myndigheterna som har bäst kunskap i en sådan fråga och som har tillgång till det, troligen sekretessbelagda, material som bedömningen vilar på. Denna tolkning får stöd i artikel 2.8.3 i dokument 9944 och av dokumentet angående implementering av PNRGOV. Det är således inte upp till lufttrafikföretagen huruvida en överföring av PNR-uppgifter ska ske i dessa fall, utan överföringen ska ske när en sådan begäran kommer in från enheten för passagerarinformation. Detta bör framgå av regleringen.

Bestämmelsen bör i övrigt genomföras i lag i enlighet med dess ordalydelse. I svensk lagstiftning brukar dock ordet fara användas i stället för hot. Ordet används bland annat i brottsdatalagen. Med hänsyn härtill föreslår vi att ordet fara används i stället för hot även i genomförandet av vår lag. Av samma anledning bör ordet avvärja användas i vår lag i stället för begreppet reagera på, som används i PNR-direktivet. Således föreslår vi att det i lagtexten anges att ytterligare överföringar ska ske när det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet.

11.4.7 Hur överföringarna ska gå till

Våra förslag: Enheten för passagerarinformation får inte medges direktåtkomst till lufttrafikföretagens uppgiftssamlingar med PNR-uppgifter.

Lufttrafikföretagen ska överföra PNR-uppgifterna i elektronisk form. Närmare bestämmelser om formen för överföringarna bör framgå av förordning.

Direktåtkomst är inte tillåten

Det finns enligt PNR-direktivet två möjliga metoder för överföring av PNR-uppgifter (skäl 16 i ingressen). Den ena är direktåtkomstmetoden (även kallad pull-metoden) som innebär att de behöriga myndigheterna i den medlemsstat som begär tillgång till PNR-uppgifter kan få direktåtkomst till lufttrafikföretagets bokningssystem för att hämta en kopia av de PNR-uppgifter som behövs. Den andra metoden är sändmetoden (även kallad push-metoden), som innebär att lufttrafikföretagen överför de begärda PNR-uppgifterna till den myndighet som har begärt dem. Båda metoderna används av Tullverket vid deras insamlande av PNR-uppgifter i dag. Sändmetoden gör det möjligt för lufttrafikföretagen att behålla kontroll över vilka uppgifter som tillhandahålls. Den metoden anses därför ge en bättre skyddsnivå för uppgifterna (jfr skäl 16). Direktivet föreskriver således att all överföring av PNR-uppgifter från lufttrafikföretagen ska ske enligt sändmetoden (artikel 3.7 och 8.1).

Det bör av lagen framgå vilken metod som ska användas för överföringarna. Enligt vår mening görs detta lämpligast genom en bestämmelse som anger att enheten för passagerarinformation inte får medges direktåtkomst till lufttrafikföretagens uppgiftssamlingar för PNR-uppgifter, så som dessa avgränsas i bilagan till lagen. Av en sådan bestämmelse framgår motsatsvis att sändmetoden ska användas för överföringarna samtidigt som det anges att direktåtkomst inte är tillåten. Med uppgiftssamlingar avses i sammanhanget lufttrafikföretagens reservationssystem eller liknande datoriserade bokningssystem.

Former för överföringarna

All överföring av PNR-uppgifter från luftrafikföretag till enheter för passagerarinformation inom ramen för PNR-direktivet ska enligt artikel 8.3 ske på elektronisk väg. Av bestämmelsen framgår också att överföringarna ska ske med användning av de gemensamma protokoll och understödda dataformat som kommer att antas av kommissionen. Vid eventuella tekniska problem får överföringarna ske på något annat sätt som säkerställer ett lämpligt dataskydd.

I artikel 16.2 finns närmare bestämmelser om formen för överföringarna. Här framgår att kommissionen ska anta en förteckning över godkända gemensamma protokoll och understödda dataformat som ska användas vid överföring av PNR-uppgifter. De gemensamma protokollen ska användas för alla överföringar, så att PNR-uppgifternas säkerhet under överföringen tryggas. Uppgifterna ska vidare överföras i ett understött format, för att säkerställa att det kan läsas av alla berörda parter. Alla luftrafikföretag ska bestämma vilket gemensamt protokoll och vilket dataformat i förteckningen som de avser att använda för sina överföringar och underrätta enheterna för passagerarinformation om detta.

Kommissionen har i ett genomförandebeslut¹³ antagit en sådan förteckning över gemensamma protokoll och understödda format. Förteckningen kan senare komma att ändras (artikel 16.3). I genomförandebeslutet anges att mindre luftrafikföretag, som inte tillhandahåller flygförbindelser i enlighet med en särskild och offentlig tidtabell och som inte har den nödvändiga infrastrukturen för att använda de gemensamma protokollen och understödda formaten, ska undantas från skyldigheten att använda dessa format och protokoll. Ett sådant luftrafikföretag ska i stället överföra sina uppgifter på något annat elektroniskt sätt som tillhandahåller tillräckliga garantier med avseende på de tekniska säkerhetsåtgärderna, och som ska överenskommas mellan luftrafikföretaget och den berörda medlemsstaten.

Ett år från den dag då kommissionen för första gången har antagit gemensamma protokoll och understödda dataformat ska all överföring av PNR-uppgifter från luftrafikföretag till enheter för passagerarinformation inom ramen för direktivet ske enligt de gemen-

¹³ Kommissionens genomförandebeslut (EU) 2017/759 av den 28 april 2017 om gemensamma protokoll och dataformat som ska användas av luftrafikföretag när PNR-uppgifter överförs till enheterna för passagerarinformation.

samma protokollen och understödda dataformaten (artikel 16.2). Inom samma tid ska medlemsstaterna vidta de tekniska åtgärder som krävs för att dessa gemensamma protokoll och dataformat ska kunna börja användas (artikel 16.5).

Till dess gemensamma protokoll och understödda dataformat finns tillgängliga ska överföringarna göras med elektroniska medel som tillhandahåller tillräckliga garantier med avseende på de tekniska säkerhetsåtgärder och de organisatoriska åtgärder som styr den behandling som ska utföras. I händelse av tekniska problem får PNR-uppgifterna överföras på annat lämpligt sätt under förutsättning att samma säkerhetsnivå upprätthålls och att unionsrätten om dataskydd respekteras fullt ut. (Artikel 16.1 och 16.4.)

Reglering av överföringsformerna

Kommissionen har således antagit en lista över gemensamma protokoll och understödda dataformat. Dessa ska användas såväl av lufttrafikföretagen som av medlemsstaterna redan när direktivet ska vara genomfört i nationell rätt. Det saknas därför anledning att reglera vad som skulle ha gällt för det fall sådana gemensamma protokoll och format inte hade antagits.

Gemensamt för alla överföringar till enheten för passagerarinformation kommer att vara att de ska ske i elektronisk form. Detta bör framgå av vår lag. De närmare formerna för överföringarna kommer dock att skifta mellan lufttrafikföretagen och bero på vilket format och protokoll de kommer att välja för överföringarna och huruvida företagen är sådana att de enligt kommissionens beslut kan använda sig av någon annan form för överföringen.

Enligt direktivets artikel 14 ska sanktioner träffa de lufttrafikföretag som inte överför PNR-uppgifter i det fastställda formatet. Det behöver därför i regleringen finnas närmare bestämmelser om formaten för överföringarna. Eftersom formaten kan komma att ändras bör denna fråga lämpligen regleras i förordning. Enligt vår mening kan frågan lämpligen lösas genom att det i den till lagen anslutande förordningen förs in en hänvisning till artikel 1 i kommissionens genomförandebeslut.

Vid eventuella tekniska problem ska överföringarna enligt artikel 8.3 ske på något annat sätt som säkerställer ett lämpligt dataskydd, se även artikel 16.1. Även denna fråga kan regleras i förordning.

11.4.8 Anlitande av personuppgiftsbiträde

Vårt förslag: Den som är skyldig att överföra PNR-uppgifter får anlita ett personuppgiftsbiträde för att utföra överföringen.

Den grundläggande skyldigheten att överföra PNR-uppgifter åläggs vissa luftrafikföretag. Som vi kommer att återkomma till i avsnitt 19.1 är luftrafikföretagen personuppgiftsansvariga för PNR-uppgifterna och ansvarar därmed för att överföringarna till enheten för passagerarinformation sker på ett säkert sätt. Det finns dock inget i direktivet som hindrar att luftrafikföretagen använder sig av mellanmän, s.k. personuppgiftsbiträden, för att utföra själva överföringen. Det är således möjligt att överföringarna kommer att ske via systemleverantörer och datoriserade bokningssystem.¹⁴ Detta bör av tydlighetsskäl framgå av lagen.

¹⁴ Se t.ex. Europaparlamentets och rådets förordning (EG) nr 80/2009 av den 14 januari 2009 om en uppförandekod för datoriserade bokningssystem och upphävande av rådets förordning (EEG) nr 2299/89.

12 Resebyråer och researrangörer

12.1 Medlemsstaternas överenskommelse och vårt uppdrag

PNR-direktivet påverkar inte medlemsstaternas möjligheter att samla in och behandla PNR-uppgifter från andra transportföretag än lufttrafikföretag. Direktivet påverkar inte heller medlemsstaternas möjlighet att begära in och behandla PNR-uppgifter från andra ekonomiska aktörer som tillhandahåller reserelaterade tjänster, såsom resebyråer och researrangörer. I båda fallen förutsätts dock att nationella bestämmelser rörande detta är förenliga med EU-rätten (se skäl 33).

I samband med att PNR-direktivet antogs har dock medlemsstaterna även antagit en deklaration som anger att de, i enlighet med sin nationella lagstiftning och med förbehåll för parlamentsbehandling i vissa medlemsstater, åtar sig att i enlighet med parlamentets önskemål utvidga insamlingen av PNR-uppgifter till att omfatta även aktörer som inte är lufttrafikföretag. Som exempel anges i deklarationen resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, för vilka sådana uppgifter samlas in och behandlas. Någon tidsgräns för när detta ska vara genomfört i nationell lagstiftning anges inte i deklarationen.

I våra kommittédirektiv anges att deklarationen innebär att medlemsstaterna ska eftersträva att införa nationella bestämmelser som innebär skyldigheter att överföra flygpassageraruppgifter även för ekonomiska aktörer som inte är transportörer, t.ex. de resebyråer och researrangörer som erbjuder bokningsförmedling vid vilken sådana uppgifter samlas in och behandlas. En utgångspunkt för vårt uppdrag är därför att skyldigheten att föra över flygpassageraruppgifter till de nationella enheterna i medlemsstaterna även ska omfatta resebyråer och researrangörer.

12.2 Resebyråer och researrangörer

Det är vanligt att dela in de aktörer som förmedlar resetjänster i resebyråer och researrangörer, där en resebyrå vanligen är att betrakta som en återförsäljare av andras resor och turisttjänster, medan en researrangör är ett företag som producerar och säljer egna resor. Denna uppdelning är emellertid inte helt skarp. En aktör kan vara resebyrå i ett sammanhang och researrangör i ett annat.

Någon definition av begreppet *resebyrå* finns inte i lagstiftningen. En resebyrå utmärks dock typiskt sett av att den förmedlar ett avtal för annan. Avtalet ingås mellan, å ena sidan, en resenär och, å andra sidan, en transportör, en researrangör eller ett hotell etc. Det finns emellertid situationer då en resebyrå kan få ställning som part i reseavtalet. Om resebyrån agerar självständigt i förhållande till transportörens avtalsvillkor, t.ex. genom att ge en egen rabatt eller göra egna utfästelser, talar det för att den agerar för egen räkning som part i reseavtalet. Frågan om resebyrån i övrigt intar partsställning får bedömas utifrån allmänna avtalsrättsliga grundsatsar (se NJA 2014 s. 978). Det är inte helt ovanligt att en resebyrå även arrangerar egna paketresor, företrädesvis grupp- och konferensresor för affärsresekunder.

Antalet svenska företag som kan betraktas som resebyråer uppgick vid utgången av år 2015 till drygt 290¹. Beräkningen inkluderar dock inte resebyråer som endast säljer resor via internet. Av resebyråerna är något mer än hälften huvudsakligen inriktade på privatreseförsäljning, ett sextiotal är renodlade affärsresebyråer och resterande säljer både privat- och affärsresor. Ca 60 procent av alla bokningar av flygbiljetter, inom EU och internationellt, utförs av resebyråer².

En *researrangör* säljer resepaket, dvs. erbjuder en paketslösning med t.ex. flyg och boende. De som säljer och arrangerar paketresor kan vara allt från mindre familjeföretag till större företag och organisationer. Bland researrangörer finns traditionella charteroperatörer som t.ex. Tui, Ving och Apollo med dotterbolag. Dessa tre researrangörer ägs alla av olika internationella resekoncerner och har egna flygbolag. Andra researrangörer använder sig av reguljärflyg eller andra transportmedel.

¹ Enligt Svenska Resebyråföreningens marknadsuppgifter för år 2015.

² Enligt uppgift från Svenska Resebyråföreningen.

I lagen (1992:1672) om paketresor (paketreselagen) regleras bl.a. arrangörers ansvar för sådana paketresor som de säljer eller marknadsför. Paketreselagen genomför det s.k. paketresedirektivet³. I lagens 3 § definieras en arrangör som den som annat än tillfälligtvis organiserar paketresor och säljer eller marknadsför dem direkt eller genom en återförsäljare. I lagens förarbeten anges att vid bedömningen av vad som är ”annat än tillfälligtvis” torde man få beakta dels hur ofta vederbörande ordnar paketresor men dels också hur regelbundet eller sporadiskt resorna återkommer. Den som varje år ordnar resor till en viss återkommande kongress eller något annat evenemang torde sålunda få anses vara arrangör i lagens mening. Men den som ordnar två eller tre paketresor tätt efter varandra till ett visst evenemang omfattas knappast av lagen, om han eller hon i övrigt inte alls organiserar resor. Detsamma torde gälla den som oregelbundet och relativt sällan ordnar resor (se prop. 1992/93:95 s. 67). En återförsäljare är enligt lagen den som säljer eller marknadsför arrangörens resor.

Ett nytt EU-direktiv om bl.a. paketresor antogs i november 2015.⁴ Genom direktivet upphävs det tidigare direktivet om paketresor. Medlemsstaterna ska senast den 1 januari 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att genomföra direktivet. Dessa bestämmelser ska tillämpas från och med den 1 juli 2018. I direktivet finns en annorlunda, och längre, definition av arrangörsbegreppet. En arrangör definieras här som en näringsidkare som kombinerar och säljer eller erbjuder paketresor, antingen direkt eller genom en annan näringsidkare eller tillsammans med en annan näringsidkare, eller den näringsidkare som överför resevärdens uppgifter till en annan näringsidkare i enlighet med en särskild bestämmelse i direktivet. Direktivet innehåller även en längre definition av begreppet näringsidkare. Återförsäljare definieras i direktivet som en annan näringsidkare än arrangören som säljer eller erbjuder paketresor som kombinerats av en arrangör.

³ Rådets direktiv (90/314/EEG) av den 13 juni 1990 om paketresor, semesterpaket och andra paketarrangemang.

⁴ Europaparlamentets och rådets direktiv (EU) 2015/2302 av den 25 november 2015 om paketresor och sammanlänkade researrangemang, om ändring av förordning (EG) nr 2006/2004 och Europaparlamentets och rådets direktiv 2011/83/EU samt om upphävande av rådets direktiv 90/314/EEG.

Paketreseutredningen överlämnade den 30 augusti 2016 sina förslag på hur det nya direktivet ska genomföras i svensk rätt. I betänkandet föreslås att den nu gällande paketreselagen byts ut mot en ny lag med samma namn. Direktivets definitioner av begreppen arrangör och återförsäljare föreslås oförändrade föras in i den nya lagen (se SOU 2016:56 s. 124 ff.). Förslaget bereds nu inom regeringskansliet.

Det finns närmare 600 researrangörsföretag i Sverige, bussreseföretagen inte inräknade.⁵ De flesta arrangerar och säljer paketresor för konsumenter. Ett fåtal är helt inriktade på arrangemang för andra företag. Härutöver finns ett antal företag i form av enskilda firmor och ideella föreningar som organiserar någon eller några enstaka resor om året.

Cirka hälften av de svenska researrangörernas och resebyråernas totala försäljning sker i dag över internet. Vissa resor säljs av s.k. OTA:er. OTA är en förkortning för "online travel agency" och begreppet används för att beskriva aktörer som är helt inriktade på att sälja resor via internet. Det är vanligt att företag som säljer resor via internet gör det under flera olika varumärken. Det företag som har de flesta varumärkena är E-traveli/Svenska resegruppen. Merparten av de företag som säljer på internet gör det under sitt eget varumärke, t.ex. Resia.se och Ticket.se. Vid sidan om onlineförsäljningen finns det digitala tjänster i form av rena söktjänster. Dessa tjänster erbjuder en möjlighet att hitta och jämföra resor från flera leverantörer. Företagen bakom söktjänsterna säljer inte själva resor, utan tjänar pengar på provisioner från reseföretagen och eventuell merförsäljning via tjänsterna. Ett exempel på en sådan s.k. metasökmotor är Flygresor.se. Flera av söktjänsterna ägs dock av koncerner som också består av företag som säljer resor.

Antalet resebyråer och researrangörer inom Europa uppgick år 2014 till omkring 50 000.⁶ Den internationella konkurrensen på marknaden har ökat i takt med att konsumenterna i högre utsträckning vant sig vid att köpa resor via internet. Det gäller både svenska företag som vänder sig till utländska resenärer och utländska företag som vänder sig till svenska resenärer. Exempel på det senare är företagen Expedia och Booking.com.

⁵ Enligt Svenska resebyråföreningens marknadsuppgifter för år 2015.

⁶ The european travel agents and tour operator association (ACTAA), Table of Statistics.

12.2.1 Resebyråers och researrangörers insamling och överföring av PNR-uppgifter till lufttrafikföretag

När en resenär väljer att boka en resa via en resebyrå eller researrangör skapas PNR-uppgifter i samband med att bokningen genomförs. PNR-uppgifterna överförs därefter till lufttrafikföretagen antingen direkt via flygbolagens hemsidor, eller, vilket är vanligast, via särskilda reservationssystem.

De reservationssystem som vanligtvis används brukar kallas Global Distribution System (GDS) eller Computer Reservation System (CRS). Reservationssystemen möjliggör direktkommunikation mellan å ena sidan den som utför bokningen och å andra sidan lufttrafikföretaget. Systemen innehåller information om bland annat flygbolagens tidtabeller, platstillgång, biljettpriser och tjänster i samband med flygbefordran. Genom reservationssystemen får en ansluten resebyrå eller researrangör tillgång till anslutna flygbolags "lager" av t.ex. flygstolar. Resebyrån eller researrangören kan därmed gå rakt in i "lagret" och sälja en flygstol till en kund för flygbolagets räkning.

Reservationssystemen byggdes ursprungligen upp och ägdes av flygbolagen. På grund av ändrade regler är det numera inte lika fördelaktigt för flygbolagen att själva äga systemen och flera flygbolag har därför helt eller delvis sålt sina ägarandelar. Det finns i dagsläget tre dominerande reservationssystem; Amadeus, Sabre och Travelport. Företaget bakom Amadeus är det enda som är lokaliserat i Europa och systemet är det som främst används i Skandinavien. Det har inom EU antagits en förordning som innehåller en uppförandekod för reservationssystemen.⁷

När en resebyrå eller researrangör tar emot en bokningsförfrågan från en resenär skapar företaget normalt en bokningsfil i det datoriserade reservationssystemet. Den bokningsfil som skapas innehåller således uppgifter om resenären och dennes bokning, dvs. PNR-uppgifter. De PNR-uppgifter som härigenom skapas överförs därefter från reservationssystemet till det flygbolag som ansvarar för flygningen. Hur många uppgifter som förs över beror på hur många uppgifter som förts in i systemet. En researrangör ansvarar gentemot kunden för avtalets fullgörande medan en resebyrå normalt

⁷ Europaparlamentets och rådets förordning (EG) nr 80/2009 av den 14 januari 2009 om en uppförandekod för datoriserade bokningssystem och upphävande av rådets förordning (EEG) nr 2299/89.

endast förmedlar en flygbiljett. Därför har resebyrån och researrangören olika behov av personuppgifter från kunden och de uppgifter som hämtas in och överförs kan variera. Hur många uppgifter som förs över kan också variera beroende på vilka krav som ställs av flygbolagen. Resebyråerna överför dock normalt på detta sätt samtliga insamlade PNR-uppgifter till lufttrafikföretagen.

De PNR-uppgifter som har överförts från resebyråerna eller researrangörerna kan senare ändras på begäran av resenären, i synnerhet vid ändring i eller avbokning av flygbiljetten. En resebyrå ställer dock vanligtvis ut resenärens biljett kort tid efter bokningen och har sedan utfört sin del av avtalet.

I vissa fall görs ändringar i PNR-uppgifterna en kort tid före avresa. Sådana ändringar kan vara avbokningar i sista minuten eller s.k. ”no-shows”, som innebär att resenären inte infinner sig till incheckning och avresa. I de flesta fall får inte resebyrån kännedom om sena ändringar, avbokningar eller no-show över huvud taget.

Det finns resebyråer och researrangörer som inte själva har tillgång till reservationssystem och som i stället köper in den tjänsten från andra resebyråer eller researrangörer.

För de researrangörer som arrangerar charterresor råder något andra förutsättningar. Resenärernas PNR-uppgifter samlas i dessa fall i charterarrangörernas interna bokningssystem. De PNR-uppgifter som efterfrågas av lufttrafikföretagen överförs i ett förutbestämt filformat en viss bestämd tid före varje flygning. I vissa fall sker överföringen via en mellanhand som har till uppgift att segmentera ut de uppgifter som respektive flygbolag kräver för aktuell transport och att formatera om de filer som överförs från researrangören till det filformat som krävs av lufttrafikföretaget. Ett exempel på mellanhand är företaget Paxport med säte i Sverige. De uppgifter som överförs består i huvudsak endast av en passagerarlista (Passenger Name List – PNL). Passagerarlistan innehåller färre uppgifter än vad som normalt brukar ingå bland PNR-uppgifterna. Dock brukar uppgifter om namn, kön, ålder på barn, förbokad måltid, specialmat, handikapp eller behov av assistans samt anmälda allergier framgå.

12.2.2 Behöriga myndigheter vill kunna få tillgång till samtliga insamlade PNR-uppgifter

För att PNR-systemet ska vara effektivt ur ett brottsbekämpningsperspektiv bör samtliga PNR-uppgifter som har samlats in om passagerare inför en flygning överföras till de nationella enheterna för passagerarinformation. De i utredningen representerade behöriga myndigheterna har uttryckt ett önskemål om att samtliga PNR-uppgifter som passagerarna har lämnat, antingen direkt till ett lufttrafikföretag eller via en resebyrå eller researrangör, och som omfattas av bilaga I i PNR-direktivet, överförs till den svenska enheten för passagerarinformation.

Flygtrafiken till vissa länder, exempelvis USA, utgörs främst av reguljärflygningar. Om en reguljär flygresa har bokats via en resebyrå, överför resebyrån normalt de PNR-uppgifter som den har samlat in om kunden till det lufttrafikföretag som ska utföra resan. Till andra länder, såsom exempelvis Turkiet, utgörs flygtrafiken främst av charterflyg. Som framgått ovan överförs vid charterresor oftast ett mindre antal PNR-uppgifter till det lufttrafikföretag som ska utföra flygningen. Således är det endast dessa uppgifter som lufttrafikföretaget i sin tur kommer att överföra till enheten för passagerarinformation. Resten av PNR-uppgifterna finns kvar hos arrangören. Många av just charterflygningarna går till länder som är känsliga utifrån perspektivet bekämpning av grov brottslighet och terroristbrottslighet. Det har därför framförts önskemål om att tillgång ska finnas även till sådana PNR-uppgifter som finns kvar hos charterarrangörerna.

12.2.3 Insamling av PNR-uppgifter från resebyråer och researrangörer i dagsläget

Insamling av PNR-uppgifter från resebyråer eller researrangörer sker i dag, såvitt vi känner till, främst via lufttrafikföretagen. Det finns dock i Frankrike en lagbestämmelse som innebär att resebyråer och researrangörer på begäran kan bli skyldiga att överföra vissa PNR-uppgifter för användning i den brottsbekämpande verksamheten.⁸ Hur denna reglering närmare är utformad eller fungerar har vi dock

⁸ Article L232-7 Code de la sécurité intérieure.

inte haft möjlighet att närmare granska. Under alla förhållanden baseras lagbestämmelsen dock inte på en implementering av PNR-direktivet eller den därtill hörande överenskommelsen.

Det är i skrivande stund inte klart hur medlemsstaterna kommer att hantera den aktuella överenskommelsen. Det har i ett sent skede i vår utredning kommit till vår kännedom att det i Tyskland finns ett förslag som innebär att andra aktörer involverade i reservation eller bokning av flygbiljetter i god tid ska överföra PNR-uppgifter till lufttrafikföretagen för vidare befordran till enheten för passagerarinformation. Huruvida förslaget innebär att resebyråer och researrangörer ska överföra fler uppgifter till lufttrafikföretagen än vad de gör idag har vi dock inte haft möjlighet att analysera. I Storbritannien har man än så länge koncentrerat sig på att genomföra direktivet i förhållande till lufttrafikföretagen och kommer först i ett senare skede att analysera hur systemet kan utvecklas till att även omfatta resebyråer och researrangörer. Ytterligare uppgifter om hur de andra medlemsstaterna kommer att genomföra den aktuella överenskommelsen har vi inte haft möjlighet att få tillgång till.

12.3 Våra överväganden

Vår bedömning: Resebyråer och researrangörer omfattas redan av systemet med insamling av PNR-uppgifter. Ytterligare utvidgning av detta system bör tills vidare anstå.

Innebörden av medlemsstaternas överenskommelse och vårt uppdrag

Medlemsstaterna inklusive Sverige har alltså i ett gemensamt uttalande från rådet, en deklARATION, åtagit sig att utvidga insamlingen av PNR-uppgifter till att omfatta aktörer som inte är lufttrafikföretag, exempelvis sådana resebyråer och researrangörer som utför resebokningar. Några närmare uppgifter om hur detta ska gå till anges inte i deklARATIONEN. Inte heller våra kommittédirektiv preciserar vad det är för insamling som det ingår i vårt uppdrag att överväga.

På motsvarande sätt som vi tolkat vårt uppdrag när det gäller lufttrafikföretagens skyldigheter kan vi inte förstå denna del av vårt

uppdrag på annat sätt än att det handlar om att överväga en utvidgning som innebär att den svenska enheten för passagerarinformationssamling av PNR-uppgifter också ska omfatta PNR-uppgifter från resebyråer och researrangörer. Härmed avses sådana uppgifter om kunder som svenska, utländska eller multinationella resebyråer och researrangörer samlar in i sin verksamhet med att arrangera och förmedla resor som innefattar flygresor till eller från Sverige. Vi kommer därför att här bara diskutera en eventuell skyldighet för resebyråer och researrangörer att överföra uppgifter till den svenska enheten för passagerarinformation. Frågan om någon eventuell skyldighet för dessa aktörer att förse övriga medlemsstaters enheter med PNR-uppgifter kommer inte att beröras i det följande.

Möjliga alternativa modeller

Det kan konstateras att resebyråerna och researrangörerna utgör en stor och brokig skara, som innehåller såväl stora internationella bolag som små enmansbolag, enskilda firmor och ideella föreningar. Vissa aktörer säljer endast resor via internet och andra såväl på traditionellt vis som via sina hemsidor. Många aktörer använder sig av de stora internationella reservationssystemen, medan andra köper in sådana tjänster från större bolag. Vidare har användandet av internet medfört att resebranschen blivit alltmer internationell. Det är således inte alls säkert att en svensk resenär köper sin resa via en svensk resebyrå eller arrangör. Vad gäller utländska resenärer till Sverige torde bilden bli ännu mera brokig.

Det framgår inte av överenskommelsen om insamlingen ska begränsas till sådana resebyråer och researrangörer som har sitt säte inom en medlemsstat eller inom unionen. För det fall insamlingen är tänkt att omfatta samtliga resebyråer och researrangörer som bokar de flygresor som direktivet träffar, skulle det innebära att alla resebyråer och researrangörer i hela världen som ordnar eller förmedlar flygresor till eller från EU träffas av överföringsskyldigheten. Således skulle alla resebyråer och researrangörer världen över som bokar en flygresa till eller från Sverige åläggas en skyldighet att överföra PNR-uppgifter till den svenska enheten för passagerarinformation. Antalet resebyråer och researrangörer i hela världen uppgår till ett okänt och otaligt antal. Bara i Europa fanns det år 2014 ca 50 000 sådana

företag. Redan här kan sägas att ett upplägg som innebär att överföringar ska ske från företag som inte har någon annan koppling till Sverige än att de förmedlar flygresor hit, får antas vara mycket svårt att anordna. De tekniska och administrativa hindren för att genomföra ett sådant system synes oändliga. Möjligheten att använda sanktioner mot de utländska företag som inte uppfyller en sådan överföringsskyldighet får också antas möta stora praktiska bekymmer.

Alldeles bortsett från dessa generella svårigheter ser vi i huvudsak tre tänkbara modeller för hur en utvidgning av insamlingen av PNR-uppgifter skulle kunna konstrueras. Vi har identifierat vissa problem med alla tre modellerna, vilka vi beskriver och diskuterar i det följande.

Modell 1) – En direkt utvidgning av direktivet

Ett sätt att genomföra medlemsstaternas överenskommelse vore att direkt utvidga tillämpningen av PNR-direktivet och den svenska lagstiftning som genomför direktivet till att även omfatta resebyråer och researrangörer. Det system för överföring av PNR-uppgifter till enheterna för passagerarinformation som direktivet reglerar är dock utformat och anpassat för att det är just lufttrafikföretag, eller deras uppdragstagare, och inte andra aktörer som ska överföra PNR-uppgifterna. Enligt direktivet ska uppgifterna överföras vid två tillfällen, det första 24–48 timmar före flygningens planerade avgång och det andra omedelbart efter det att gatens dörrar har stängts.

Flygbiljetter bokas många gånger långt i förväg. Efter det att en resebyrå har ställt ut önskade flygbiljetter har resebyrån normalt fullgjort sin del av avtalet. Det finns i dag inget givet system som ger resebyråer eller researrangörer möjlighet att söka fram de passagerare som ska resa ett antal dagar och timmar senare. Rent tekniskt skulle i vart fall de stora researrangörerna kunna bygga om sina system för att kunna uppfylla denna skyldighet. Det skulle dock få ske till relativt omfattande kostnader. För mindre resebyråer och researrangörer skulle det vara mycket svårt att bära en sådan kostnad.

En resebyrå eller researrangör kommer dock aldrig att kunna veta om alla passagerare som är bokade på en flygning också infinner sig till denna. Det är flygbolagens personal som har hand om incheckningen på flygplatsen, som står uppe vid flyget och som assisterar

så att flyget kan avgå. Ibland kan charterpersonal finnas på flygplatserna, men i sådana fall är den personalen inhyrd av flygbolagen. Det är således normalt endast det lufttrafikföretag som utför flygningen som har kontroll över inchecknings- och ombordstigningsprocessen. Komplet och uppdaterad information om vilka resenärer som faktiskt går ombord på flygplanet har därmed endast lufttrafikföretaget.

En flygning kan bli försenad av många anledningar. En flygresa kan ställas in och ersättningsflyg kan behöva användas. Resebyråerna och researrangörerna har ingen del i denna process. Dessa aktörer kan därför omöjligen veta när gatens dörrar har stängts. För att kunna uppfylla överföringsskyldigheten enligt direktivet skulle samtliga resebyråer och researrangörer behöva ha personal på plats på samtliga flygplatser vid gaterna, vilket förefaller vara en omöjlighet. Vi kan således inte se att resebyråer och researrangörer har möjlighet att överföra PNR-uppgifter vid de tidpunkter som anges i PNR-direktivet. En direkt utvidgning av direktivets bestämmelser till att omfatta även resebyråer och researrangörer ter sig därför inte praktiskt möjlig.

Modell 2) – Ytterligare överföring via lufttrafikföretagen

En utvidgning av insamlandet av PNR-uppgifter till att även omfatta resebyråer och researrangörer synes ha till syfte att tillse att alla de PNR-uppgifter som har samlats in av någon aktör i flygresebranschen också överförs till de nationella myndigheterna. Det främsta skälet till att ålägga resebyråer och researrangörer en egen överföringsskyldighet får antas vara att endast en mindre del av de insamlade PNR-uppgifterna i dagsläget överförs från charterarrangörerna till de lufttrafikföretag som utför charterflygningar. Vi har full förståelse för de behöriga myndigheternas önskemål om att få tillgång även till de uppgifter som i dessa fall finns kvar hos charterarrangörerna. En lösning på denna problematik vore att charterarrangörerna ålades att överföra fler PNR-uppgifter till lufttrafikföretagen än i dag, för vidare överföring av dessa uppgifter till enheten för passagerarinformation. Så skulle i princip kunna göras även beträffande resebyråer och andra researrangörer än charterbolag.

Det är emellertid en grundläggande tanke bakom PNR-direktivet att lufttrafikföretagen inte ska åläggas att samla in eller lagra ytterligare uppgifter om sina passagerare (se skäl 8 i direktivets ingress). Det är alltså endast de PNR-uppgifter som lufttrafikföretagen redan samlar in som en del av sin normala kommersiella verksamhet som enligt direktivet ska överföras till de nationella enheterna för passagerarinformation. Således vore det enligt vår mening oförenligt med PNR-direktivet att i lag eller förordning ålägga lufttrafikföretagen att samla in fler uppgifter än de som de redan samlar in för den egna verksamheten. Vi kan inte heller se att en ordning som innebär en skyldighet för resebyråer och researrangörer att leverera fler PNR-uppgifter till lufttrafikföretagen än vad de sistnämnda i dag behöver skulle vara förenlig med den nyss nämnda grundläggande tanken bakom direktivet. Detta gäller i synnerhet om sådana uppgifter som emanerat från resebyråernas och researrangörernas leveransskyldighet skulle behandlas av enheten för passagerarinformation och överföras mellan medlemsstaterna i enlighet med det system som PNR-direktivet ålägger medlemsstaterna att genomföra. Vi har nämligen svårt att se att direktivet ger rättsligt stöd för ett uppgiftsutbyte avseende andra slags PNR-uppgifter än de som samlas in från lufttrafikföretagen eftersom uppgifterna behandlas i deras kommersiella verksamhet. Att hålla isär de PNR-uppgifter som emanerar från charterarrangörernas uppgiftsskyldighet från sådana som överförs enligt PNR-direktivets bestämmelser, och därför också skulle omfattas av direktivets bestämmelser om uppgiftsutbyte mellan medlemsstaterna m.m., torde emellertid vara en svår utmaning praktiskt sett. Redan det sagda innebär enligt vår mening att det vi kallar modell 2 inte kan föreslås inom ramen för vårt arbete. Det kan i sammanhanget dessutom erinras om att skäl 8 i ingressen anger att direktivet inte bör medföra någon skyldighet för passagerare att tillhandahålla några uppgifter utöver de som redan tillhandahålls *lufttrafikföretagen* (vår kursivering).

Vi vill framhålla att en lösning enligt modell 2 torde kunna åstadkommas på frivillig väg. Beroende på hur en sådan lösning riggas skulle den dock av allt att döma innebära utvecklingskostnader för charterarrangörerna och eventuellt ytterligare kostnader för mottagandet hos lufttrafikföretagen. Dessutom skulle ett antal frågor rörande integritet och dataskydd behöva analyseras närmare, såsom om överföringarna till lufttrafikföretagen skulle kräva samtycke

från resenärerna eller om någon annan rättslig grund i dataskyddsförordningen kan tillämpas, vem som skulle ha personuppgiftsansvaret för uppgifterna och därmed ansvara för säkerhetsfrågor osv.

Modell 3) – Överföring från resebyråer och researrangörer direkt till enheten för passagerarinformation

Den tredje modellen tar sin utgångspunkt i skäl 33 i PNR-direktivet enligt vilket direktivet inte påverkar medlemsstaternas möjligheter att i enlighet med nationell rätt tillhandahålla ett system för insamling och behandling av PNR-uppgifter från ekonomiska aktörer som inte är transportörer, t.ex. resebyråer och researrangörer som samlar in PNR-uppgifter i sin verksamhet. Detta förutsätter givetvis att den nationella rätten är förenlig med unionsrätten. PNR-direktivet som sådant hindrar alltså inte att det införs en lagstiftning i Sverige om att resebyråer och researrangörer ska överföra PNR-uppgifter direkt till enheten för passagerarinformation.

Ett system med direktöverföring från resebyråer och researrangörer till enheten för passagerarinformation reser ett flertal frågor.

En första fråga är givetvis hur systemet lämpligen skulle utformas i fråga om när och hur resebyråer och researrangörer skulle överföra PNR-uppgifter till enheten för passagerarinformation. *När* vore det möjligt i förhållande till flygplans planerade avgångar? *När* vore det lämpligt utifrån enhetens behov av uppgifterna? Är ett jämfört med lufttrafikföretagens sändningar tidigarelagt översändande till enheten, t.ex. vid biljettering, alls acceptabelt från integritetsynpunkt? *Hur* skulle uppgifterna överföras? Hur kan man undvika att enheten får samma PNR-uppgifter i dubbel upplaga, dvs. både direkt från resebyråerna eller researrangörerna och via lufttrafikföretagen? Kan man utgå från att det finns standardiserade format och språk för alla de olika aktörernas samtliga PNR-uppgifter på motsvarande sätt som det finns för lufttrafikföretagens? Om inte, vem ska utveckla sådana? Hade det varit tillräckligt att överföringar skedde på särskild begäran?

En ytterligare fråga är vilka möjligheter enheten för passagerarinformation har att inom en nära överskådlig tid ta emot PNR-uppgifter direkt från små och stora resebyråer och researrangörer i Sverige och i andra länder vid sidan av dem som kommer från lufttrafikföretagen. Enligt vad vi inhämtat är de tekniska och perso-

nella förberedelserna för att kunna ta emot PNR-uppgifter bara från lufttrafikföretagen ingen okomplicerad process. Vi befarar att en utvidgning med ett nytt system med direktöverföringar från resebyråer och researrangörer kan, i vart fall på kort sikt, bli en övermäktig uppgift som i värsta fall riskerar att försvåra det faktiska genomförandet av PNR-direktivets system.

Det måste också beaktas att ett åläggande för resebyråer och researrangörer att själva överföra PNR-uppgifter till enheten för passagerarinformation skulle få betydande tekniska, driftsmässiga och ekonomiska konsekvenser för företagen. Den infrastruktur som krävs för en sådan lösning finns inte i dag varför ett sådant åläggande torde medföra stora utvecklings- och investeringskostnader. Lönsamheten i branschen är generellt sett svag och företagen har normalt små marginaler. De minsta bolagen med bara ett fåtal anställda skulle drabbas hårdast då de skulle ha svårt att klara av att bevaka och säkerställa överföringen av uppgifterna.

Som tidigare konstaterats består branschen av ett stort antal aktörer av skiftande slag och storlek. Att finna ett överföringssystem som kan tillgodose alla aktörers möjligheter och tekniska lösningar är en grannlaga uppgift. Att på egen hand finna ett system som reglerar överföring från all världens eller unionens resebyråer och researrangörer får ses som en näst intill omöjlig uppgift inom ramen för detta uppdrag. En begränsning av överföringsskyldigheten till att endast omfatta svenska företag kan inte heller anses lämpligt. Resebyråerna och researrangörerna agerar på en internationell och kommersiell marknad. För det fall Sverige skulle införa en lösning som endast eller till största del träffade svenska företag, skulle företag från andra länder få konkurrensfördelar. Vi kan inte förorda en lösning som innebär att svenska resebyråer och researrangörer drabbas hårdare än andra. Sammantaget är det vår uppfattning att överväganden angående införandet av ett system med direktöverföring av PNR-uppgifter från resebyråer och researrangörer till enheten för passagerarinformation måste föregås av ett mer grundligt analys- och kartläggningsarbete än vad som är möjligt att utföra inom ramarna för vårt uppdrag.

Vår sammanfattande bedömning

Resebyråerna och researrangörerna kommer att bli en del av PNR-systemet, eftersom de redan i dag överför PNR-uppgifter till lufttrafikföretagen för vidare befordran till enheterna för passagerarinformation i Sverige och i andra medlemsstater och kommer att fortsätta göra det. Som angetts ovan är det inte möjligt att därutöver göra PNR-direktivets bestämmelser om överföring från lufttrafikföretagen till de nationella enheterna för passagerarinformation direkt tillämpliga för resebyråerna och researrangörerna. Inte heller är det enligt direktivet möjligt att ålägga lufttrafikföretagen att hämta in fler uppgifter från dessa aktörer. Enligt vår mening kan det knappast ses som ett tillåtet kringgående att – i stället för att ålägga lufttrafikföretagen en ökad insamling – ålägga resebyråer och researrangörer att föra över ytterligare PNR-uppgifter till lufttrafikföretagen; uppgifter som de sistnämnda inte behöver för sin kommersiella verksamhet. För att införa bestämmelser om överföring direkt från resebyråerna eller researrangörerna till den nationella enheten för passagerarinformation skulle det därför vara nödvändigt att åstadkomma en egen nationell lösning. Som vi anført ovan förefaller ett sådant nationellt system inte vara lämpligt att införa i nuläget.

Vi är medvetna om att det möjligen har gjorts andra tolkningar av direktivet i Tyskland än de som vi har kommit fram till ovan. Det förändrar inte våra bedömningar i detta läge. Vi ser det dock som troligt att en utvidgning av systemet med insamling av PNR-uppgifter till att omfatta ytterligare uppgifter från resebyråer och researrangörer kommer att ske genom en användning av det vi kallar modell 2. En sådan utvidgning kräver dock, som vi ser det, en justering av PNR-direktivet alternativt att en frivillig överenskommelse i frågan ingås mellan lufttrafikföretagen och resebranschen.

Kommissionen ska senast den 25 maj 2020 utföra en översyn av PNR-direktivet. Vid denna översyn ska det beaktas huruvida det är nödvändigt att låta resebyråer och researrangörer omfattas av direktivets tillämpningsområde (artikel 19.3). Mot bakgrund av översynen ska kommissionen, om det är lämpligt, lägga fram ett lagstiftningsförslag i syfte att ändra direktivet (artikel 19.4).

Som tidigare har angetts finns det inte någon tidsangivelse för när medlemsstaternas överenskommelse ska vara genomförd i natio-

nell rätt. Enligt vår mening finns det därför all anledning att avvakta den översyn som kommer att ske av kommissionen, innan överenskommelsen genomförs i svensk rätt genom en utvidgad insamling av PNR-uppgifter från resebyråer och researrangörer utöver den överföring av PNR-uppgifter som redan i dag sker via lufttrafikföretagen.

En skyldighet för resebyråer och researrangörer att överföra PNR-uppgifter till de nationella enheterna för passagerarinformation bör, precis som frågan om överföring av dessa uppgifter från lufttrafikföretagen, behandlas på samma sätt inom samtliga medlemsstater. Det är således angeläget att följa utvecklingen i denna fråga inom EU. Med hänsyn härtill och av de skäl som tidigare anförts, finns inte förutsättningar att i nuläget föreslå en ytterligare utvidgning av PNR-systemet. Frågan bör dock bevakas och eventuellt utredas vidare.

13 Behandling av PNR-uppgifter vid enheten för passagerarinformation

13.1 En databas för PNR-uppgifter

Vårt förslag: En bestämmelse förs in i lagen som anger att de PNR-uppgifter som överförs från lufttrafikföretagen ska lagras i en databas vid enheten för passagerarinformation.

De PNR-uppgifter som enligt direktivets artikel 8 ska överföras från lufttrafikföretagen (av dem själva eller deras personuppgiftsbiträden) ska samlas in av varje medlemsstats enhet för passagerarinformation. Av artikel 6.1 framgår inledningsvis att för det fall de överförda PNR-uppgifterna avser andra uppgifter än de som anges i direktivets bilaga I, ska enheten för passagerarinformation omedelbart och slutgiltigt radera dessa vid mottagandet. Denna fråga kommer vi att återkomma till i avsnitt 18.3. De PNR-uppgifter som inte gallras bort redan i samband med mottagandet ska föras in i en databas vid enheten för passagerarinformation (artikel 12.1). Samtliga överförda PNR-uppgifter, som inte har raderats vid den inledande gallringen, kommer således att lagras i denna databas.

Det bör av lagen framgå att det vid enheten för passagerarinformation ska finnas en datoriserad uppgiftssamling där de PNR-uppgifter som har överförts från lufttrafikföretagen ska lagras. Med hänsyn till det stora antalet passagerare som reser till och från Sverige varje år kommer uppgiftssamlingen att innehålla miljontals PNR-uppgifter. Uppgiftssamlingen kommer att bestå av ett urval av uppgifter som ska hanteras på ett strukturerat sätt. Uppgifterna ska behandlas för särskilda och begränsade ändamål och vara avgränsade från andra

uppgiftssamlingar. Visserligen kommer uppgiftssamlingen att innehålla vissa fritextfält. Den kommer dock troligen inte att innehålla löpande texter eller elektroniska dokument av olika slag. Detta talar för att det snarare är fråga om ett register i begreppets traditionella bemärkelse än en databas. Dock är de tekniska lösningarna ännu inte uppbyggda och det är därför inte helt klart hur dessa närmare kommer att vara utformade. Vi har därför valt att i implementeringen hålla oss så nära direktivets ordalydelse som möjligt. I lagförslaget används därför ordet databas för att beskriva den datoriserade uppgiftssamlingen.

13.2 Ändamål för behandling av PNR-uppgifter

Vårt förslag: Enheten för passagerarinformation får endast behandla PNR-uppgifter som har överförts från lufttrafikföretagen för uttryckliga ändamål som anges i lagen.

Direktivets bestämmelser

De PNR-uppgifter som har överförts från lufttrafikföretagen i enlighet med direktivets bestämmelser får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Denna utgångspunkt och grundförutsättning framgår av direktivets artikel 1.2 och har behandlats i avsnitt 9.5. I artikel 6.2 finns de närmare bestämmelserna om vad enheten för passagerarinformation får göra med de insamlade PNR-uppgifterna. Här anges att enheten endast får behandla PNR-uppgifterna för följande tre ändamål:

- a) Göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från den berörda medlemsstaten, för att identifiera personer som de behöriga myndigheterna och i förekommande fall Europol behöver utreda ytterligare, på grund av att dessa personer kan vara inblandade i terroristbrott eller grov brottslighet.
- b) I enskilda fall, besvara en vederbörligen motiverad förfrågan som bygger på tillräckliga skäl från de behöriga myndigheterna om att tillhandahålla och behandla PNR-uppgifter i specifika fall i

syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet och tillhandahålla de behöriga myndigheterna eller, när så är lämpligt, Europol resultaten av sådan behandling.

- c) Analysera PNR-uppgifter för att uppdatera och skapa nya kriterier som ska användas vid de bedömningar som genomförs enligt artikel 6.3 b, i syfte att identifiera personer som kan vara delaktiga i terroristbrott eller grov brottslighet.

Våra överväganden

Artikel 6.2 utgör en verksamhetsreglering som anger hur de insamlade PNR-uppgifterna ska behandlas för att uppgifterna ska komma till användning vid bekämpande av terroristbrottslighet eller grov brottslighet. Bestämmelsen utgör dock även en dataskyddsbestämmelse som anger för vilka ändamål de insamlade PNR-uppgifterna över huvud taget får behandlas. Genom ändamålen sätts ramen för vilken behandling som är tillåten och på så sätt kan användning och spridning av personuppgifter begränsas. Av andra bestämmelser i direktivet framgår emellertid att artikel 6.2 inte är helt exklusiv. Av artikel 9 och 11 framgår nämligen att PNR-uppgifter får behandlas även för att lämnas ut till andra medlemsstater och tredjeländer.

Ändamålsbestämning är central i dataskyddsreglering. I 2 kap. 3 § BDL anges att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. I 2 kap. 4 § framgår under vilka förutsättningar personuppgifter får behandlas för ett nytt ändamål. Normalt är det den personuppgiftsansvarige själv som bestämmer ändamålen med en behandling. I registerförfattningar kan det emellertid finnas bestämmelser om ändamålsbestämmelser som kan vara mer eller mindre preciserade. I polisdatalagen finns sådana allmänt formulerade ändamålsbestämmelser för Polismyndighetens del främst i 2 kap. 7–9 §§.

Genom PNR-direktivet sjösätts ett nytt system för inhämtande, användande och utbyte inom EU av uppgifter om flygpassagerare och deras resande. Det är nödvändigt, menar vi, för ett korrekt genomförande av direktivet att i lag reglera för vilka ändamål PNR-uppgifter som mottagits från lufttrafikföretagen får användas. Enligt vår mening bör artikel 6 genomföras genom en paragraf som på ett

enklare sätt beskriver enhetens olika uppgifter och som dessutom inkluderar behandling för sådana ändamål som anges i artiklarna 9 och 11, dvs. behandling för översändande till andra medlemsstater och till tredjeländer.

Bestämmelsen om ändamål kommer att ersätta de ändamålsbestämmelser som anges i 2 kap. 7 och 8 §§ PDL. Den exkluderar även en tillämpning av bestämmelsen om nya ändamål i 2 kap. 4 § BDL. Uppräkningen i bestämmelsen är uttömmande och innebär att endast sådan personuppgiftsbehandling som inryms i något av de i paragrafen angivna ändamålen får äga rum. Dock är behandling alltid tillåten för att uppfylla de syften som anges i 2 kap. TF. Vidare får PNR-uppgifterna alltid behandlas för att besvara en förfrågan från en enskild om huruvida dennes personuppgifter behandlas vid enheten eller för att ge tillsynsmyndigheten tillgång till behandlade uppgifter.

Hur de närmare ändamålen ska regleras i lagen diskuteras nedan.

13.2.1 PNR-uppgifterna får behandlas för att utföra förhandsbedömningar

Våra förslag: Från lufttrafikföretag insamlade PNR-uppgifter får behandlas för att göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från Sverige, för att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att dessa personer kan vara inblandade i terroristbrottslighet eller grov brottslighet. Denna behandling bör i lagen kallas för förhandsbedömning.

Användning av PNR-information i realtid

PNR-uppgifter kan användas för att göra en bedömning av passagerare redan innan de har anlänt till eller avrest från en medlemsstat. Syftet med en sådan användning är att övervaka eller gripa personer innan ett brott har begåtts. Uppgifterna kan även användas för att ingripa mot personer på grund av att ett brott har begåtts eller håller på att begås. PNR-uppgifterna kan således vara ett användbart verktyg för behöriga myndigheter i realtid.

Vidare kan kontroll av PNR-uppgifter före passagerarnas ankomst ge de behöriga myndigheterna möjlighet att göra en mer ingående bedömning av personer som, baserat på objektiva bedömningskriterier och tidigare erfarenheter, kan utgöra ett säkerhetshot. Detta underlättar resandet för andra passagerare och minskar risken för att människor olovligen kontrolleras på grundval av kriterier som nationalitet eller hudfärg.¹

PNR-uppgifterna ger således de behöriga myndigheterna möjlighet att identifiera, dvs. välja ut, personer som kanske inte tidigare varit misstänkta för inblandning i grov brottslighet eller terrorism, men som enligt en analys av uppgifterna kan vara involverade i sådan brottslighet och därför bör bli föremål för ytterligare utredning. Identifieringen av sådana personer ger de behöriga myndigheterna möjlighet att förebygga och avslöja grov brottslighet, inklusive terrorhandlingar.

Genom artikel 6.2 a ges enheten för passagerarinformation en möjlighet att använda de insamlade PNR-uppgifterna för att göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från den berörda medlemsstaten.

Våra överväganden och förslag

Bestämmelsen i artikel 6.2 a bör föras in i lagen i stort sett i enlighet med sin ordalydelse. Således bör det av bestämmelsen framgå att PNR-uppgifterna får behandlas i syfte att identifiera sådana personer som behöver utredas ytterligare. Med att en person har identifierats torde i vanligt språkbruk menas att man har erhållit säkra identitetsuppgifter, såsom namn, födelsedata osv. om personen. För att en sådan identifikation ska kunna ske krävs att det är möjligt att erhålla säkra identitetsuppgifter om den resande. PNR-uppgifterna består dock av sådana uppgifter som har lämnats av passagerarna själva i samband med beställning och bokning av flygresor och anses inte innehålla verifierade identitetsuppgifter. Det vid bokningen uppgivna namnet behöver nämligen inte korrespondera med det namn som anges i en persons pass, eftersom en sådan korrelation inte alltid är nödvändig för att genomföra en resebokning. Säkra identitets-

¹ KOM (2011) 32 slutlig av den 2 februari 2011, s. 6.

uppgifter kan endast erhållas för det fall enheten för passagerarinformation också får tillgång till API-uppgifter, som främst innehåller uppgifter hämtade från den resandes pass. API-uppgifter samlas dock inte in inför resor inom EU. Säkra identitetsuppgifter kan således inte erhållas avseende de personer som endast företar resor inom unionen. Med hänsyn härtill bör med ordet identifiering i sammanhanget förstås att en resenär har valts ut såsom intressant för vidare kontroller. För att undvika missförstånd föreslår vi att orden ”välja ut” användas i lagen i stället för direktivets uttryck.

Syftet med behandlingen är att PNR-informationen ska utredas vidare av nationella behöriga myndigheter eller av Europol. Behandlingen ska således inte ske för att finna personer som bör behandlas vidare vid andra medlemsstaters enheter för passagerarinformation. För det fall enheten skulle finna att den framtagna informationen kan vara av intresse även för en annan medlemstat ska dock informationen sändas även till den medlemsstatens enhet för passagerarinformation. Se vidare i avsnitt 15.3.2.

Bestämmelsen som genomför artikel 6.2 a kommer att behandlas återkommande i betänkandet och i lagförslaget. Av denna anledning och för att förenkla lagtexten föreslår vi att den bedömning som ska göras enligt bestämmelsen benämns som förhandsbedömning. Benämningen bör föras in i lagtexten.

13.2.2 Förfarandet vid förhandsbedömningar

Vårt förslag: Vid förhandsbedömningar får PNR-uppgifter

1. jämföras med register eller andra uppgiftssamlingar som är relevanta för ett eller flera av syftena att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet, eller
2. behandlas enligt på förhand utformade och fastställda kriterier som är riktade, proportionella och avgränsade och som inte grundas på känsliga personuppgifter.

Som tidigare framgått kommer enheten för passagerarinformation att få del av PNR-uppgifter från miljontals flygresor. För att enheten utifrån dessa uppgifter ska kunna välja ut de personer som kan vara

intressanta för vidare utredning bör den ha tillgång till vissa hjälpmedel. Således anges i artikel 6.3 att enheten vid förhandsbedömningarna får jämföra PNR-uppgifter dels med uppgifter i relevanta databaser, dels med på förhand fastställda kriterier.

Jämförelser med relevanta databaser

Direktivet anger inte vilka databaser eller register som får användas vid förhandsbedömningarna. I artikel 6.3 a anges i stället att databaserna ska vara relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och att det inkluderar databaser över personer eller föremål som är eftersökta eller finns uppförda på en spärlista. Vidare anges att jämförelserna ska göras i enlighet med unionsbestämmelser eller internationella eller nationella bestämmelser som är tillämpliga på sådana databaser.

Direktivet innehåller således en generell begränsning av vilka typer av uppgiftssamlingar PNR-uppgifterna kan jämföras med. Medlemsstaterna får dock själva bestämma vilka uppgiftssamlingar som ska användas. Artikel 6.3 är inte heller tvingande utan ger endast medlemsstaterna en möjlighet att söka mot relevanta databaser.

Våra överväganden

Artikel 6.3 a är av sådan vikt för PNR-uppgifternas användning att den bör genomföras i lagen. Av bestämmelsen bör framgå att PNR-uppgifter vid förhandsbedömningar – utöver jämförelser med tidigare uppgifter i PNR-databasen – får jämföras med sådana register eller andra uppgiftssamlingar som är relevanta för direktivets syften, dvs. för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet. De aktuella uppgiftssamlingarna utgör normalt i traditionell mening register och inte databaser. Vi föreslår därför att begreppen register eller andra uppgiftssamlingar används i lagtexten.

Det är i nuläget inte klart vilka register eller uppgiftssamlingar som PNR-uppgifterna kommer att jämföras med vid enheten för passagerarinformation. De man kan tänka sig är i fråga om EU-register t.ex. Sis-registret, där personer efterlysta för brott registreras. I fråga om internationella register finns t.ex. Interpols databas där kända

internationella brottslingar kan registreras. Ett nationellt register man kan tänka sig är misstankeregistret. Som angetts i avsnitt 10.5 är det vår utgångspunkt att enheten, när den startar det operativa arbetet, kommer att använda sig av de system som den nuvarande registerförfattningsregleringen ger förutsättningar för och som regleras i annan författning. Bestämmelser härom behöver därför inte föras in i denna reglering. Dock krävs, som angetts ovan, att registren eller uppgiftssamlingarna är relevanta för PNR-direktivets syften.

Det bör i sammanhanget noteras att vissa uppgiftssamlingar som kan bli aktuella för jämförelser kan innehålla uppgifter om personer som inte faller inom direktivets tillämpningsområde eftersom de t.ex. är misstänkta för annat slags eller lindrigare brottslighet. En automatisk sökning i dessa uppgiftssamlingar skulle kunna innebära att PNR-uppgifterna leder till träffar avseende sådan brottslighet som inte omfattas av direktivet. Dock kan en träff avseende exempelvis ett lindrigare brott, en person som är försvunnen eller ett dokument som är stulet, leda till andra antaganden och annan information, som i sin tur leder till misstanke om inblandning i grov brottslighet eller terroristbrottslighet. Sökningarna i de olika databaserna bör därför, enligt vår mening, inte begränsas till att endast omfatta sådana brott som avses i direktivet.

Jämförelser med på förhand fastställda kriterier

Vid förhandsbedömningarna får enheten för passagerarinformation enligt artikel 6.3 b även behandla PNR-uppgifter i enlighet med på förhand fastställda kriterier. Med behandling i enlighet med på förhand fastställda kriterier avses vad som i polisiära sammanhang kallas för profilering. Med en profil menas en icke personanknuten företeelse och kan avse uppgifter om exempelvis avreseort, resrutt, betalningssätt, bokningsrutin, bagage m.m. Vissa mönster och beteende i resandeflödet utgör riskprofiler som kan ge anledning att kontrollera en viss person. En profil används således för att leta efter mönster som kan indikera att en person är av intresse för vidare kontroller.

En analys av PNR-uppgifter kan exempelvis ge indikationer på de vanligaste rutterna för människohandel och narkotikahandel, information som sedan kan användas som bedömningskriterier. I ett konkret fall från en medlemsstat avslöjade PNR-analysen en grupp

människohandlare som alltid reste samma väg. De använde falska handlingar för att checka in till en flygning inom EU samtidigt som de använde äkta handlingar för att checka in till en annan flygning med destination i ett tredjeland. Så snart de befann sig i flygplatsens lounge-område gick de ombord på det plan som skulle avgå till en destination inom EU. Utan hjälp av PNR-uppgifter skulle det ha varit omöjligt att nysta upp detta nätverk för människohandel.²

I artikel 6.4 anges att förhandsbedömningen av passagerare i enlighet med på förhand fastställda kriterier ska utföras på ett icke-diskriminerande sätt. De på förhand fastställda kriterier måste vara riktade, proportionella och specifika. Medlemsstaterna ska se till att kriterierna fastställs och regelbundet ses över av enheterna för passagerarinformation i samarbete med behöriga myndigheter. Dessa på förhand fastställda kriterier får dessutom under inga omständigheter vara baserade på känsliga personuppgifter.

Inte heller direktivets bestämmelse om de på förhand fastställda kriterierna i artikel 6.3 b är tvingande. Det utgör således en frivillig möjlighet för medlemsstaterna att använda sig av profilering. Om en profilering sker ska dock bestämmelserna i artikel 6.4 vara uppfyllda.

Våra överväganden

Även artikel 6.3 b och 6.4 bör genomföras i lagen. Det bör här framgå att PNR-uppgifter får behandlas i enlighet med på förhand utformade och fastställda kriterier i samband med förhandsbedömningar av passagerare. Vidare bör det anges att dessa kriterier ska vara riktade och proportionella. Enligt vår mening utgör *avgränsade* ett bättre ord i sammanhanget än *specifika*, varför vi väljer att också använda det i lagen.

Förbudet mot behandling av känsliga personuppgifter bör föras in i lagen genom en hänvisning till den bestämmelse i brottsdatalagen där dessa uppgifter behandlas. Dock följer det redan av 1 kap. 9 § RF att en myndighet inte ska utföra sitt arbete på ett diskriminerande sätt. Enligt vår mening saknas det därför anledning att i lagen särskilt ange detta kriterium.

² A.a. s. 5.

Det kan i förordning regleras att kriterierna ska fastställas och regelbundet ses över av enheten för passagerarinformation i samarbete med behöriga myndigheter.

Konsekvenser av förhandsbedömningarna

I artikel 6.9 anges att konsekvenserna av förhandsbedömningarna inte får äventyra rätten för personer som åtnjuter fri rörlighet enligt unionsrätten att resa in på den berörda medlemsstatens territorium i enlighet med Europaparlamentets och rådets direktiv 2004/38/EG³. När bedömningarna sker i samband med flygningar inom EU mellan medlemsstater för vilka kodexen om Schengengränserna⁴ är tillämplig, ska vidare konsekvenserna av sådana bedömningar vara förenliga med den förordningen.

I rådets direktiv 2004/38/EG slås unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorium fast. Direktivet har genomförts i Sverige främst genom ändrade bestämmelser i utlänningslagen.

Kodexen om Schengengränserna syftar till att precisera unionens bestämmelser om gränskontroller vid personers passage av EU:s yttre gränser och tillfälliga inre gränser. Kodexen gäller som lag i Sverige. Enligt gränskodexen får alla personer, oavsett nationalitet, passera de inre gränserna vid vilket övergångsställe som helst, utan att någon in- eller utresekontroll genomförs. Detta utesluter inte möjligheten att den nationella polismyndigheten utövar sina befogenheter, på villkor att det inte har samma verkan som gränskontroller. Därutöver finns det i gränskodexen bestämmelser om att de EU-länder som tillhör Schengenområdet under vissa förutsättningar får återinföra gränskontroller.

³ Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier och om ändring av förordning (EEG) nr 1612/68 och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG.

⁴ Direktivet hänvisar till Europaparlamentets och rådets förordning (EG) nr 562/2006 av den 15 mars 2006 om en gemenskapskodex om gränspassage för personer (kodex om Schengengränserna). Den har emellertid ersatts av Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna).

PNR-direktivet syftar inte till att förbättra gränskontrollerna eller reglera invandringen, utan syftar till att bekämpa terroristbrottslighet och grov brottslighet. Direktivet innehåller vidare inga bestämmelser om avvisning eller utvisning av personer. Med hänsyn härtill är det vår uppfattning att den grundbestämmelse om att PNR-uppgifter endast får användas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet som föreslås införas i lagen, är tillräcklig för att säkerställa att kraven i artikel 6.9 efterlevs.

13.2.3 PNR-uppgifterna får behandlas för att överföra PNR-information till behöriga mottagare och tredjeland

Våra förslag: Från lufttrafikföretag insamlade PNR-uppgifter får behandlas för att enheten ska kunna fullgöra sina uppgifter enligt direktivet att på eget initiativ överföra PNR-information eller för att besvara en begäran från en behörig mottagare. Vidare ska i ändamålsbestämmelsen framgå att PNR-uppgifter får överföras till tredjeland enligt bestämmelserna om detta i lagen.

Reaktiv behandling av PNR-uppgifter

PNR-uppgifter behöver inte endast användas i realtid för att förhindra brottslighet. Uppgifterna kan även användas reaktivt efter det att ett brott har begåtts för att ta fram bevisning och, i förekommande fall, hitta medbrottslingar och nysta upp kriminella nätverk. I brottsutredningar kan äldre PNR-uppgifter användas exempelvis för att kartlägga var en misstänkt har befunnit sig vid vissa tidpunkter, vem personen har rest med och vem som har betalat för resan. Exempelvis kan kreditkortsinformation som ingår bland PNR-uppgifterna göra det möjligt för de behöriga myndigheterna att identifiera och styrka kopplingar mellan en person och en känd brottsling eller ett kriminellt nätverk. Ett exempel från en medlemsstat rörde storskalig människo- och narkotikahandel med anknytning till en medlemsstat och flera tredjeländer. Karteller importerade narkotika till flera olika destinationer i Europa. Människor som själva var offer för människohandel tvingades svälja narkotika och transportera

den till EU. Personerna identifierades genom att det på grundval av PNR-uppgifter kunde konstateras att de hade köpt flygbiljetten med stulna kreditkort. Detta ledde till gripanden i den berörda medlemsstaten. På denna grund skapades ett bedömningskriterium som i sig ledde till flera ytterligare gripanden i andra medlemsstater och tredjeländer.⁵

Lagrade PNR-uppgifter kan även vara av intresse i underrättelseverksamhet eller annan verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet.

Behöriga myndigheter som tror sig kunna ha nytta av äldre PNR-uppgifter kan vända sig till enheten för passagerarinformation och begära att få ut äldre PNR-uppgifter som kan vara av värde för dem i deras arbete. Således anges i artikel 6.2 b att PNR-uppgifterna får användas i enskilda fall för att besvara en vederbörligen motiverad förfrågan (*request* i den engelska versionen av direktivet) från en behörig myndighet om att tillhandahålla och behandla PNR-uppgifter i ett specifikt fall. Förfrågan ska bygga på tillräckliga skäl och vara ställd i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet. Resultatet av en sådan behandling av PNR-uppgifter ska enligt bestämmelsen lämnas till de behöriga myndigheterna eller, när så är lämpligt, till Europol.

Av andra bestämmelser i direktivet framgår att enheten för passagerarinformation under vissa förutsättningar även ska besvara förfrågningar från andra än behöriga myndigheter om att få ta del av sådana PNR-uppgifter som lagras vid enheten. Sådana förfrågningar kan komma från andra medlemsstaters enheter för passagerarinformation (artikel 9.2), myndigheter som har utsetts till behöriga i andra medlemsstater (artikel 9.4), Europol (artikel 10.2) och tredjeländer (artikel 11.2).

Våra överväganden

Bestämmelsen i artikel 6.2 b bör genomföras på så sätt att det av bestämmelsen framgår att PNR-uppgifter som överförts från lufttrafikföretagen får behandlas för att besvara en begäran från samtliga mottagare som enligt direktivet är behöriga att motta PNR-

⁵ KOM (2011) 32 slutlig av den 2 februari 2011, s. 5 f.

uppgifter från enheten för passagerarinformation och för att tillhandahålla dessa mottagare resultatet av sådan behandling. Detta kan lösas genom att det i lagen hänvisas till behöriga mottagare i stället för endast behöriga myndigheter och Europol. Vidare bör framgå att PNR-uppgifter får behandlas av enheten för att den på eget initiativ ska överföra uppgifter till andra medlemsstater enligt artikel 9.1. De närmare förutsättningarna som anges i artikel 6.2 b och i artikel 9 bör dock inte framgå av ändamålsbestämmelsen utan genomföras i andra bestämmelser i lagen och som vi behandlar i avsnitt 15.

Enligt artikel 11 i direktivet får i vissa fall PNR-uppgifter behandlas genom att överföras till tredjeland. Även detta bör framgå i lagens ändamålsbestämmelse. Förutsättningarna för överföring till tredjeland behandlar vi i avsnitt 17.

13.2.4 PNR-uppgifterna får behandlas för att utforma kriterier

Vårt förslag: Från lufttrafikföretag insamlade PNR-uppgifter får analyseras för att uppdatera eller skapa nya kriterier som ska användas vid förhandsbedömningarna.

Som tidigare har angetts ska de på förhand fastställda kriterierna regelbundet ses över av enheterna för passagerarinformation i samarbete med behöriga myndigheter. De PNR-uppgifter som har samlats in från lufttrafikföretagen och finns lagrade i databasen vid enheten för passagerarinformation får således även användas för att uppdatera riskprofilerna eller skapa nya sådana. Det är därmed möjligt för personalen inom enheten att gå igenom de PNR-uppgifter som finns samlade i databasen för att leta efter mönster som kan indikera att personer kan vara av intresse för vidare kontroller. PNR-uppgifterna kan på detta sätt användas för att förbättra urvalet av de passagerare som kan komma att vara intressanta för vidare granskning. Detta framgår av artikel 6.2 c.

Enligt vår mening bör även denna ändamålsbestämmelse föras in i lagen. Det bör här framgå att PNR-uppgifter får analyseras för att uppdatera eller skapa nya kriterier som ska användas vid förhandsbedömningarna.

13.2.5 PNR-information som tas emot från andra medlemsstaters enheter för passagerarinformation

Vårt förslag: PNR-information som enheten för passagerarinformation mottar från motsvarande enheter i andra medlemsstater får endast behandlas i syfte att vidarebefordra uppgifterna till behöriga myndigheter för fortsatt användning för ett eller flera av syftena att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

En enhet för passagerarinformation som vid sin förhandsbedömning av passagerare har identifierat en person kan i vissa fall överföra PNR-informationen om denna person inte bara till en myndighet som har utsetts till behörig i det egna landet utan även till en motsvarande enhet i en annan medlemsstat. Detta framgår av artikel 9.1 och behandlas närmare i avsnitt 15.3.2. Vår enhet för passagerarinformation kommer således inte bara att behandla PNR-uppgifter som har kommit in från lufttrafikföretagen till den egna databasen, utan kommer därutöver också att motta och behandla PNR-information från andra medlemsstaters motsvarande enheter. Enligt artikel 9.1 ska den mottagande enheten överföra de på detta sätt mottagna uppgifterna till sina behöriga myndigheter. De uppgifter som överförs från andra länders enheter för passagerarinformation ska således lämnas vidare från enheten till de nationella behöriga myndigheterna, och inte bevaras vid enheten för passagerarinformation.

Vidare kommer enheten för passagerarinformation att motta PNR-information från andra medlemsstaters enheter för passagerarinformation som svar på sådana förfrågningar som enheten ställt till den andra enheten (artikel 9.2). Det framgår dock inte av direktivet vad enheten ska göra med denna information. Enligt vår bedömning bör enheten för passagerarinformation uppfattas som en förmedlare av PNR-information och inte som en slutlig destinationsinstans när det gäller det internationella utbytet av PNR-information. Således ska PNR-information som finns sparad i databaser vid andra medlemsstaters enheter för passagerarinformation endast hämtas in när det är tillåtet enligt direktivet och därefter föras vidare till behöriga myndigheter. PNR-information kan därmed, enligt vår bedömning, inte hämtas in från andra medlemsstater för att enheten för passagerarinformation ska kunna verifiera sin egen databas eller finslipa

sina kriterier etc. Den PNR-information som hämtas in med stöd av bestämmelserna ska således, enligt vår bedömning, inte bevaras hos enheten, i vart fall inte någon längre tid. Den frågan återkommer vi till i avsnitt 18 om gallring.

Den behandling som ska ske av PNR-information som mottagits från andra medlemsstater ska således syfta till att uppgifterna ska föras vidare till behöriga myndigheter för användning för något av de syften som framgår av artikel 1.2 i direktivet. Detta bör enligt vår mening komma till klart uttryck i lagen. Vi föreslår således en bestämmelse som anger att den PNR-information som enheten för passagerarinformation mottar från motsvarande enheter i andra medlemsstater endast får behandlas i syfte att överföra informationen till behöriga myndigheter för att där komma till användning i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Det finns dock inget som hindrar enheten från att inte överföra all denna information, för det fall enheten skulle bedöma den totalt onödig för de behöriga myndigheterna. Hur enheten i övrigt ska gå till väga vid överlämnandet av PNR-information till behöriga myndigheter behandlas i avsnitt 15.2.2.

13.3 Maskering av PNR-uppgifter

Våra förslag: En bestämmelse förs in i lagen som anger att vissa PNR-uppgifter ska maskeras sex månader efter mottagandet från lufttrafikföretagen. Dessa uppgifter räknas upp i lagen och motsvarar artikel 12.2 i direktivet.

Vidare ska det föras in definitioner i lagen som anger att

- med *maskering* ska förstås en åtgärd som innebär att tillgängliga uppgifter som direkt kan hänföras till en fysisk person görs osynliga för en användare av ett informationssystem som saknar särskild behörighet för åtkomst till uppgifterna,

- med *maskerade PNR-uppgifter* avses personuppgifter som genomgått en maskering, och
- med *avmaskerade PNR-uppgifter* avses fullständiga flygpassageraruppgifter där personuppgifter tidigare genomgått en maskering.

13.3.1 Direktivets bestämmelser

Enligt direktivets artikel 12.2 ska PNR-uppgifterna i PNR-databasen avidentifieras genom maskering efter en inledande sexmånadersperiod. Med *avidentifiering genom maskering av uppgifter* menas, enligt direktivets definition i artikel 3.10, att göra de uppgifter som kan användas för att omedelbart identifiera den registrerade osynliga för en användare.

Av artikel 12.2 framgår således att vid utgången av en period på sex månader efter överföringen från lufttrafikföretagen ska PNR-uppgifterna avidentifieras genom maskering av vissa särskilt uppräknade uppgifter som kan användas för att omedelbart identifiera de passagerare som PNR uppgifterna avser.

I artikelns uppräkning ingår

- a) namn, inklusive namn på andra passagerare i PNR samt antal passagerare i PNR som reser tillsammans,
- b) adress och kontaktuppgifter,
- c) alla former av betalningsinformation, inbegripet faktureringsadress om denna innehåller uppgift som kan användas för att omedelbart identifiera den passagerare som personuppgiftssamlingar avser eller andra personer,
- d) uppgifter om bonusprogram,
- e) allmänna anmärkningar, om dessa innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som personuppgiftssamlingar avser, samt
- f) alla API-uppgifter som samlats in.

13.3.2 Våra överväganden och förslag

Av direktivets skäl 25 framgår att syftet med maskering av PNR-uppgifter som direkt identifierar en person är att en oproportionerlig användning av uppgifterna ska undvikas. Tanken torde vara att efter hand som tiden går efter det att det inte längre är aktuellt att göra en förhandsbedömning av passagerare, minskar behovet av tillgång till direkt utpekande personuppgifter om passagerare. Efter så lång tid som sex månader torde det i huvudsak endast vara vid undersökningar på särskild förfrågan som tillgång till sådana uppgifter om passagerare kan vara av intresse.

Artikel 12.2 är en bestämmelse som enligt vår uppfattning måste genomföras genom författningsreglering. Den har en central ställning och bör därför genomföras i den nya lagen.

I den svenska översättningen av direktivet används begreppet av-identifiering genom maskering för att beskriva denna ordning. Med avidentifierade data avses dock i andra lagstiftningar och i andra sammanhang att kopplingen mellan uppgifterna och en fysisk person har eliminerats. I PNR-direktivet är inte tanken att kopplingen mellan PNR-uppgifterna och den fysiska personen ska brytas. Under vissa förutsättningar ska nämligen de fullständiga uppgifterna kunna plockas fram. Regleringen i direktivet avser i stället att direkt utpekande personuppgifter ska göras osynliga för en användare. Ordet avidentifiering bör därför undvikas i lagförslaget.

Ordet maskering är ett tämligen ovanligt begrepp i lagstiftningssammanhang. I artikel 4 i dataskyddsförordningen definieras det till synes näraliggande begreppet pseudonymisering. Vi har övervägt om det vore ett ord som lämpligen borde användas i stället för maskering. Begreppet pseudonymisering definieras emellertid i förordningen med att det avser ”behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person”. Enligt vår mening kommer det beträffande det som kallas maskerade PNR-uppgifter i direktivet att brista i den förutsättning i dataskyddsförordningen som kräver separat förvaring. Det som avses ske med PNR-uppgifterna är i stället, i praktiken,

att behörigheten för åtkomst eller tillgång till de direkt identifierande uppgifterna ska snävas in så att en vanlig befattningshavare vid enheten för passagerarinformation som dittills haft tillgång till fullständiga uppgifter, inte längre kommer att ha det. Begreppet pseudonymiserade PNR-uppgifter bör således inte användas i den nya lagen.

Vi bedömer det i stället som lämpligast att använda samma begrepp som i direktivet, dvs. maskering. Ordet förekommer redan i författningstext, nämligen i lagen (2005:900) om förbud mot maskering i vissa fall. Den lagen innehåller förbud att i vissa sammanhang, t.ex. en demonstration, helt eller delvis täcka för ansiktet på ett sätt som försvårar identifikation. Att ordet förekommer i ett annat slags sammanhang med en annorlunda innebörd utgör enligt vår mening inget hinder mot att vi använder ordet i den nya lagen för att genomföra direktivets bestämmelse om den åtgärd som avses där. Detta gäller särskilt eftersom användningsområdena i den nyssnämnda lagen och den av oss föreslagna nya lagen är så pass åtskilda att risken för missuppfattningar om innebörden av ordet i den ena eller andra lagen inte torde kunna uppstå. Vi föreslår således en bestämmelse om att PNR-uppgifter ska maskeras sex månader efter mottagandet från lufttrafikföretagen.

Med maskering ska förstås en åtgärd som innebär att tillgängliga uppgifter som direkt kan hänföras till en fysisk person görs osynliga för en användare av ett informationssystem som saknar särskild behörighet för åtkomst till uppgifterna. Detta föreslår vi ska definieras i lagen.

Vi föreslår också att det i lagen definieras att med maskerade PNR-uppgifter avses personuppgifter som genomgått en maskering samt att med avmaskerade PNR-uppgifter avses fullständiga flygpassageraruppgifter där personuppgifter tidigare genomgått en maskering.

Direktivets uppräkningslista av de uppgifter som ska maskeras är uttömmande. Bestämmelsen i artikel 12.2 bör genomföras i den nya lagen genom en motsvarande uppräkningslista, men med några språkliga justeringar enligt följande.

I direktivet anges under punkten a namn, inklusive namn på andra passagerare i PNR samt antal passagerare i PNR som reser tillsammans. Med PNR torde i sammanhanget avses passageraruppgiftssamlingen. Det är, enligt vår bedömning, tillräckligt om det i lagen

anges att maskering ska ske av alla namnuppgifter samt av uppgifter om antalet passagerare som reser tillsammans.

Under punkten c anges alla former av betalningsinformation, inbegripet faktureringsadress, om denna innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som passageraruppgiftssamlingen avser eller andra personer. All betalningsinformation som kan användas för att direkt identifiera en person ska alltså maskeras, oavsett om denna person är en passagerare eller inte. Detta bör framgå av vår bestämmelse.

När det gäller de allmänna anmärkningarna enligt punkten e ska dessa maskeras om de innehåller uppgifter som kan användas för att direkt identifiera en passagerare. Även detta bör framgå av bestämmelsen.

13.4 Begränsad tillgång till maskerade uppgifter

Våra förslag: Det ska införas ett författningsreglerat krav på att tillgången till maskerade uppgifter ska vara strikt begränsad. Det kan ske genom att det i förordningen förs in en bestämmelse om att endast dataskyddsombudet samt den som har ett särskilt behov av fullständiga uppgifter för att kunna utföra sina arbetsuppgifter vid enheten för passagerarinformation ska kunna ges behörighet för tillgång till maskerade PNR-uppgifter. Behörigheten ska bara få utnyttjas när det i ett enskilt fall är absolut nödvändigt med tillgång till fullständiga uppgifter.

Enligt direktivets skäl 25 bör åtkomst till maskerade uppgifter endast beviljas under mycket strikta och begränsade villkor för att säkerställa högsta möjliga nivå av dataskydd. Som ett komplement till bestämmelserna om maskering bör det därför föras in bestämmelser som ställer krav på att behörigheten för åtkomst till fullständiga PNR-uppgifter som har maskerats ska vara särskilt begränsad. Sådana bestämmelser bör kunna tas in i den till den nya lagen anslutande förordningen. Vi föreslår där en bestämmelse som anger att endast dataskyddsombudet samt den som har ett särskilt behov av fullständiga uppgifter för att kunna utföra sina arbetsuppgifter vid enheten ska kunna ges behörighet för tillgång till uppgifterna. Vi föreslår även att behörigheten bara får utnyttjas när det i ett enskilt fall är

absolut nödvändigt med tillgång till fullständiga uppgifter. Som framgår av artikel 6.7 ska enhetens dataskyddsbud ha åtkomst till alla uppgifter som enheten behandlar. Dataskyddsbudet måste därför ha tillgång även till de fullständiga uppgifterna bakom maskerade PNR-uppgifter. Givetvis måste även befattningshavare på enheten för passagerarinformation som hanterar frågor om utlämnande av avmaskerade uppgifter ha tillgång till uppgifterna. Vidare måste någon befattningshavare finnas som kan möta andra slags behov av att kunna ta fram fullständiga uppgifter, exempelvis på tillsynsmyndighetens begäran i samband med tillsyn eller i samband med att en enskild registrerad passagerare begär information om behandlingen. Det följer dock av den föreslagna bestämmelsen att behörighetstilldelningen till maskerade personuppgifter ska vara mycket strikt. Vilka befattningshavare på enheten som kan komma i fråga bör dock överlämnas åt Polismyndigheten att bestämma. Det finns som vi ser det inget hinder i och för sig mot att befattningshavare som har sin grundanställning utanför Polismyndigheten, t.ex. hos Tullverket eller Säkerhetspolisen, ges sådan behörighet, förutsatt att detta skett efter en vederbörligen noggrann behovsanalys.

14 PNR-direktivets förhållande till API-direktivet och dess genomförande i svensk rätt

14.1 PNR- och API-uppgifter

Som har framgått av tidigare avsnitt kan de uppgifter som överförs från lufttrafikföretagen avse såväl PNR- som API-uppgifter. Den förhandsinformation om passagerare (API-uppgifterna) som samlas in utgörs främst av sådan information som finns på passets maskinläsbara del, såsom namn, födelsedatum, nationalitet och passnummer. API-uppgifterna innehåller även viss information om resrutten, såsom avgångs- och ankomstort, beräknad avgångs- och ankomsttid samt flygnummer. Uppgifterna anses utgöra verifierbar information. PNR-uppgifterna däremot består, som tidigare angetts, av sådan information om passagerare som samlas in vid beställning och bokning av flygresor. PNR-uppgifterna kan beskriva vart och när en passagerare har tänkt flyga, hur bokningen är gjord och om någon ytterligare service kommer att behövas under resan. Sådan information anses inte vara verifierad. Det uppgivna namnet behöver inte korrespondera med det namn som anges i en persons pass, eftersom en sådan korrelation inte alltid är nödvändig för att genomföra en resebokning.

En viss överlappning mellan vad som är en PNR-uppgift och vad som är en API-uppgift kan förekomma. Vissa lufttrafikföretag lagrar insamlade API-uppgifter som en del av PNR-uppgifterna, andra gör det inte. Sådana API-uppgifter som finns på passets maskinläsbara del samlas endast in av lufttrafikföretagen inför resor till och från länder utanför Schengensamarbetet. Inom Schengenområdet råder passfrihet och de uppgifter som endast finns på passets maskinläsbara del samlas därmed inte in. PNR-uppgifter samlas dock in inför samtliga flygresor.

De API-uppgifter som är kopplade till en viss person blir tillgängliga för de lufttrafikföretag som utför reguljärflygningar i samband med incheckningen. En incheckning kan vanligtvis ske via internet upp till 48 timmar före flygets avgång. Incheckning kan även ske vid disk på flygplatsen och passet läses då av maskinellt. De API-uppgifter som är knutna till en person läggs då samman med uppgifterna om den avgående flighten. Vid incheckning via internet kan passageraren själv fylla i sina pass- och personuppgifter. Uppgifterna blir då verifierade först när passet läses av maskinellt på flygplatsen i samband med ombordstigningen. PNR-uppgifterna blir tillgängliga för de lufttrafikföretag som utför reguljärflygningar i samband med att uppgifterna läggs in i bokningssystemen.

För de lufttrafikföretag som utför charterflygningar blir endast en mindre del av PNR-uppgifterna tillgängliga. Detta sker i samband med att uppgifterna överförs från researrangörerna inför flygningen. Tidpunkten för överföringen kan variera. Vid flygningar till tredje-länder får de lufttrafikföretag som utför charterflygningar även del av API-uppgifter genom ett särskilt meddelande, som ska vidarebehandlingas till ankomstlandet.

Överförda API-uppgifter utgör huvudsakligen ett verktyg för identifiering. Uppgifterna kan således användas för att underlätta och påskynda identitetskontrollen av passagerare vid gränsen. Tillgång till API-uppgifter kan också göra det möjligt att förhindra att personer som till exempel har belagts med uppehållsförbud reser in i landet. Uppgifterna kan även göra det möjligt att utföra en utökad gränskontroll av vissa i förväg identifierade personer. Uppgifterna kan således användas som ett led i gränskontrollerna. API-uppgifter kan dock även användas av myndigheterna för att de även i andra fall ska kunna identifiera misstänkta och eftersökta personer. Uppgifterna kan således komma till användning i underrättelsearbetet med att exempelvis kartlägga var vissa personer har befunnit sig vid olika tidpunkter. Eftersom API-uppgifterna avser verifierbara uppgifter om en persons identitet är de värdefulla för att jämförelser mot olika databaser ska kunna genomföras.

PNR-uppgifter används snarare som ett verktyg för underrättelsearbetet än som ett verktyg för identitetskontroll. Uppgifterna används främst för att göra riskbedömningar av passagerare och för att välja ut personer som skulle kunna vara av intresse för vidare kontroller, men som inte är misstänkta sedan tidigare. Uppgifterna

kan även användas för att analysera och fastställa misstänkta rese- och beteendemönster. PNR-uppgifterna kan vidare användas i samband med brottsutredningar och för lagföringsåtgärder.

Det kan innebära ett mervärde att behandla API-uppgifter tillsammans med PNR-uppgifter. Med hjälp av API-uppgifterna kan en individs identitet säkerställas. De misstänkta rese- och beteendemönster som kan upptäckas med hjälp av PNR-uppgifterna kan därmed matchas med en identitetsuppgift. Sådana korsjämförelser kan minimera risken för att oskyldiga personer kontrolleras och utreds.

API-direktivet¹ reglerar, som har beskrivits i avsnitt 4.5, transportörens ansvar för att förse nationella myndigheter med API-uppgifter vid ankommande resor från tredjeländer som står utanför Schengen-samarbetet. Direktivet syftar, enligt artikel 1, till att förbättra gränskontrollerna och bekämpa olaglig invandring. API-direktivet har i svensk rätt genomförts främst genom vissa bestämmelser i utlänningslagen (2005:716) samt genom lagen (2006:444) om passagerarregister. Enligt uppgift från kommissionen kommer en översyn av direktivet att ske under år 2017.

14.2 Vårt uppdrag i denna del

I kommittédirektiven framhålls att regeringen i skrivelsen Förebygga, förhindra, försvåra – den svenska strategin mot terrorism (skr. 2014/15:146) angett att systemet för hantering av flygpasageraruppgifter bör samordnas med systemet för API-uppgifter, eftersom de tillsammans kan vara ett användbart verktyg i terrorismbekämpningen. Mot denna bakgrund ska utredningen

- analysera om och i så fall hur PNR-direktivet påverkar regleringen i 9 kap. 3 a § utlänningslagen och lagen om passagerarregister, dvs. det svenska genomförandet av API-direktivet,
- föreslå hur systemet med flygpasageraruppgifter ska möjliggöra hantering av både PNR-uppgifter och API-uppgifter, och
- föreslå de författningsändringar som bedöms nödvändiga.

¹ Rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare.

14.3 Direktivens olika mål och syften

API-direktivet är en rättsakt som bygger vidare på Schengenregelverket. Direktivet har tillkommit för att den olagliga invandringen ska kunna bekämpas effektivt och gränskontrollerna förbättras (se skäl 1). I direktivets artikel 1 anges således att direktivet syftar till att förbättra gränskontrollerna och bekämpa olaglig invandring. Att detta är direktivets syften uttrycks också i skäl 3, 7, 9, 11 och 12. Av skäl 2 framgår att rådet antagit en förklaring om terrorism, i vilken det betonats behovet av att påskynda behandlingen av åtgärder på det området och påskynda arbetet med ett förslaget rådsdirektiv om skyldighet för transportörer att lämna uppgifter om passagerare. Detta har i det svenska genomförandet uttryckts som att direktivet också utgör ett led i kampen mot terrorismen (se prop. 2005/06:129 s. 18 och 20).

API-direktivet har i svensk rätt, som tidigare angetts, införts bl.a. genom lagen om passagerarregister. Av lagens 4 § framgår att passagerarregistret ska föras för att underlätta verkställandet av personkontroller vid Sveriges gräns mot stater som inte tillhör EU och inte heller har träffat avtal om samarbete enligt Schengenkonventionen med konventionsstaterna. I motiven klargörs att uppgifter enligt lagen bör kunna begäras från en transportör när uppgifterna kan antas ha betydelse för personkontrollverksamheten. Med detta begrepp avses verksamheten för att kontrollera invandringen men även för att förebygga och bekämpa därmed förknippad brottslighet (se prop. 2005/06:129 s. 38).

PNR-direktivets mål är, förutom att inrätta en rättslig ram till skydd för användningen av PNR-uppgifter, att trygga säkerheten och skydda personers liv och säkerhet (skäl 5). En effektiv behandling av PNR-uppgifter har ansetts nödvändig för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten. En sådan behandling av PNR-uppgifter har även ansetts nödvändig för att samla in bevisning och i förekommande fall för att hitta medbrottslingar och avslöja kriminella nätverk (skäl 6). PNR-direktivet kan således sägas ha ett brottsbekämpande syfte där målsättningen är att trygga den allmänna säkerheten. PNR-uppgifter får dock endast användas för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet (se t.ex. artikel 1).

14.3.1 Innebörden av den personkontroll som görs inom ramen för gränskontrollen

Sverige deltar sedan år 2001, i likhet med ett flertal andra EU-stater, i Schengensamarbetet. Schengensamarbetet kan sägas innefatta två grundtankar, som är starkt sammanlänkade med varandra. Den första är den fria rörligheten för personer, i den betydelsen att personkontrollerna vid nationsgränserna mellan Schengenstater – inre gräns – ska upphöra. Den andra grundtanken är att kampen ska stärkas mot internationell kriminalitet och mot sådan invandring som är illegal.

Vid Schengenterritoriets yttre gränser utförs gränskontroll i enlighet med EU:s kodex om Schengengränserna², som gäller som lag i Sverige. Enligt Schengenregelverket får inre gräns passeras överallt utan att någon in- och utresekontroll genomförs. Medlemsstaterna har dock möjlighet att tillfälligt återinföra gränskontroll vid de inre gränserna, om det uppkommer ett allvarligt hot mot allmän ordning eller inre säkerhet. Regeringen beslutade den 12 november 2015 att tillfälligt återinföra gränskontroll vid inre gräns. De tillfälliga gränskontrollerna gäller alltså.

I Sverige ansvarar Polismyndigheten för kontroll av personer vid de yttre gränserna (9 kap. 1 § utlänningslagen). Tullverket och Kustbevakningen är efter en begäran av Polismyndigheten skyldiga att bistå vid en sådan kontroll. Även Migrationsverket får efter överenskommelse med Polismyndigheten hjälpa till vid kontrollen. Kustbevakningen ska medverka i Polismyndighetens kontrollverksamhet genom att utöva kontroll av sjötrafiken.

Den personkontroll som görs inom ramen för gränskontrollerna syftar i första hand till att fastställa behörigheten för icke-svenska medborgare att resa in och vistas här i landet. I huvudsak inriktas kontrollen på att identitet, pass, visering och andra handlingar är i ordning. Denna del av personkontrollen är ett led i Sveriges reglerade invandring. Personkontrollen syftar dock också till att förhindra gränsöverskridande brottslighet. Någon klar och entydig definition av denna brottslighet finns inte, men den innefattar i vart fall en brottslighet som på olika sätt har koppling till fler länder än Sverige,

² Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna).

bl.a. genom resande- och invandrarströmmar. I begränsat avseende hör till den gränsöverskridande brottsligheten de utlänningar som i strid med utlänningslagens bestämmelser reser in eller vistas i Sverige. Brott mot utlänningslagen kan exempelvis avse utlänningar som vistas i Sverige utan erforderliga tillstånd eller bryter mot återreseförbud. Olika former av smugglingsbrott – av varor, narkotika och människor – är därtill naturligtvis att betrakta som gränsöverskridande brottslighet. Även andra brott kan dock vara gränsöverskridande, om de har koppling till flera länder genom att planering eller genomförande inte enbart sker i Sverige. (Jfr SOU 2004:110 s. 291 och 331 ff.)

Personkontrollens syfte att förhindra gränsöverskridande brottslighet har efter Sveriges inträde i Schengensamarbetet fått en än mer framträdande roll. En av grundtankarna bakom Schengensamarbetet är att genom olika kompensatoriska åtgärder i form av bl.a. ökat polissamarbete och annat rättsligt samarbete förhindra att den fria rörligheten inom Schengen får till följd att kriminella personer och organisationer fritt kan verka inom Schengenområdet. (Se SOU 2004:110 s. 344.)

Kontrollen vid de yttre gränserna har tre huvudinriktningar. Den första är den traditionella gränskontrollen, dvs. kontroll av att den inresande har erforderliga handlingar och uppfyller övriga villkor för inresa i Schengenområdet. Den andra är kontrollen av om den inresande har begått brott eller är efterlyst för brott. Slutligen har den yttre gränskontrollen till syfte att vara ett verktyg för att avvärja hot mot allmän ordning och säkerhet. Personkontrollen vid de yttre gränserna kan således sägas innehålla ett i vid mening brottsförebyggande moment. (Jfr SOU 2004:110 s. 59 och 61, se även prop. 2015/16:65 s. 61 f.)

I förarbetena till lagen om passagerarregister angavs att förbättrade gränskontroller ökar möjligheten att motverka organiserade smugglingsaktioner och att människor utan skyddsbehov luras att till smugglare betala stora summor för att sedan bli avvisade. Förbättrade gränskontroller ansågs även innebära att möjligheterna ökar att tidigt kunna identifiera eventuella terrorister och avvärja nya terroråd (se prop. 2005/06:129 s. 35).

14.4 Överföring av API-uppgifter ska ske även enligt PNR-direktivet

För att uppnå PNR-direktivets mål om att trygga säkerheten och skydda personer från terroristbrottslighet eller grov brottslighet har det ansetts vara av största vikt att alla medlemsstater inför bestämmelser om skyldigheter för lufttrafikföretag att överföra såväl sina PNR-uppgifter som sina API-uppgifter. Således framgår av punkten 18 i direktivets bilaga I att eventuellt insamlade API-uppgifter ingår bland de uppgifter som ska överföras från lufttrafikföretagen till den nationella enheten för passagerarinformation enligt artikel 8.1. I artikel 8.2 anges vidare att direktivets samtliga bestämmelser ska vara tillämpliga även vid överföring av de uppgifterna. Av direktivets skäl 10 framgår att bestämmelserna inte bör påverka tillämpningen av API-direktivet.

Förpliktelser att överföra API-uppgifter finns därmed inte bara i API-direktivet utan även i PNR-direktivet. De API-uppgifter som samlas in enligt PNR-direktivet ska behandlas enligt det direktivet. Samtidigt kan API-uppgifter även samlas in i enlighet med genomförandet av API-direktivet och detta ska inte påverkas av PNR-direktivets bestämmelser. API-direktivet har inte heller upphävts eller ändrats i och med PNR-direktivets antagande.

Vår utmaning är att försöka få genomförandena av de båda direktiven att fungera sida vid sida. Kan något föras ihop? Eller talar övervägande skäl för att genomförandena och tillämpningen av dessa behöver hållas isär?

14.5 Skillnader mellan PNR- och API-direktiven

Det kan inledningsvis konstateras att de båda direktiven har delvis olika, delvis överlappande mål och syften. PNR-direktivet syftar till att skydda den allmänna säkerheten genom att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet, dvs. avser bekämpning av viss brottslighet. API-direktivet däremot syftar till att förbättra gränskontrollerna och bekämpa olaglig invandring. Förbättrade gränskontroller kan visserligen medföra att hot mot den allmänna säkerheten avvärs. De personkontroller som ingår i gränskontrollerna har också som delmål att förhindra

gränsöverskridande brottslighet. API-direktivets syfte att förbättra gränskontrollerna kan därför i en vid mening anses förenligt med PNR-direktivets syfte. Det kan dock konstateras att API-direktivet också har syften som faller utanför brottsbekämpning, nämligen migrationskontroll, se avsnitt 14.3.1.

En ytterligare väsentlig skillnad är att PNR-direktivet inte, såsom API-direktivet, enbart är knutet till resor *från* tredjeland och den gränskontroll som därmed blir aktuell. PNR-direktivet ska ju tillämpas även vid flygresor från Sverige och, på grund av medlemsstaternas åtagande, för resor mellan EU-länder. Terrorism och grov brottslighet utgör visserligen sådan brottslighet som ofta innehåller gränsöverskridande moment. Dock behöver så inte alltid vara fallet. I PNR-direktivets katalog över grov brottslighet ingår brott som naturligen kan ses som gränsöverskridande, såsom t.ex. olaglig handel med narkotika. Brottskatalogen har dock inte något uttalat gränsöverskridande syfte. PNR-direktivet kan således sägas omfatta en rad olika slags brott utan direkt koppling till sådan gränsöverskridande brottslighet som är av intresse vid en gränskontroll. API-direktivets syfte att bekämpa den olagliga invandringen sammanfaller, som angetts ovan, inte uttryckligen med PNR-direktivets syften. Dock ingår vissa brott med koppling till olaglig invandring i PNR-direktivets brottskatalog, t.ex. människohandel och hjälp till olovlig inresa eller olovlig vistelse.

API-direktivet innehåller inte några brottskataloger eller hänvisningar till särskilda brott, såsom PNR-direktivet. De inhämtade API-uppgifterna enligt API-direktivet synes i stället kunna användas för att bekämpa all sorts gränsöverskridande brottslighet. API-direktivet innehåller inte heller någon straffvärdesbegränsning, vilket innebär att det direktivet även kan tillämpas vid mindre grov brottslighet än PNR-direktivet.

API-direktivet ålägger transportörer skyldigheten att överföra API-uppgifterna medan det enligt PNR-direktivet är lufttrafikföretag som åläggs ett ansvar att överföra uppgifter. Med transportör enligt API-direktivet avses varje fysisk eller juridisk person som bedriver yrkesmässig persontrafik luftvägen. Som framgått i avsnitt 11.3 kan också lufttrafikföretagen utgöras av såväl fysiska som juridiska personer. I praktiken torde därmed överföringsskyldigheten träffa samma slags aktörer.

I API-direktivet specificeras ett antal uppgifter som ska överföras av transportörerna. Kön ingår exempelvis inte i uppräknningen. Enligt PNR-direktivet ska i stället lufttrafikföretagen överföra alla de eventuella API-uppgifter som de har samlat in (se vidare om detta i avsnitt 11.4.4).

Direktiven innehåller vidare olika bestämmelser om överföringstider. Enligt API-direktivet ska API-uppgifterna överföras senast vid slutet av incheckningen. Denna tidpunkt har i 9 kap. 3 a § utlänningslagen förtydligats till så snart incheckningen har avslutats. Enligt PNR-direktivet ska överföringen av uppgifter ske vid två tillfällen, det första 24–48 timmar före flygningens avgång, och det andra omedelbart efter det att gatens dörrar har stängts. Därtill anges i API-direktivet att uppgifterna ska överföras på begäran. Enligt PNR-direktivet ska dock överföringarna ske inför varje flygning och inte endast när en begäran härom har framställts. Det finns dock inte, som vi ser det, något som hindrar en stående begäran om överföring av uppgifter enligt API-direktivet.

Enligt PNR-direktivet ska de överförda uppgifterna sparas i en databas vid enheten för passagerarinformation. PNR-direktivet innehåller strikta bestämmelser om hur uppgifterna får behandlas där och hur de behöriga myndigheterna ska få tillgång till uppgifterna. I API-direktivet anges endast att de överförda uppgifterna ska sparas i ett tillfälligt register. Genom det svenska genomförandet gäller en uppgiftsskyldighet i förhållande till Säkerhetspolisen och Tullverket då uppgifter begärs ut för personkontroll vid inresa från tredjeland. Regeringen får också meddela föreskrifter om att uppgifter i registret ska lämnas ut även till andra myndigheter. Säkerhetspolisen har också direktåtkomst till uppgifterna i passagerarregistret. Tullverket har nyligen i en framställan till regeringen begärt att få direktåtkomst till passagerarregistret. Några sådana lösningar är dock inte aktuella för genomförandet av PNR-direktivet (se avsnitt 10.4.1).

En stor skillnad mellan de båda direktiven är vidare direktivens olika lagringstider för de överförda uppgifterna. Enligt API-direktivet ska de överförda uppgifterna raderas från det tillfälliga registret inom 24 timmar efter översändandet såvida inte uppgifterna behövs för att de myndigheter som ansvarar för genomförandet av personkontrollerna vid de yttre gränserna ska kunna utföra sina lagstadgade uppgifter. I lagen om passagerarregister anges således att en uppgift i passagerarregistret ska gallras inom 24 timmar efter överföringen

till Polismyndigheten. Om uppgifter i registret behövs för att Polismyndigheten, Säkerhetspolisen eller Tullverket ska kunna verkställa personkontroller, får uppgifterna i registret dock stå kvar till dess att myndighetens kontroller är slutförda. I PNR-direktivet ska uppgifterna lagras i en databas vid enheten för passagerarinformation under en period om fem år. Det gäller även för de uppgifter som kan användas för att omedelbart identifiera de personer som PNR-uppgifterna avser och som ska maskeras, se avsnitt 13.3.

14.6 Våra överväganden

14.6.1 Hur PNR-direktivet påverkar det svenska genomförandet av API-direktivet

Vår bedömning: PNR-direktivet varken ersätter eller påverkar API-direktivet eller dess genomförande i Sverige. Direktiven och deras respektive genomföranden kommer därför att vara parallellt tillämpliga.

Genomförandet av PNR-direktivet innebär att en ny möjlighet för behöriga myndigheter att ta del av API-uppgifter införs i svensk rätt. Överföringen av API-uppgifter enligt PNR-direktivet kommer att avse lufttrafikföretags resor till och från Sverige. Således kommer API-uppgifter efter PNR-direktivets genomförande att överföras inför långt fler resor än vad som tidigare varit möjligt, även om det åtminstone för närvarande torde vara resor till och från tredjeland som det i praktiken kommer att handla om eftersom det är vid sådana resor som API-uppgifter samlas in av lufttrafikföretagen. Överföringen av uppgifterna kommer också, om de finns tillgängliga, att ske vid ytterligare två tillfällen inför varje resa (dels 24–48 timmar före avgång, dels omedelbart efter det att gatens dörrar har stängts) jämfört med vad som följer av API-direktivet (senast vid slutet av incheckningen). Vidare ska överföringen av uppgifterna enligt PNR-direktivet ske inför varje flygresa och inte endast på begäran. Således kan införandet av PNR-direktivet sägas ha en stor betydelse för användningen av API-uppgifter i den brottsbekämpande verksamheten.

För de API-uppgifter som har inhämtas med stöd av PNR-direktivet ska enligt artikel 8.2 det direktivets bestämmelser i övrigt

vara tillämpliga. De API-uppgifter som överförs från lufttrafikföretagen med stöd av de bestämmelser som genomför PNR-direktivet ska således behandlas enligt det direktivets bestämmelser och påverkas inte av hur API-direktivet är genomfört i svensk rätt.

Vår bedömning är mot denna bakgrund att PNR-direktivets bestämmelser om att API-uppgifter ska överföras inte kan förstås på det sättet att de ska gälla i stället för API-direktivets bestämmelser i något avseende. PNR-direktivets genomförande i svensk rätt innebär således inte något helt eller delvis ersättande av API-direktivet eller dess genomförande i Sverige. Direktiven och deras respektive genomföranden kommer därför framöver att få tillämpas parallellt.

I rättslig mening påverkar PNR-direktivet därmed inte i sig genomförandet av API-direktivet i svensk rätt. Detta medför, enligt vår mening, att transportörernas skyldigheter att på begäran lämna API-uppgifter bör vara kvar i utlänningslagen. Vidare bör regleringen av Polismyndighetens behandling av API-uppgifterna enligt API-direktivet inte inordnas i den reglering av PNR- och API-uppgifter som genomför PNR-direktivet, dvs. den nya lag som vi föreslår. Där emot kommer PNR-direktivets genomförande att få betydelse för hur API-uppgifterna framöver kan komma att hanteras i praktiken.

Som tidigare har angetts kommer en översyn av API-direktivet att genomföras under år 2017. Det är i nuläget inte känt vad denna översyn kan komma att innebära. Detta förhållande utgör ännu ett skäl till att inte i detta läge genomföra några förändringar gällande API-direktivets genomförande i svensk rätt.

14.6.2 Är en samordnad hantering av PNR- och API-uppgifter möjlig?

Vår bedömning: En samordnad hantering av PNR- och API-uppgifter vid enheten för passagerarinformation är möjlig även avseende API-uppgifter som behandlas enligt lagen om passagerarregister. Det kräver dock att API-uppgifter som behandlas enligt lagen om passagerarregister hålls isär från de API-uppgifter som överförs från lufttrafikföretagen enligt den nya lagen, att det alltid står klart för vilket syfte och enligt vilket regelverk API-uppgifter behandlas samt att det säkerställs att regelverkens olikheter i fråga om t.ex. tillgång till uppgifterna följs.

En gemensam hantering av de PNR- och API-uppgifter som överförs med stöd av bestämmelserna i PNR-direktivet är självklart möjlig och dessutom nödvändig för att det direktivets bestämmelser ska kunna efterlevas. Frågan vi ställer oss är hur behandlingen av dessa uppgifter ska förhålla sig till behandlingen av de API-uppgifter som hämtas in med stöd av de bestämmelser som genomför API-direktivet. Vi har förstått att det i projektet med att inrätta den i PNR-direktivet avsedda enheten för passagerarinformation planeras att enheten ska behandla samtliga inkomna API-uppgifter, dvs. även sådana som samlas in enligt de bestämmelser som genomför API-direktivet. En sådan samordnad hantering har naturligen stora fördelar, bl.a. då tillgängliga kunskaps- och materiella resurser kan samlas på samma ställe. En samordnad hantering av de olika passageraruppgifterna skulle därmed utgöra den mest effektiva lösningen, inte bara ur kostnadssynpunkt. Som vi har förstått saken behandlas också API- och PNR-uppgifter gemensamt i flera andra länder. Som tidigare angetts framgår det även av regeringens skrivelse Förebygga, förhindra, försvåra – den svenska strategin mot terrorism (skr. 2014/15:146) att det svenska systemet för hantering av PNR-uppgifter bör samordnas med systemet för API-uppgifter, eftersom de tillsammans kan vara ett användbart verktyg i terrorismbekämpningen.

Enligt vad som framgått ovan finns det dock stora skillnader mellan API- och PNR-direktivet. API-uppgifter överförs enligt de båda direktiven inför olika sorts resor och vid olika antal tillfällen per resa. API-uppgifterna får enligt de båda direktiven också lagras och användas på olika sätt. PNR-direktivet innehåller klart fler bestämmelser och begränsningar kring hur de överförda PNR- och API-uppgifterna får bearbetas. Det direktivet innehåller också helt andra krav på egenkontroll, tillsyn och dataskydd.

PNR-direktivet syftar, som tidigare har angetts, till att skydda den allmänna säkerheten genom att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet, dvs. viss slags brottslighet. API-direktivet däremot syftar till att förbättra gränskontrollerna och bekämpa olaglig invandring. I detta ligger, som framgått ovan, dels brottsbekämpning avseende gränsöverskridande brottslighet, dels migrationskontroll som inte utgör brottsbekämpning. Detta medför en rad komplikationer för en samordnad behandling av uppgifter som samlas in med stöd av de båda direktiven. I de fall syftet med en behandling av API-uppgifter är kopplat

till att bekämpa olaglig invandring, och inte avser brottsbekämpning av något slag eller avser bekämpning av annan brottslighet än sådan som omfattas av PNR-direktivets definitioner av grov brottslighet eller terrorism, faller den behandlingen således utanför ändamålet med PNR-direktivet. Uppgifterna i den databas som avses i PNR-direktivet får inte användas i detta syfte. I de fall API-uppgifter ska användas i syfte att bekämpa olaglig invandring utan anknytning till sådan brottslighet som anges i PNR-direktivet, kan alltså de bestämmelser som genomför det direktivet inte tillämpas. I stället får API-uppgifterna i sådant fall begäras in med stöd av de bestämmelser som genomför API-direktivet och behandlas i passagerarregistret för API-uppgifter. Är syftet med behandlingen däremot att utföra en gränskontroll i brottsförebyggande syfte, torde bestämmelserna i PNR-direktivet vara tillämpliga, men endast för det fall behandlingen avser att förebygga, förhindra, upptäcka, utreda eller lagföra sådan terroristbrottslighet eller sådan grov brottslighet som avses i PNR-direktivet. Är det fråga om annan eller lindrigare brottslighet får även här API-uppgifter i stället begäras in och behandlas med stöd av de bestämmelser som genomför API-direktivet.

Det kan te sig svårt att inom samma enhet hantera passageraruppgifter som inhämtas enligt bestämmelserna i två direktiv med så pass olika bestämmelser och delvis olika syften och tillämpningsområden.

PNR-direktivet innebär inrättandet av databaser i medlemsstaterna för brottsbekämpande ändamål med uppgifter om EU-medborgares och andra personers flygresor till och från samt, på grund av medlemsstaternas särskilda åtagande, även deras flygresor inom EU. Direktivet antogs efter en mångårig process där integritetsriskerna med dessa databaser och utbytet av PNR-uppgifter mellan medlemsstaterna ledde till omfattande politiska diskussioner. De detaljerade bestämmelserna i PNR-direktivet om hur och för vad PNR-uppgifterna får lagras, användas och överförs till andra m.m. måste ses mot denna bakgrund. Det är därför av största vikt att genomförandet av PNR-direktivet sker på ett sätt som inger förtroende för att PNR-uppgifterna inte används på ett sätt som står i strid med de ovillkorliga begränsningar som direktivet föreskriver. Detta gäller även de API-uppgifter som ska samlas in med stöd av direktivet.

Med hänsyn till det ovanstående kan det alltså synas svårt att hantera API-uppgifter inhämtade enligt de bestämmelser som genomför API-direktivet samordnat med de PNR- och API-uppgifter som överförs enligt PNR-direktivets genomförande. Det skulle i och för sig kunna anses tala emot att det sker en sådan samordning inom enheten för passagerarinformation som nu planeras i Polismyndighetens tekniska och organisatoriska genomförande av PNR-direktivet. Samtidigt finns det dock uppenbara rättsliga och praktiska beröringspunkter mellan de båda direktiven. Till det kommer att effektivitetsvinsterna med en samordning torde vara mycket stora. Vi bedömer därför, i likhet med Polismyndigheten, att en sådan samordning som nu planeras – och som innebär att även passagerarregistret med API-uppgifter enligt API-direktivet hanteras inom enheten för passagerarinformation – kan vara möjlig både rättsligt och förtroendemässigt. För att en samordnad hantering inom enheten ska kunna vara genomförbar fordras dock att enheten och dess hantering av uppgifterna lever upp till vissa krav.

För det första behöver det säkerställas att de API-uppgifter som hämtas in med stöd av de bestämmelser som genomför API-direktivet i rättslig och användningsmässig mening hålls isär från de uppgifter som överförs enligt de bestämmelser som genomför PNR-direktivet. De uppgifter som hämtas in med stöd av PNR-direktivet ska enligt det direktivet föras över av lufttrafikföretagen till en databas vid enheten för passagerarinformation, inte till flera. För de inkomna uppgifterna gäller också, som framkommit ovan, olika bestämmelser om bl.a. gallring. Det är alltså inte möjligt att behandla alla API-uppgifter inkomna enligt bestämmelserna i de båda direktiven på samma sätt. De tekniska lösningarna måste därför klara av att behandla mottagna API-uppgifter på dessa olika sätt och utifrån förutsättningarna i respektive direktiv.

För det andra är det av största vikt att det i alla lägen står klart enligt vilket syfte API-uppgifter behandlas. Behandlingens ändamål är av stor betydelse för enhetens fortsatta behandling av uppgifterna och har relevans för frågor om gallring, sekretess m.m. Det är även av stor betydelse för utflödet till den brottsbekämpande verksamheten att det står klart vilket regelverk som är styrande för uppgifterna. För det fall syftet med behandlingen är kopplat till att bekämpa olaglig invandring som ett led i Sveriges migrationskontroll, kan uppgifterna i PNR-databasen vid enheten för passagerarinforma-

mation inte användas. Inte heller kan uppgifterna i den databasen användas när syftet med behandlingen är att utföra en gränskontroll avseende annan eller lindrigare brottslighet än den som avses i PNR-direktivet. I sådana fall får i stället passagerarregistret innehållandes endast API-uppgifter användas.

För det tredje krävs ett säkerställande av att extern tillgång, dvs. åtkomst från operativa delar av Polismyndigheten eller direktåtkomst för Säkerhetspolisen och eventuellt även Tullverket, endast är möjlig till det passagerarregister som genomför API-direktivet. Som har angetts tidigare är det vår bedömning att direktåtkomst inte bör få förekomma till de uppgifter som har överförts med stöd av PNR-direktivet. Även av denna anledning är det således av stor vikt att de API-uppgifter som samlas in enligt de bestämmelser som genomför API-direktivet inte sammanblandas med de API-uppgifter som samlas in med stöd av PNR-direktivet.

För att säkerställa att användandet av uppgifterna från respektive inhämtning endast används på de sätt som direktiven medger krävs alltså en bra riggad organisation, god kunskap i dessa frågor hos befattningshavarna vid enheten för passagerarinformation och en närvarande rättslig kompetens. Vidare kommer en tät intern kontroll och extern tillsyn att vara nödvändig.

I övrigt vill vi understryka att det ovan sagda handlar om rättsliga gränser och begränsningar för behandlingen och användningen av de olika uppgiftsslagen inom enheten för passagerarinformation samt för vidareanvändningen av uppgifterna. De informations-tekniska systemen måste tekniskt och logiskt klara av att hantera de krav som ställs upp, särskilt i de bestämmelser som genomför PNR-direktivet. Så länge detta sker, är frågor om hur de informations-tekniska systemen anordnas eller fungerar inte något som bör bli föremål för författningsreglering.

15 Enhetens överföring och utbyte av PNR-information

15.1 Inledning

Det är ett centralt syfte med PNR-direktivet att varje nationell enhet för passagerarinformation ska fungera som en nod vid vilken massan av PNR-uppgifter som lufttrafikföretagen överför tas emot, lagras och analyseras översiktligt. Endast sådan PNR-information som bedömts vara av intresse för att bekämpa terroristbrottslighet eller grov brottslighet ska därefter nå ut till behöriga myndigheter i det egna landet för vidare analys och åtgärder. Vidare är systemet uppbyggt så att de nationella enheterna ansvarar för det internationella utbytet av PNR-uppgifter. Direktivets reglering av under vilka förutsättningar PNR-uppgifter ska eller får överföras – självmant eller på begäran – är omfattande och detaljerad. Reglerna gäller visavi samtliga behöriga mottagare av PNR-uppgifter från den nationella enheten, dvs. det egna landets behöriga myndigheter (artikel 7), andra medlemsstaters nationella enheter för passagerarinformation och myndigheter som har utsetts som behöriga i dessa stater (artikel 9) samt Europol (artikel 10). I detta avsnitt behandlas genomförandet av direktivet vad gäller den svenska enhetens överföring av PNR-uppgifter till dessa mottagare. I avsnitt 17 behandlas enhetens överföring av PNR-information till tredjeländer.

Direktivets bestämmelser om utbyte mellan medlemsstaterna innebär även att den svenska enheten för passagerarinformation kommer att kunna begära och få ta emot PNR-information från andra medlemsstater. I detta avsnitt behandlas även vidarebefordringen av sådan PNR-information och den reglering som vi bedömer behövs för att genomföra direktivet i dessa avseenden.

Slutligen finns en bestämmelse som innebär att behöriga svenska myndigheter i undantagsfall kan vända sig direkt till andra medlems-

stater med en begäran om överföring av PNR-uppgifter. Den bestämmelsen kommer att behandlas i avsnitt 16.1.

15.2 Överföring av PNR-information till behöriga nationella myndigheter

15.2.1 Behörig myndighet

Vårt förslag: En behörig myndighet definieras i lagen som en sådan av regeringen utsedd myndighet som har behörighet att behandla PNR-information i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Av direktivets artikel 7.1 framgår att varje medlemsstat ska utse de myndigheter som ska vara behöriga att begära eller ta emot PNR-information från enheten för passagerarinformation. Dessa myndigheter ska ansvara för den vidare granskningen av informationen samt för att vidta lämpliga åtgärder för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet. De myndigheter som utses ska därmed, som får anses framgå av artikel 7.2, vara sådana myndigheter som är behöriga att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Varje medlemsstat ska enligt artikel 7.3 senast den 25 maj 2017 meddela kommissionen vilka myndigheter som har utsetts.

Det ingår inte i vårt uppdrag att föreslå vilka myndigheter som ska anses behöriga enligt PNR-direktivet. Regeringen har den 4 maj 2017 utsett Polismyndigheten, Säkerhetspolisen, Tullverket, Ekobrottsmyndigheten och Försvarsmakten som behöriga myndigheter. Utpekandet av de behöriga myndigheterna får enligt artikel 7.3 när som helst ändras. Ytterligare behöriga myndigheter kan således komma att utses i framtiden.

Våra överväganden

Det är en lämplig ordning att regeringen avgör vilka brottsbekämpande myndigheter som ska vara behöriga enligt direktivet. Av vårt lagförslag bör emellertid framgå vilka myndigheter som regeringen

över huvud taget kan ge behörighet att begära eller ta emot PNR-uppgifter och som därmed är skyldiga att behandla dessa uppgifter på det sätt som anges i direktivet. Detta kan åstadkommas genom att det i lagen förs in en definition av begreppet behörig myndighet som inte räknar upp olika myndigheter men som avgränsar vad för slags myndighet som kan komma i fråga och hur den utses som behörig enligt direktivet. En definition av detta slag har den fördelen att den inte behöver ändras om nya myndigheter skulle utses som behöriga. Genom att definiera begreppet undviks också att en uppräknning av de behöriga myndigheterna behöver införas i lagens olika bestämmelser.

Enligt vårt förslag ska med en behörig myndighet avses en sådan av regeringen utsedd myndighet som har behörighet att behandla PNR-information i sin verksamhet med att förebygga, förhindra, upptäcka, utreda eller lagföra sådan terroristbrottslighet eller sådan grov brottslighet som omfattas av lagens definition av dessa begrepp. Endast en sådan av regering utsedd myndighet ska ha befogenhet att motta PNR-information från en enhet för passagerarinformation. Att det ska vara fråga om en svensk myndighet behöver inte särskilt anges.

15.2.2 Överföring av PNR-information till behöriga myndigheter

Vårt förslag: Enheten för passagerarinformation ska i enskilda fall lämna PNR-information till en eller flera behöriga myndigheter för att

1. en vidare granskning ska ske av PNR-information rörande passagerare som valts ut vid enhetens förhandsbedömning,
2. besvara en motiverad begäran från en behörig myndighet om att tillhandahålla och behandla PNR-uppgifter för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet och tillhandahålla resultaten av sådan behandling, eller

3. vidarebefordra PNR-information som har mottagits från en motsvarande enhet i en annan medlemsstat.

En befattningshavare vid enheten ska ha gjort en bedömning av PNR-informationen innan den lämnas från enheten.

I vilka situationer ska PNR-information överföras till behöriga myndigheter?

Enheten för passagerarinformation ska enligt direktivet föra vidare PNR-information till behöriga nationella myndigheter i tre olika situationer. *För det första* ska en överföring ske av resultatet av en sådan förhandsbedömning som görs av passagerare före deras beräknade ankomst till eller avresa från Sverige (artikel 6.2 a och 6.6). *För det andra* ska PNR-information överföras för att besvara en förfrågan från en behörig myndighet (artikel 6.2 b). *För det tredje* ska enheten för passagerarinformation vidarebefordra sådan PNR-information som den har mottagit från andra medlemsstaters motsvarande enheter eftersom en sådan enhet vid en förhandsbedömning har ansett att informationen är intressant för vidare granskning i Sverige (artikel 9.1).

Enheten kan dock även motta PNR-information från andra länders motsvarande enheter såsom svar på sådana frågor som vår enhet har ställt på uppdrag av en behörig myndighet (artikel 9.2). Det anges inte uttryckligen i direktivet vad enheten ska göra med denna information. Det får dock förutsättas att denna PNR-information ska överföras till den behöriga myndighet som ursprungligen har ställt frågan via den svenska enheten.

Enligt vår mening bör det i författning klargöras i vilka situationer enheten för passagerarinformation får överföra PNR-information till behöriga myndigheter. Med hänsyn till den grundläggande betydelsen som en sådan bestämmelse har för integritetsskyddet bör bestämmelsen införas på lagnivå. Vilka närmare förutsättningar som ska vara uppfyllda och vilka närmare överväganden enheten ska göra inför en överföring av PNR-information till behöriga myndigheter behandlas nedan.

Närmare förutsättningar för att en överföring ska få ske

Direktivets bestämmelser

I artikel 6.5 och 6.6 finns närmare bestämmelser om hur enheten för passagerarinformation ska gå till väga när en träff har uppkommit i samband med en förhandsbedömning av passagerare. Av artikel 6.5 framgår att sådana träffar alltid ska granskas individuellt med icke-automatiska metoder för att det ska gå att verifiera huruvida en behörig myndighet behöver vidta åtgärder i anledning av informationen. Alla träffar som uppkommer vid jämförelser med uppgifter i register eller andra uppgiftssamlingar eller vid behandling i enlighet med på förhand fastställda kriterier måste alltså alltid genomgå en granskning innan uppgifterna får användas vidare. Vid denna granskning ska avgöras huruvida det finns anledning att agera vidare på uppgifterna. Om så är fallet ska enheten, enligt artikel 6.6, översända PNR-uppgifterna beträffande personer som har identifierats eller resultaten av behandlingen av dessa uppgifter, till behöriga myndigheter i samma stat för vidare granskning. Överföring till en behörig myndighet får enligt bestämmelsen dock endast ske i enskilda fall och vid automatisk behandling av PNR-uppgifter, som angetts ovan, efter en individuell och icke-automatisk granskning.

När enheten för passagerarinformation mottar uppgifter från en annan medlemsstats motsvarande enhet efter en förhandsbedömning vid den enheten ska, enligt artikel 9.1, bestämmelsen i artikel 6.6 tillämpas. Således får även i dessa fall en överföring av PNR-information till en behörig myndighet endast ske i enskilda fall och efter en individuell och icke-automatisk granskning av uppgifterna.

Hur enheten ska gå till väga när den ska besvara en särskild förfrågan framgår indirekt av artikel 6.2 b. Enligt bestämmelsen ska en sådan förfrågan endast besvaras i enskilda fall. För att enheten ska behandla en begäran krävs vidare att den är vederbörligen motiverad. Vidare ska förfrågan enligt artikel 6.2 b bygga på tillräckliga skäl om att tillhandahålla och behandla PNR-uppgifter i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet. Härmed bör, enligt vår bedömning, avses att förfrågan ska vara tillräckligt motiverad för att det ska framgå att syftet med begäran om att enheten ska tillhandahålla och behandla PNR-uppgifter är att förebygga, förhindra, upptäcka, utreda eller lagföra sådan brottslighet som avses i direktivet. För det fall

de PNR-uppgifter som ska överföras är äldre än sex månader och därmed är maskerade, krävs därutöver, för att fullständiga, avmaskerade, PNR-uppgifter ska kunna lämnas ut, att förutsättningarna i artikel 12.3 är uppfyllda. Detta behandlas nedan i avsnitt 15.5.

Våra överväganden

Förutsättningarna för att en överföring alls ska få ske till de behöriga myndigheterna bör framgå av lagen. Således bör det av lagen framgå att överföringar från enheten för passagerarinformation till behöriga myndigheter endast får ske i enskilda fall. Det krävs således alltid att en individuell bedömning utförs innan PNR-information sänds vidare till behöriga myndigheter. PNR-information kan alltså inte per automatik föras vidare från enheten till en behörig myndighet.

Enligt direktivet ska träffar i samband med automatisk behandling av PNR-uppgifter granskas individuellt med icke-automatiska metoder innan de får vidarebefordras till de behöriga myndigheterna. Med icke-automatiska metoder torde, enligt vår mening, inte menas att granskningen måste ske utan inblandning av informationstekniska hjälpmedel. Det kan t.ex. knappast menas att granskningen behöver göras endast med användning av papper och penna. Det som avses torde vara att ett översändande inte får grundas enbart på en automatiserad behandling av PNR-uppgifter. Varje beslut om överföring måste i stället föregås av en bedömning utförd av en person som tjänstgör vid enheten för passagerarinformation. Detta bör framgå av lagen.

En rent automatisk behandling av PNR-uppgifter torde endast bli aktuell vid en sådan förhandsbedömning av passagerare som sker vid jämförelser mot relevanta register eller andra uppgiftssamlingar eller mot på förhand fastställda kriterier. En rent automatisk behandling torde alltså inte bli aktuell vid sådan behandling av PNR-information som sker för att besvara en förfrågan eller för att vidarebefordra PNR-information från en annan medlemsstat som svar på en förfrågan. Dock ska även överföringar som sker som svar på förfrågningar behandlas i enskilda fall. Enligt vår bedömning bör därmed även dessa överföringar föregås av en bedömning utförd av en person som tjänstgör vid enheten. Vi föreslår att detta anges i

lagen. Vidare bör det av lagen framgå att en förfrågan från en behörig myndighet ska vara motiverad och avse behandling av PNR-information för ett eller flera av de syften som anges i lagens portalbestämmelse.

Närmare om den bedömning som ska göras vid enheten

Utöver vad som angetts ovan innehåller direktivet inte några närmare bestämmelser om vilka överväganden som bör göras vid enheten för passagerarinformation vid bedömningen av om en träff i samband med en förhandsbedömning av passagerare ska överföras till behöriga myndigheter. Det uppställs således inte något krav på att en person ska finnas med i något eller några relevanta register eller andra uppgiftssamlingar för att informationen ska anses vara tillräckligt intressant för att föras vidare. Det anges inte heller i vilket skede som sökningar i olika register eller andra uppgiftssamlingar får göras. Enligt vår mening bör det, utöver vad som anges i direktivet, inte närmare i lag eller förordning anges hur enheten för passagerarinformation ska göra sitt urval. Det bör således vara upp till personalen vid enheten för passagerarinformation att bedöma huruvida viss information är så pass intressant att den bör sändas vidare för närmare granskning. Det kan i sammanhanget tilläggas att de behöriga myndigheterna kan ha annan information om de resande som inte finns tillgänglig för enheten för passagerarinformation, vilket medför att även vissa inledningsvis mindre intressanta träffar visar sig vara högtintressanta för de behöriga myndigheterna.

Den granskning som ska utföras vid enheten för passagerarinformation innan PNR-information får sändas vidare till de behöriga myndigheterna bör dock syfta till att den aktuella PNR-informationen avser personer som kan vara inblandade i sådan brottslighet som omfattas av direktivet. Det kan vara svårt, för att inte säga omöjligt, för personalen vid enheten för passagerarinformation att bedöma i fall den PNR-information som har tagits fram vid en förhandsbedömning är relevant för att bekämpa den aktuella brottsligheten. Dock kan man inför en överföring av den framtagna informationen se till att det inte av misstag följer med PNR-information som avser sådana personer som inte alls kan bedömas vara intressanta för vidare granskning på grund av att de kan vara inblandade i

terroristbrottslighet eller grov brottslighet. Så kan vara fallet exempelvis om en sökning mot på förhand fastställda kriterier ger ett orimligt stort utfall. Vidare anser vi att det av artikel 6.5 och 6.6 rimligen följer att granskningen också ska omfatta att överföring bara sker till en behörig myndighet som kan antas behöva PNR-informationen för att göra en närmare granskning av informationen och eventuellt göra insatser för att bekämpa aktuell brottslighet. T.ex. bör ett översändande till Ekobrottsmyndigheten endast ske när det kan vara fråga om sådan brottslighet som den myndigheten arbetar mot.

I artikel 6.2 b anges att svaret på en viss förfrågan från en behörig myndighet ska tillhandahållas de behöriga myndigheterna. Skrivningen kan tolkas som att svaret på en förfrågan ska överföras till samtliga behöriga myndigheter. De behöriga myndigheterna har dock olika uppdrag och därmed olika intressen av att få ta del av PNR-information. Enligt vår mening bör därför direktivet tolkas som att ett svar på en viss förfrågan ska översändas endast till den myndighet som har ställt frågan.

För det fall PNR-information har tagits fram för att besvara en begäran från en behörig myndighet bör den kontroll som ska utföras vid enheten omfatta att uppgifterna kommer att överföras till just den behöriga myndigheten som har framställt frågan. I direktivet anges att en sådan förfrågan från behöriga myndigheter ska vara vederbörligen motiverad och bygga på tillräckliga skäl. Med skrivningen bör, enligt vår bedömning, avses att förfrågan ska vara tillräckligt motiverad för att det ska framgå att syftet med begäran om att enheten ska tillhandahålla och behandla PNR-uppgifter är att förebygga, förhindra, upptäcka, utreda eller lagföra sådan brottslighet som avses i direktivet. En granskning av att dessa villkor är uppfyllda ska göras innan enheten ens väljer att behandla förfrågan. En granskning av de framtagna uppgifterna inför att de ska överföras till den behöriga myndigheten bör, enligt vår mening, ändå genomföras för att säkerställa att syftet med behandlingen har varit just någon av de brottsbekämpande åtgärderna och sådan brottslighet som PNR-informationen får användas för.

Vidare bör det alltid kontrolleras att PNR-informationen inte innehåller några uppgifter som dessförinnan borde ha raderats av enheten, antingen eftersom de avser andra uppgifter än de som framgår av bilaga I till direktivet, eller eftersom de innehåller känsliga person-

uppgifter. Som tidigare har angetts kan sådana känsliga personuppgifter t.ex. dölja sig bland de allmänna anmärkningarna (se vidare i avsnitt 18.5).

Vad som bör ingå i den granskning som ska utföras av enheten för passagerarinformation innan en överföring görs framgår implicit av andra bestämmelser i lagen eller förordningen och behöver, enligt vår mening, inte anges särskilt i regleringen.

15.3 Utbyte av PNR-information med andra medlemsstater

15.3.1 Medlemsstat

Vårt förslag: En medlemsstat definieras i lagen som en stat som är medlem i EU, med undantag för Danmark.

Artikel 9 gäller vid utbyte av PNR-uppgifter mellan medlemsstaterna. I vanligt språkbruk benämns en stat som är medlem i EU medlemsstat. Direktivet utgår också från att det gäller för alla EU:s medlemsstater. Av skäl 40 framgår dock att det inte är bindande för eller tillämpligt på Danmark.

Ordet medlemsstat används på flera håll i direktivet, främst i fråga om överföring av PNR-uppgifter. Det är svårt att undvika att använda ordet medlemsstat i lagförslaget. Eftersom inte alla EU:s medlemsstater omfattas går det inte att använda ordet medlemsstat i lagen utan att definiera det. Ett alternativ skulle vara att räkna upp alla berörda stater, men det skulle bli onödigt omfattande och komplicerat att göra det i alla tillämpliga bestämmelser. Genom att definiera medlemsstat blir det tydligt för vilka stater bestämmelserna gäller utan att lagen tyngs av långa uppräkningslistor. Medlemsstat bör därför definieras i lagen. En medlemsstat bör definieras som en stat som är medlem i EU, med undantag för Danmark.

Om Danmark skulle besluta att ansluta sig till direktivet kommer Danmark att ingå bland de medlemsstater som omfattas av direktivet. I sådant fall skulle en definition av begreppet inte behövas.

15.3.2 Utbyte mellan medlemsstaternas enheter för passagerarinformation

Vår bedömning: Regleringen ska innehålla bestämmelser om den svenska enheten för passagerarinformations skyldigheter att överföra PNR-information till övriga medlemsstaters enheter för passagerarinformation och i dessa stater utsedda behöriga myndigheter. Regleringen ska också innehålla bestämmelser om hur vår nationella enhet för passagerarinformation samt våra behöriga myndigheter ska gå till väga för att hämta in uppgifter från motsvarande enheter i de andra medlemsstaterna.

Av direktivets skäl 23 framgår att medlemsstaterna bör utbyta PNR-uppgifter med varandra om det bedöms nödvändigt för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Där framgår även att enheterna för passagerarinformation bör, om det är lämpligt, utan dröjsmål översända resultatet av behandlingen av PNR-uppgifterna till motsvarande enheter i andra medlemsstater för ytterligare utredning. De PNR-uppgifter som lufttrafikföretagen överför till enheterna för passagerarinformation och resultatet av behandlingen av sådana uppgifter som tas fram av enheterna enligt bestämmelserna i artikel 6 kommer således inte endast att komma de nationella behöriga myndigheterna till del. Den PNR-information som väljs ut av en enhet för passagerarinformation vid en förhandsbedömning kan således i vissa fall överföras till andra medlemsstaters motsvarande enheter. Vidare kan en enhet för passagerarinformation begära att få ta del av uppgifter i PNR-databasen vid en annan medlemsstats enhet för passagerarinformation. I undantagsfall kan en sådan nationell enhet också begära att en annan enhet för passagerarinformation införskaffar PNR-uppgifter från lufttrafikföretag på andra tider än normalt och vidarebefordrar dessa till den begärande enheten.

Bestämmelserna i artiklarna 9.1–9.4 innehåller såväl skyldigheter för respektive medlemsstat att överföra uppgifter till andra medlemsstater, som möjligheter för medlemsstaterna att få ta del av dessa uppgifter. Vi ser det som vårt uppdrag att reglera den svenska enhetens skyldigheter att under vissa förhållanden överföra PNR-uppgifter till de andra medlemsstaterna. Skyldigheterna för de andra medlemsstaternas enheter för passagerarinformation att överföra uppgifter

till vår nationella enhet får självfallet regleras i respektive medlemsstats rättsordning. Våra förslag till reglering kommer således att innehålla bestämmelser om den nationella enhetens skyldigheter att under de förutsättningar som anges i direktivet överföra uppgifter till övriga medlemsstaters motsvarande enheter och behöriga myndigheter. Våra förslag kommer också att innehålla vissa bestämmelser om hur enheten för passagerarinformation samt våra behöriga myndigheter ska gå till väga för att inhämta uppgifter från motsvarande enheter i de andra medlemsstaterna. Våra behöriga myndigheters möjlighet i denna del kommer att behandlas i avsnitt 16.1.

Överföring av PNR-information vid förhandsbedömningar

Vårt förslag: Enheten för passagerarinformation ska till en motsvarande enhet i en annan medlemsstat överföra sådan PNR-information som behandlats för ändamålet förhandsbedömning och som bedömts vara relevant och nödvändig för vidare granskning i den andra medlemsstaten.

Direktivets bestämmelse

När personer har identifierats av en enhet för passagerarinformation i enlighet med artikel 6.2, ska enheten enligt artikel 9.1 även översända alla relevanta och nödvändiga PNR-uppgifter eller resultaten av en eventuell behandling av dessa uppgifter till motsvarande enheter i de andra medlemsstaterna. Enheterna för passagerarinformation i de mottagande medlemsstaterna ska därefter översända den mottagna informationen till sina behöriga myndigheter enligt artikel 6.6. på samma sätt som om uppgifterna hade tagits fram vid det egna landets enhet.

Våra överväganden

Artikel 9.1 innebär att enheten för passagerarinformation självant ska överföra PNR-information till motsvarande enheter i de övriga medlemsstaterna. Artikeln hänvisar till artikel 6.2, som omfattar både förhandsbedömningar av PNR-uppgifter (6.2 a) och överföring

av sådana uppgifter på begäran (6.2 b). Dock anges i bestämmelsen också att ett översändande ska ske när någon har identifierats, vilket enligt bestämmelsen i artikel 6.2 endast sker vid förhandsbedömningar. Dessutom anges att de översända uppgifterna ska behandlas enligt artikel 6.6 i den mottagande staten. Artikel 6.6 behandlar också endast förhandsbedömningar av passagerare. Med hänsyn härtill är det vår uppfattning att artikel 9.1 ska läsas som att den endast avser överföring av sådan PNR-information som väljs ut vid en förhandsbedömning av passagerare. Den tolkningen är också rimlig med tanke på att nästföljande artikel, 9.2, innehåller bestämmelser om överföring av PNR-information till en annan medlemsstat på begäran.

Således ska enheten för passagerarinformation enligt bestämmelsen i artikel 9.1 överföra sådan PNR-information som väljs ut vid en förhandsbedömning av passagerare även till en motsvarande enhet i en annan medlemsstat. Överföring ska dock endast ske om PNR-informationen anses vara relevant och nödvändig. All PNR-information som bedöms intressant för en eller flera av den egna medlemsstatens behöriga myndigheter skulle i och för sig kunna anses vara i någon mån relevant och nödvändig även för andra medlemsstater. Utbyte mellan samtliga medlemsstater av all sådan information som tas fram av varje enhet för passagerarinformation skulle dock leda till att alltför stora mängder PNR-information utbyttes mellan medlemsstaterna. Det skulle knappast vara förenligt med proportionalitetsprincipen och passagerarnas rätt till respekt för privatlivet och skydd av sina personuppgifter. Systemet skulle vidare tyngas av all denna information och ett långt större antal personer än beräknat skulle behöva anställas vid varje enhet för passagerarinformation för att ta hand om mottagna uppgifter. Bestämmelsen får enligt vår mening därför tolkas som att det bara är sådan PNR-information som anses vara relevant och nödvändig för just en specifik medlemsstat som ska överföras. Det får alltså i varje fall göras en bedömning av vilka som kan tänkas beröras av informationen. En typisk situation skulle kunna vara när vår enhet för passagerarinformation har valt ut en viss person inför dennes resa till en annan medlemsstat. Information kan då lämpligen överföras till enheten för passagerarinformation i det land som den aktuella flighten ankommer till, och inte till samtliga medlemsstaters motsvarande enheter. Det måste således alltid från fall till fall göras en bedömning

och ett urval både av vilken eller vilka mottagare som kan komma i fråga och vilken PNR-information som ska föras över.

Artikel 9 gäller vid utbyte av PNR-uppgifter eller resultatet av en eventuell behandling av dessa uppgifter, dvs. PNR-information. Som angetts ovan bör med resultatet av en eventuell behandling av PNR-uppgifter avses de träffar som har uppkommit genom de automatiska sökningarna mot de på förhand fastställda kriterierna samt eventuella uppgifter om att personen även förekommer i en viss databas. Det är dock, enligt vår mening, inte tänkt att direkta uppgifter ur dessa databaser ska överföras från enheten för passagerarinformation till motsvarande enheter i andra medlemsstater. Utbyte av sådan information får ske mellan medlemsstaterna med hjälp av redan upparbetade informationsvägar och enligt bestämmelserna i annan lagstiftning samt efter vederbörlig sekretessprövning.

En bestämmelse om under vilka förutsättningar den svenska enheten för passagerarinformation på eget initiativ ska överföra PNR-uppgifter till utlandet är av så grundläggande betydelse att den bör genomföras i lag.

Överföring av PNR-information på förfrågan

Vårt förslag: Enheten för passagerarinformation ska så snart som möjligt besvara en motiverad begäran från en motsvarande enhet i en annan medlemsstat och överföra lagrade PNR-uppgifter och resultatet av en eventuell behandling av dessa uppgifter dit.

Direktivets bestämmelse

Enligt artikel 9.2 ska enheten för passagerarinformation i en medlemsstat ha rätt att vid behov begära att en motsvarande enhet i en annan medlemsstat tillhandahåller PNR-uppgifter som lagras i den senares databas och som ännu inte har genomgått en maskering. Vid behov ska även resultaten av en eventuell behandling av dessa uppgifter, om en sådan redan har utförts i enlighet med artikel 6.2 a (dvs. i samband med en förhandsbedömning), tillhandahållas. En begäran om att få ta del av uppgifter ska vederbörligen motiveras. Begäran får avse en viss uppgift eller en kombination av sådana upp-

gifter, beroende på vilken information den begärande enheten för passagerarinformation anser vara nödvändig i ett särskilt fall för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet. Enheterna för passagerarinformation ska tillhandahålla den begärda informationen så snart som möjligt.

Om de begärda uppgifterna är äldre än sex månader och därmed har maskerats får enheten för passagerarinformation tillhandahålla fullständiga, avmaskerade, PNR-uppgifter endast om det rimligen kan antas vara nödvändigt för de ändamål som anges i artikel 6.2 b, och endast efter tillstånd från en sådan myndighet som avses i artikel 12.3.

Våra överväganden

En bestämmelse som genomför enheten för passagerarinformations skyldigheter att överföra PNR-information enligt artikel 9.2 bör föras in på lagnivå. Av bestämmelsen bör framgå att enheten för passagerarinformation är skyldig att så snart som möjligt besvara en förfrågan från en enhet för passagerarinformation i en annan medlemsstat och föra över PNR-uppgifter dit. För det fall enheten har tillgång till ett resultat av behandling av de aktuella PNR-uppgifterna som har tagits fram i samband med en förhandsbedömning av uppgifterna, och detta resultat ännu inte har gallrats, ska även det resultatet överföras. Detta bör framgå av bestämmelsen. Härmed framgår att enheten för passagerarinformation inte är skyldig att på begäran av en annan enhet exempelvis jämföra PNR-uppgifterna med uppgifterna i något register eller någon annan uppgiftssamling. Endast för det fall en sådan bedömning redan är genomförd och alltjämt finns sparad vid enheten, ska resultatet av den också översändas. Som kommer att framgå i avsnitt 18.6 torde det dock höra till rena undantagsfall att sådana resultat finns sparade vid enheten.

Av bestämmelsen bör vidare framgå att förfrågan från den andra medlemsstaten ska vara motiverad. Skälen till detta är att enheten för passagerarinformation ska kunna bedöma huruvida den begärda informationen behövs för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet och begäran därmed över huvud taget får behandlas.

Vi kommer att återkomma till frågan om överföring av avmaske-
rade PNR-uppgifter i avsnitt 15.5.

Inför ett överlämnande av PNR-information på begäran från en
annan medlemsstat bör enheten göra samma överväganden som inför
en överföring till en behörig myndighet, se ovan i avsnitt 15.2.2.

Överföring efter begäran om att inhämta PNR-uppgifter från lufttrafikföretag

Vårt förslag: När det i ett enskilt fall är nödvändigt med tillgång
till PNR-uppgifter för att avvärja en specifik och faktisk fara
med anknytning till terroristbrottslighet eller grov brottslighet,
ska enheten för passagerarinformation på begäran av en motsva-
rande enhet i en annan medlemsstat inhämta PNR-uppgifter från
lufttrafikföretagen vid andra tidpunkter än som i övrigt följer av
direktivet och överföra dessa till den begärande enheten.

Om åtkomst till PNR-uppgifter är nödvändig för att reagera på ett
specifikt och faktiskt hot med anknytning till terrorism eller grov
brottslighet, ges enligt artikel 9.4 enheten för passagerarinformation
i en medlemsstat i undantagsfall rätt att begära att en motsvarande
enhet i en annan medlemsstat införskaffar PNR-uppgifter i enlighet
med artikel 8.5 och vidarebefordrar dessa till den begärande enheten
för passagerarinformation. Enligt artikel 8.5, som behandlats i av-
snitt 11.4.6, ska lufttrafikföretagen under vissa särskilda omständig-
heter, överföra PNR-uppgifter vid andra tidpunkter än vad som i
övrigt följer av direktivet.

Även en bestämmelse som genomför enheten för passagerar-
informations skyldigheter enligt artikel 9.4 bör genomföras i lag. Av
bestämmelsen bör framgå att enheten för passagerarinformation på
begäran av en motsvarande enhet i annan medlemsstat ska inhämta
uppgifter från lufttrafikföretagen på andra tider än normalt och
överföra dessa till den begärande enheten. Uppgifterna ska enligt
direktivet hämtas in endast i undantagsfall, vilket torde innebära att
det endast är tillåtet i vissa särskilda situationer. Vi föreslår därför
att det i lagen anges att uppgifterna endast ska hämtas in på detta sätt
i ett enskilt fall. Vidare ska enligt direktivet uppgifter endast hämtas
in på andra tider än normalt för det fall de är nödvändiga för att

reagera på ett specifikt och faktiskt hot med anknytning till terroristbrottslighet eller grov brottslighet. I svensk lagstiftning brukar ordet fara användas i stället för hot. Ordet används bland annat i brottsdatalogen. Med hänsyn härtill föreslår vi att ordet fara används i stället för hot även i genomförandet av denna lag. Av samma anledning bör ordet avvärja användas i vår lag i stället för begreppet reagera på, som används i PNR-direktivet. Vidare finner vi att ordet tillgång bättre än ordet åtkomst beskriver det sätt på vilket uppgifterna kommer att komma en annan enhet till del.

15.3.3 Överföring på direkt begäran från en behörig myndighet i en annan medlemsstat

Vårt förslag: Endast när det i ett enskilt brådskande fall är absolut nödvändigt ska enheten för passagerarinformation besvara en motiverad förfrågan från en myndighet som utsetts som behörig i en annan medlemsstat och överföra PNR-uppgifter och resultatet av en eventuell behandling av dessa uppgifter direkt till den myndigheten.

PNR-uppgifter ska som huvudregel utbytas mellan medlemsstaterna bara via medlemsstaternas enheter för passagerarinformation. I artikel 9.3 ges dock möjlighet för en medlemsstats behöriga myndigheter att i undantagsfall vända sig direkt till enheten för passagerarinformation i en annan medlemsstat med en begäran om utlämnande av PNR-uppgifter som finns lagrade i den enhetens databas. En sådan begäran får endast framställas i nödfall och i övrigt på samma villkor som anges i artikel 9.2. Även en sådan begäran ska vara vederbörligen motiverad. En kopia av begäran ska alltid skickas till enheten för passagerarinformation i den begärande medlemsstaten. Som angetts ska denna möjlighet endast användas i undantagsfall. I alla andra fall ska de behöriga myndigheterna översända sina framställningar via enheten för passagerarinformation i den egna medlemsstaten.

Enheten för passagerarinformations skyldigheter enligt artikel 9.4 bör genomföras i lag. Av en sådan lagbestämmelse bör framgå att enheten endast i speciella undantagsfall ska besvara en begäran från en behörig myndighet i en annan medlemsstat om att få ta del av

PNR-information. I direktivets svenska översättning används ordet nödfall (jfr *hastende* i den danska översättningen). Med nödfall torde menas detsamma som om det är absolut nödvändigt i ett brådskande fall. Enligt vår mening passar detta uttryckssätt bättre in i svensk lagstiftning. Vi föreslår därför att detta används i lagtexten. Överföring ska i övrigt ske endast under samma förutsättningar som överföring till en annan enhet för passagerarinformation. Det innebär bl.a. att endast motiverade förfrågningar ska besvaras. För det fall en förfrågan avser avmaskerade PNR-uppgifter ska förutsättningarna för överföring av sådana vara uppfyllda, se vidare i avsnitt 15.5.

15.3.4 Enhetens inhämtande av PNR-uppgifter från andra medlemsstaters motsvarande enheter

Våra förslag: En begäran om att få ta del av PNR-information som lagras hos en enhet för passagerarinformation i en annan medlemsstat ska bara få göras om syftet därmed faller inom ramen för när PNR-uppgifter alls får behandlas, dvs. för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Endast när det i ett enskilt fall är nödvändigt för att reagera på en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet, får enheten för passagerarinformation hos en motsvarande enhet i en annan medlemsstat begära att PNR-uppgifter ska hämtas in från lufttrafikföretag i enlighet med artikel 8.5 i PNR-direktivet för vidarebefordran till enheten.

Bestämmelser om detta kan tas in i förordning.

Som framgått ovan innehåller artikel 9.2 och 9.4 också vissa uppgifter om hur en nationell enhet för passagerarinformation ska gå till väga när den vill ha tillgång till PNR-information som lagras hos en motsvarande enhet i en annan medlemsstat. Av artikel 9.2 framgår att en enhet för passagerarinformation har rätt att vid behov begära att få del av sådan information. Således ska en begäran framställas. Vidare ska begäran vara vederbörligen motiverad. Härmed torde i huvudsak avses att informationen kan antas behövas av enheten eller de svenska behöriga myndigheterna för att förebygga,

förhindra, upptäcka, utreda eller lagföra sådan brottslighet som omfattas av direktivet. Begäran får vidare enligt artikel 9.2 avse en viss uppgift eller en kombination av uppgifter. Något krav på formen för begäran anges inte och därmed inte heller något uttryckligt skriftlighetskrav. Av artikel 9.5 framgår att informationsutbytet får ske via alla befintliga kanaler för samarbete mellan staterna. En begäran om att få ta del av PNR-information som finns lagrad vid en annan medlemsstats enhet för passagerarinformation kommer troligen normalt sett att överföras elektroniskt och därmed skriftligt. Det finns dock alltså inget som hindrar att en begäran framställs muntligen. Av artikel 13.5 b framgår dock att den mottagande enheten ska dokumentera varje begäran. Den frågan återkommer vi till i avsnitt 19.3.

Enligt vår mening kan frågan om enheten för passagerarinformations skyldigheter i samband med en begäran om att få ta del av PNR-information från en motsvarande enhet i ett annat land enligt artikel 9.2 regleras i förordning. En sådan bestämmelse kan dock inskränkas till att ange att en förfrågan bara ska få göras om syftet därmed faller inom ramen för när PNR-uppgifter alls får behandlas enligt direktivet, dvs. för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

I artikel 9.4 behandlas vår nationella enhets möjlighet att begära att en annan medlemsstats motsvarande enhet hämtar in uppgifter från lufttrafikföretag på andra tider än som i övrigt följer av direktivet. En bestämmelse som genomför artikeln i fråga om enhetens begäran bör utformas på samma sätt som angetts ovan för den situation där vår enhet mottar en sådan begäran. Även denna fråga kan regleras i förordning.

15.3.5 Former för informationsutbytet

Informationsutbytet mellan medlemsstaterna får enligt artikel 9.5 ske via alla befintliga kanaler för samarbete mellan medlemsstaternas behöriga myndigheter. Det språk som används i samband med begäran och informationsutbytet ska vara det som gäller för den kanal som används. Medlemsstaterna ska i samband med att de lämnar meddelanden i enlighet med artikel 4.5 även meddela kommissionen uppgifter om de kontaktpunkter till vilka framställningar kan sändas

i nödfall. Kommissionen ska underrätta medlemsstaterna om dessa uppgifter.

Bestämmelserna i artikel 9.5 behöver enligt vår bedömning inte författningsregleras.

15.4 Europols tillgång till PNR-information

15.4.1 Europol och dess verksamhet

Europol är EU:s gemensamma polisbyrå och utgör en del av det brottsbekämpande samarbetet i unionen. Europol har till uppgift att stödja och stärka medlemsstaternas polismyndigheter och andra brottsbekämpande organs insatser och deras samarbete för att förebygga och bekämpa viss brottslighet.

Europol är en egen juridisk person och har ställning av en EU-enhet, finansierad genom unionens allmänna budget. Europols behörighet omfattar organiserad brottslighet, terrorism och vissa andra former av allvarlig brottslighet som rör två eller flera medlemsstater på ett sådant sätt att det krävs en gemensam åtgärd från medlemsstaternas sida på grund av brottslighetens omfattning, betydelse eller följder.

Europol arbetar till stor del med insamling, behandling och analys av underrättelser om allvarlig och gränsöverskridande brottslighet inom unionen och fungerar som en knutpunkt för utbyte av uppgifter mellan medlemsstaterna. Medlemsstaterna tillhandahåller Europol uppgifter främst ur sina nationella polisregister. Dessa uppgifter sammanställs och bearbetas samt kompletteras i vissa fall med uppgifter från annat håll. Uppgifterna analyseras sedan hos Europol. Underrättelser går tillbaka till medlemsstaternas brottsbekämpande myndigheter som härigenom får ett bättre underlag för sin operativa verksamhet. Härutöver stödjer Europol medlemsstaterna med rådgivning och fördjupade specialkunskaper vid utredningar och tillhandahåller även strategiska underrättelser för att främja operationer i medlemsländerna m.m.

Europol har egna datasystem och upprättar särskilda analysfiler för de ärenden där Europol tar på sig att utföra analysarbetet. Regelverket innehåller detaljerade bestämmelser om dataskyddet hos Europol och om tillgång till uppgifter som behandlas av Europol.

Inom ramen för samarbetet finns också ett gemensamt informationssystem (Siena) för säkert informationsutbyte.

I varje medlemsstat finns det en nationell enhet som är kontaktpunkt och förbindelseänk mellan Europol och medlemsstaternas myndigheter. Chefen för den nationella enheten har också en formell roll i Europols interna verksamhet. I Sverige är Polismyndigheten nationell enhet. Det operativa ansvaret har lagts vid Polismyndighetens nationella operativa avdelning. Den nationella enheten har till huvudsaklig uppgift att förse Europol med den information från de nationella polisregistren eller motsvarande som ska överlämnas till Europol, samt att ta emot information som kommer från Europol och vidarebefordra denna till sådana nationella myndigheter och organ som är ansvariga för att förebygga och bekämpa brott.

Europols ledning utgörs dels av en styrelse bestående av representanter från alla medlemsstater och kommissionen, dels en verkställande direktör som assisteras av tre biträdande verkställande direktörer. Europols huvudkontor ligger i Haag i Nederländerna. Vid huvudkontoret finns personal som är direkt anställd av Europol, t.ex. experter och analytiker inom olika områden. Där arbetar också särskilda sambandsmän som är utsända av medlemsstaterna. Sambandsmännen har till uppgift att praktiskt genomföra informations- och underrättelseutbytet mellan Europol och de nationella enheterna samt att samverka med Europols anställda i bl.a. analysarbetet.

Europol inrättades genom Europolkonventionen år 1995. När Sverige tillträdde Europolkonventionen år 1997 gjordes bedömningen att tillträdet till konventionen endast i mycket begränsad omfattning krävde lagändringar (prop. 1996/97:164). Europols verksamhet inleddes år 1999. Europolkonventionen ersattes sedermera av rådets beslut 2009/371/RIF av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europolrådsbeslutet). PNR-direktivet hänvisar till detta rådsbeslut.

15.4.2 Europolförordningen

Den 11 maj 2016 antog Europaparlamentet och rådet förordning (EU) 2016/794 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF,

2009/936/RIF och 2009/968/RIF (Europolförordningen). Förordningen ska i sin helhet tillämpas från och med den 1 maj 2017 då Europolradsbeslutet upphörde att gälla. Eftersom Europolförordningen är bindande och direkt tillämplig i medlemsstaterna har bestämmelserna i förordningen inte genomförts i svensk lagstiftning. Europolförordningen har inte heller bedömts medföra behov av några kompletterande bestämmelser i svensk rätt (se prop. 2016/17:139 s. 81).

Europolförordningen innehåller det styrande regelverket för Europol. Europol kommer även fortsättningsvis ha som huvudsaklig uppgift att stödja och stärka insatser som utförs av de brottsbekämpande myndigheterna i medlemsstaterna samt deras ömsesidiga samarbete för att förebygga och bekämpa allvarlig brottslighet som rör två eller fler medlemsstater, terrorism och sådana former av brottslighet som påverkar ett gemensamt intresse som omfattas av unionens politik. Vilken form av brottslighet som avses anges i bilaga I till Europolförordningen. Genom Europolförordningen har Europolis uppgifter och mandat utökats något. Europol har bl.a. fått i uppgift att samordna, organisera och initiera insatser tillsammans med medlemsstaterna.

Medlemsstaternas skyldighet att förse Europol med den information som byrån behöver för att genomföra sitt uppdrag förtydligas i Europolförordningen. Enligt artikel 7.6 ska varje medlemsstat tillhandahålla Europol den information som är nödvändig för att den ska kunna uppfylla sina mål. Varje medlemsstat ska också säkerställa att nationell rätt efterlevs vid tillhandahållande av information till Europol. Enligt förordningen föreligger således en uppgiftsskyldighet för de nationella myndigheterna gentemot Europol. Ansvaret för att översändandet av uppgifterna är lagenlig ligger enligt förordningen hos den medlemsstat som lämnade uppgifterna.

En annan skillnad i förhållande till rådsbeslutet är att den procedur enligt vilken Europol kan ingå avtal med tredjeland och villkoren för överförande av personuppgifter till tredjeland regleras. Europolförordningen innehåller även ett uppdaterat avsnitt med dataskyddsregler. Europolförordningen innehåller därmed en komplett och enhetlig uppsättning regler som omfattar alla relevanta aspekter av dataskydd och som är mer detaljerade än det nya dataskyddsdirektivet (se SOU 2017:29 s. 577).

Av artikel 41 framgår att Europols styrelse ska utse ett dataskyddsombud, som ska vara anställd vid Europol. Vid fullgörandet av sina arbetsuppgifter ska dataskyddsombudet agera oberoende.

15.4.3 Direktivets bestämmelser

Europol har enligt PNR-direktivet rätt att både motta och begära tillgång till PNR-information. Europols rätt att motta PNR-uppgifter framgår på flera ställen i direktivet. I artikel 4.2 anges att enheten för passagerarinformation ska ansvara för att bl.a. utbyta PNR-uppgifter och resultatet av behandlingen av dessa uppgifter med Europol. Även av artikel 6.2 a och b framgår att enheten för passagerarinformation får behandla PNR-uppgifter för ändamålen att tillhandahålla Europol resultatet av en behandling av dessa uppgifter. I artikel 6.2 a, som behandlar enhetens förhandsbedömningar, anges bl.a. att sådana ska göras för att identifiera personer som i förekommande fall Europol enligt artikel 10 behöver utreda ytterligare.

De närmare bestämmelserna om Europols tillgång till PNR-uppgifter finns i artikel 10. Av artikel 10.1 framgår att Europol, inom ramen för sina befogenheter och för fullgörandet av sina arbetsuppgifter, ska ha rätt att begära specifika PNR-uppgifter eller resultatet av behandlingen av dessa uppgifter från enheterna för passagerarinformation i medlemsstaterna. Detta ska, enligt artikel 10.2, gå till på så sätt att Europol från fall till fall via sin nationella enhet lämnar in en elektronisk, vederbörligen motiverad begäran om översändande av specifika PNR-uppgifter eller resultaten av behandlingen av dessa uppgifter till enheten för passagerarinformation i en medlemsstat. Europol får lämna in en sådan begäran när detta är absolut nödvändigt för att stödja och stärka medlemsstaternas åtgärder för att förebygga, förhindra, upptäcka eller utreda ett specifikt terroristbrott eller grovt brott i den mån brottet i fråga omfattas av Europols behörighet enligt Europolrådsbeslutet. I den motiverade begäran ska rimliga skäl anges till varför Europol anser att översändandet av PNR-uppgifterna eller resultaten av behandlingen av PNR-uppgifterna väsentligt kommer att bidra till att brottet i fråga förebyggs, upptäcks eller utreds.

Enligt artikel 10.3 ska Europol informera det dataskyddsombud som har utsetts i enlighet med artikel 28 i Europolrådsbeslutet om

varje informationsutbyte enligt den här artikeln. Som angetts finns en liknande bestämmelse i artikel 41 i Europolförordningen.

I artikel 10.4 anges att informationsutbyte enligt artikeln ska äga rum via Siena och i enlighet med Europolradsbeslutet. Det språk som används för framställningen och informationsutbytet ska vara det som gäller för Siena.

Av direktivets skäl 23 framgår att medlemsstaterna bör utbyta PNR-uppgifter som de har mottagit med Europol om det bedöms vara nödvändigt för att förebygga, förhindra, upptäcka utreda och lagföra terroristbrott och grov brottslighet. Vidare anges att bestämmelserna i direktivet inte bör påverka andra unionsinstrument om informationsutbyte mellan polismyndigheter och andra brottsbekämpande och rättsliga myndigheter. Som exempel på ett sådant unionsinstrument anges Europolradsbeslutet.

15.4.4 Våra överväganden och förslag

Vårt förslag: Enheten för passagerarinformation ska besvara en motiverad begäran från Europol och överföra PNR-information dit.

PNR-direktivets förhållande till Europolförordningen

PNR-direktivet innehåller hänvisningar till Europolradsbeslutet som upphörde att gälla den 1 maj 2017. Direktivets hänvisningar till radsbeslutet får därför tolkas som hänvisningar till den ersättande Europolförordningen.

Regleringen i Europolförordningen innebär bl.a. att Sverige, liksom övriga medlemsstater, har en skyldighet att lämna sådan information till Europol som är nödvändig för att den ska kunna uppfylla sina mål. PNR-uppgifterna utgör sådana uppgifter som kan vara nödvändiga för att Europol ska kunna uppfylla sina mål och utföra sina arbetsuppgifter. Uppgiftsskyldigheten omfattar således även PNR-uppgifter.

En tanke bakom PNR-direktivet är att det inte ska påverka andra unionsinstrument om informationsutbyte på det brottsbekämpande området. Uppgiftsskyldigheten i Europolförordningen kan därför sägas gälla framför PNR-direktivet (jfr SOU 2017:29 s. 577.). Dock

ansvarar enligt förordningen medlemsstaterna för att nationell rätt efterlevs vid tillhandahållande av information till Europol. För det fall det i svensk rätt genomförs närmare bestämmelser om hur PNR-uppgifterna får överföras till Europol, kommer dessa bestämmelser att behöva tillämpas av enheten för passagerarinformation vid överföringar till Europol.

Enligt vår bedömning är det inte tillräckligt att luta sig mot de bestämmelser om tillhandahållande av uppgifter som anges i Europolförordningen. För att genomföra PNR-direktivet på ett korrekt sätt bör vår lag även innehålla en bestämmelse som reglerar överföring av PNR-uppgifter till Europol. Hur uppgifterna därefter får behandlas av Europol och hur en eventuell vidarebefordran av uppgifter därifrån får gå till regleras av Europolförordningen. Därtill hörande data-skyddsfrågor regleras också i Europolförordningen.

Genomförandet av direktivets bestämmelser

Artikel 10 innehåller såväl skyldigheter för medlemsstaternas enheter för passagerarinformation att på begäran vidarebefordra PNR-information till Europol, som en rättighet för Europol att begära och motta sådana uppgifter. På samma sätt som vid överföring till andra medlemsstater ser vi det som vår uppgift att författningsreglera vår enhet för passagerarinformations skyldighet att i vissa fall översända uppgifter till Europol. I den mån bestämmelserna innehåller stadganden om i vilka fall och hur Europol ska gå till väga för att begära in PNR uppgifter från de nationella enheterna för passagerarinformation, bör dessa tas om hand av Europol. Det kan i vart fall inte ankomma på Sverige att genomföra dessa bestämmelser.

De grundläggande förutsättningarna för den svenska enheten för passagerarinformations överföring av PNR-information till Europol bör regleras i lag. En nationell bestämmelse om överföring av PNR-uppgifter till Europol bör innehålla den grundläggande anvisningen att PNR-information på begäran ska överföras till Europol. En sådan överföringsskyldighet kan enligt vår tolkning av direktivet inte begränsas till information om resenärer som har flugit, utan ska omfatta även uppgifter om resenärer som ännu inte har flugit. Således ska Europol på begäran kunna få tillgång till såväl förhandsbedömningar av passagerare (artikel 6.2 a) som information om tidigare

resor (artikel 6.2 b). Med hänsyn härtill och till skyldigheterna enligt Europolförordningen att tillhandahålla Europol med information, bör lagen inte innehålla närmare reglering om i vilka fall PNR-information får överföras till Europol. Innehållet i artikel 10 och direktivets skäl 23 medför dock enligt vår mening att det i bestämmelsen bör anges att en begäran från Europol ska vara motiverad. Härigenom säkerställs att överföringar endast sker för användning i verksamhet med att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

I artikel 10 anges inte närmare i vilken form de efterfrågade uppgifterna ska tillhandahållas. För det fall de begärda PNR-uppgifterna är äldre än sex månader kommer de uppgifter som kan användas för att omedelbart identifiera passagerare att vara maskerade (se avsnitt 13.4). För att utlämnande av fullständiga uppgifter i sådant fall ska få ske krävs att de förutsättningar som anges i artikel 12.3 är uppfyllda. Det finns inte något undantag i den bestämmelsen för det fall uppgifterna ska tillhandahållas Europol. Bestämmelsen är därför tillämplig även på sådana uppgifter som ska överföras dit. Denna fråga behandlas närmare nedan i avsnitt 15.5.

Enligt artikel 10.3 ska Europol informera sitt dataskyddsombud om varje informationsutbyte som sker enligt artikeln. Det bör ankomma på Europol, och således inte på den nationella lagstiftaren, att genomföra denna bestämmelse.

Bestämmelsen i artikel 10.4 innebär enligt vår tolkning att informationsutbytet med Europol ska ske via Siena och i enlighet med Europolförordningen. Dessa frågor behöver enligt vår mening inte författningsregleras.

15.5 Överföring av avmaskerade PNR-uppgifter

15.5.1 Direktivets bestämmelser

När de PNR-uppgifter som har överförts från lufttrafikföretagen har lagrats i databasen vid enheten för passagerarinformation under sex månader kommer de att vara maskerade på ett sådant sätt att uppgifter som identifierar den eller de personer som uppgifterna avser döljs och bara blir tillgängliga efter en avmaskering. Om någon utanför enheten för passagerarinformation som enligt direktivet har rätt att få ta del av PNR-uppgifter begär tillgång till uppgifter, kom-

mer därmed endast de maskerade uppgifterna att lämnas ut. Fullständiga PNR-uppgifter kan dock lämnas ut även efter den inledande sexmånadersperioden i vissa fall.

I artikel 12.3 anges således att vid utgången av sexmånadersperioden ska utlämnande av fullständiga PNR-uppgifter tillåtas endast om två förutsättningar är uppfyllda.

För det första ska ett utlämnande rimligen kunna antas vara nödvändigt för de ändamål som anges i artikel 6.2 b. Av den bestämmelsen följer att enheten får behandla personuppgifter för ändamålet att i enskilda fall besvara en vederbörligen motiverad förfrågan som bygger på tillräckliga skäl från de behöriga myndigheterna om att tillhandahålla och behandla PNR-uppgifter i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet och tillhandahålla de behöriga myndigheterna eller, när så är lämpligt, Europol resultaten av en sådan behandling.

För det andra krävs tillstånd från

- a) en rättslig myndighet, eller
- b) en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång (på eng. *disclosure*) är uppfyllda. Detta gäller under förutsättning att dataskyddsombudet vid enheten för passagerarinformation informeras och att denne genomför en efterhandsutvärdering.

Enligt artikel 9.2 sista meningen och 9.3 gäller likalydande villkor vid utlämnande från enheten till en enhet eller behörig myndighet i en annan medlemsstat. I artikel 9.2 anges således att enheten för passagerarinformation ska tillhandahålla avmaskerade uppgifter endast om det rimligen kan antas vara nödvändigt för de ändamål som anges i artikel 6.2. b och detta endast efter tillstånd från en behörig myndighet som avses i artikel 12.3 b. I artikel 9.3 hänvisas till denna bestämmelse.

I artikel 11.1 d görs också en hänvisning varav framgår att samma villkor också gäller vid överföring till tredjeland, utöver de ytterligare begränsningar som finns föreskrivna i artikel 11, se avsnitt 17.3.2.

15.5.2 Vilka överföringar kräver att särskilda förutsättningar är uppfyllda?

Vårt förslag: Överföring av avmaskerade PNR-uppgifter ska bara få ske för ändamålet att besvara en begäran av behöriga mottagare eller tredjeland om tillgång till uppgifterna för användning i mottagarens verksamhet med att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Artikel 12.3 anger alltså förutsättningarna för överföring av fullständiga, dvs. avmaskerade PNR-uppgifter, efter den inledande sexmånadersperioden. Av artikeln framgår bl.a. att utlämnande av avmaskerade uppgifter bara får ske för ändamålet att besvara en begäran enligt artikel 6.2 b. Artikeln har en central funktion för integritetsskyddet i PNR-direktivet och måste genomföras av medlemsstaterna. Enligt vår uppfattning bör den genomföras genom reglering i den nya lagen. I bestämmelsen anges inte att de begränsande förutsättningarna enligt artikeln skulle vara tillämpliga endast vid överföring till någon särskild mottagare. Att bestämmelsen är tillämplig vid överföring på begäran från andra medlemsstaters enheter för passagerarinformation och behöriga myndigheter i de staterna framgår av artiklarna 9.2 och 9.3. En hänvisning i artikel 11.1 d innebär att bestämmelsen är tillämplig även vid överföringar på begäran till tredje-länder.

Det förhållandet att det i vissa artiklar särskilt anges att artikel 12.3 ska vara tillämplig vid en överföring kan, enligt vår mening, inte tas till intäkt för att bestämmelsen inte är tillämplig vid andra överföringar enligt lagen. Bestämmelsen i artikel 12.3 är generellt formulerad och träffar därmed överföringar från enheten för passagerarinformation till i och för sig behöriga mottagare. Artikel 12.3 ska därför tillämpas även vid överföringar till svenska behöriga myndigheter och till Europol. Att bestämmelsen är generellt tillämplig vid sådana överföringar som omfattas av direktivet bör framgå genom reglering i den nya lagen.

15.5.3 Vilken prövning ska enheten göra?

Vårt förslag: Enheten för passagerarinformation ska göra en egen bedömning av om en överföring av fullständiga uppgifter rimligen kan antas vara nödvändig för att besvara mottagarens begäran.

För att avmaskerade PNR-uppgifter, dvs. fullständiga uppgifter, ska få lämnas ut från enheten krävs alltså enligt artikel 12.3 a att det rimligen kan antas vara nödvändigt för de ändamål som avses i artikel 6.2 b (jfr artiklarna 9.2 sista meningen, 9.3 och 11.1 d).

Enligt vår tolkning av bestämmelserna innebär detta att en förutsättning för överföring av avmaskerade uppgifter är att en särskild förfrågan ställts till enheten av en behörig mottagare eller ett tredjeland. En ytterligare förutsättning är att enheten har gjort en egen prövning av motiven till förfrågan och funnit att det rimligen kan antas vara nödvändigt för att besvara förfrågan korrekt att mottagaren i sin bekämpning av terroristbrottslighet eller grov brottslighet får tillgång inte bara till maskerade PNR-uppgifter utan även till fullständiga uppgifter, dvs. avmaskerade uppgifter. Man kan givetvis fråga sig om det verkligen är ändamålsenligt att införa en sådan prövning eller kontroll när exempelvis en åklagare under pågående förundersökning fattat ett beslut om inhämtande av avmaskerade uppgifter, se nedan. Som vi ser det ställer direktivet dock krav på något slags egen prövning av enheten. Det är en annan sak att denna, i det nämnda fallet, kan göras tämligen summariskt och i praktiken inskränka sig till en kontroll av att det av begäran framgår att framställningen även omfattar utfående av avmaskerade, fullständiga uppgifter om en person (förutom den förutsättning som alltid ska prövas nämligen att mottagarens begäran sker i syfte att använda mottagna uppgifter för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet).

Direktivets bestämmelser om överföring av avmaskerade uppgifter ger inte medlemsstaterna utrymme att införa snävare förutsättningar för överföring än de som direktivet föreskriver. Således vore det som vi ser det inte förenligt med direktivet att t.ex. föreskriva att överföring av avmaskerade PNR-uppgifter bara skulle få förekomma om mottagaren avser använda uppgifterna i en förundersökning, dvs. inte i underrättelseverksamhet. Samtliga förutsättningar

för enhetens prövning av om en överföring av avmaskerade PNR-uppgifter är motiverad bör framgå genom bestämmelser i lagen som med vissa tillägg hänvisar till de bestämmelser som genomför artiklarna 6.2 b och 9.2.

I detta sammanhang förtjänar att påpekas att utlämnanden med stöd av tryckfrihetsförordningen inte kan begränsas på grund av de bestämmelser vi föreslår för att genomföra direktivet.

15.5.4 Vem ska lämna tillstånd till överföring av fullständiga uppgifter?

En ytterligare förutsättning för överföring av avmaskerade uppgifter, dvs. fullständiga PNR-uppgifter, är som redan nämnts att det finns tillstånd till överföringen från

- a) en rättslig myndighet, eller
- b) en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda, under förutsättning att dataskyddsombudet vid enheten för passagerarinformation informeras och att denne gör en efterhandsutvärdering.

I EU:s rättsakter för samarbete i rättsliga frågor används ofta begreppet rättslig myndighet. Med en sådan myndighet avses enligt en vedertagen uppfattning i första hand domstol eller, för svenska förhållanden, åklagare. PNR-direktivet öppnar dock även upp för att en annan nationell myndighet kan lämna behövligt tillstånd. Frågan är hur detta krav ska tillgodoses i Sverige. Vi kommer nedan att analysera frågan om vilken myndighet det bör vara som ger tillstånd eller godkänner utlämnande från enheten för passagerarinformation av avmaskerade uppgifter. Som en bakgrund redogör vi dock först för ett delvis näraliggande exempel med brottsbekämpande myndigheters tillgång till teleoperatörens datalagrade uppgifter där frågan om hur tillgången ska prövas har diskuterats ingående. Vidare redovisar vi i korthet den parallellt med vår utredning pågående processen i EU-domstolen angående PNR-avtalet mellan Kanada och EU.

Datalagring

Brottsbekämpande myndigheters tillgång till trafikuppgifter om elektronisk kommunikation via data- eller telenät företer vissa likheter med systemet för lagring och utbyte av PNR-uppgifter. I båda fallen handlar det om att enskilda aktörer åläggs skyldigheter att tillhandahålla sin för kommersiella syften insamlade information för brottsbekämpande ändamål. I båda fallen finns bakomliggande EU-direktiv och i båda fallen handlar det om generell lagring av oselekterade uppgifter för sådant ändamål. Det sista syftar på att uppgifter om alla användare av elektronisk kommunikation och alla passagerare blir behandlade, trots att det beträffande nästan alla helt saknas anledning att anta att de kan vara inblandade i brottslighet av något slag.

Det finns dock stora skillnader. Systemet med datalagring av trafikuppgifter innebär en skyldighet för teleoperatörer m.fl. att lagra sin kommersiella information om kunders teletrafik m.m. under viss tid och således inte att leverera den till en nationell enhet för att där samlas i en databas såsom enligt PNR-systemet. Inom lagringstiden för trafikuppgifter, sex månader, ska det vara möjligt för brottsbekämpande myndigheter att under vissa förutsättningar få ut informationen från teleoperatörerna. Beskrivningen i det följande tar sikte på sådan lagring av trafikuppgifter som avser vem som kommunicerade med vem, när och hur länge det skedde, var de som kommunicerade befann sig och vilken typ av kommunikation som användes. Uppgifterna om innehållet i kommunikationen omfattas alltså inte.

Datalagringsdirektivet och det svenska genomförandet

Datalagringsdirektivet¹, som antogs den 15 mars 2006, syftade till att harmonisera medlemsstaternas bestämmelser om skyldighet att lagra vissa uppgifter om elektronisk kommunikation för att på så sätt säkerställa att uppgifterna är tillgängliga för avslöjande, utredning och åtal av allvarliga brott. Direktivet genomfördes i svensk rätt bl.a. genom införandet av nya bestämmelser i 6 kap. 16 a–f §§ lagen (2003:389) om elektronisk kommunikation (LEK).

¹ Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

Tillgång till datalagrade uppgifter var inget nytt verktyg inom den svenska brottsbekämpningen när datalagringsdirektivet antogs. Redan vid genomförandet av datalagringsdirektivet var tillgången reglerad såsom ett hemligt tvångsmedel i 27 kap. 19 § RB genom bestämmelser om hemlig teleövervakning (numera hemlig övervakning av elektronisk kommunikation). Den regleringen var och är tillämplig när trafikuppgifter ska inhämtas i en förundersökning. Tillstånd meddelas av allmän domstol. I lagen om elektronisk kommunikation fanns vidare bestämmelser om tillgång till trafikuppgifter i bl.a. underrättelseverksamhet. Dessa bestämmelser upphävdes dock vid genomförandet av datalagringsdirektivet och ersattes dels av bestämmelser i rättegångsbalken som under vissa förutsättningar möjliggör hemlig övervakning av elektronisk kommunikation i en förundersökning även om det inte finns någon som är skäligen misstänkt för brott, dels av bestämmelser i en ny lag om inhämtning av sådana uppgifter i underrättelseverksamhet.

Frågan om beslutsordningen i underrättelseverksamhet blev i förarbetena till inhämtningslagen föremål för regeringens allmänna överväganden (prop. 2011/12:55 s.88 f.). Regeringen bedömde att rätten att hämta uppgifter om elektronisk kommunikation i förundersökningar alltid ska prövas av domstol. Att allmän domstol fattar beslut om hemliga tvångsmedel under en förundersökning ansågs lämpligt och väl förenligt med det tvåpartsförfarande och de möjligheter till rättslig prövning som gäller där. Vidare ställde sig regeringen frågan om allmän domstol borde fatta beslut om inhämtning i underrättelseverksamhet. I ett utförligt resonemang betonades det bl.a. att det vore principiellt tveksamt att de allmänna domstolarna på förhand rättsligt prövar olika åtgärder som vidtas inom ramen för underrättelseverksamhet. Därmed kunde det finnas risk för att domstolens roll som oberoende prövningsinstans i brottmålsförfarandet ifrågasätts, i varje fall när åtgärderna senare leder fram till förundersökning och åtal. En sådan roll skulle för domstolen också vara delvis främmande i det svenska rättssystemet. Domstolarna kunde inte heller tillgodose behovet av snabba beslut utanför kontorstid. Mot den bakgrunden ansåg regeringen att allmänna domstolar inte borde ges beslutanderätten för inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Att tilldela åklagare en roll i polisens allmänna underrättelsearbete ansågs också olämpligt. Beslutanderätten borde

därför inte heller läggas hos åklagare. Inte heller ansågs det lämpligt att inrätta särskilda beslutsnämnder för beslut om inhämtning av övervakningsuppgifter i underrättelseverksamhet. I stället landade regeringen i bedömningen att beslutanderätten borde tillkomma de inhämtande myndigheterna själva med myndighetschefen som beslutande, dock med möjlighet till delegation.

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) reglerar alltså Polismyndighetens, Säkerhetspolisens och Tullverkets möjligheter att hämta in uppgifter om elektronisk kommunikation i underrättelseverksamhet. Beslut om inhämtning enligt inhämtningslagen fattas av myndigheten själv och är inte föremål för någon utomstående förhandskontroll (4 §). Det är myndighetschefen som fattar beslut om inhämtning av trafikuppgifter. Myndighetschefen får delegera rätten att fatta beslut om inhämtning till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Den som rätten att fatta beslut har delegerats till, får inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon deltar i. Enligt 5 § gäller vissa krav på innehållet i beslutet. I 6 § föreskrivs vidare att Säkerhets- och integritetsskyddsmyndigheten (SIN) ska underrättas om beslut om inhämtning av trafikuppgifter enligt inhämtningslagen. Enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet har nämnden tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel.

Sammanfattningsvis fungerar systemet således på det sättet att när trafikuppgifter hämtas in i en pågående förundersökning, gäller rättegångsbalkens bestämmelser om hemlig övervakning av elektronisk kommunikation med krav på tillstånd från allmän domstol efter ansökan av åklagare, dvs. förundersökningsledaren. I brådskande fall har åklagaren dock möjlighet att fatta interimistiska beslut i väntan på rättens prövning. Inhämtande i underrättelseverksamhet beslutas av varje myndighet själv. Tullverkets myndighetschef, eller efter delegation någon annan inom Tullverket, prövar inhämtande i Tullverkets underrättelseverksamhet osv. Enskilda som har utsatts för tvångsmedlet ska normalt underrättas om åtgärden i efterhand om det handlar om inhämtning i förundersökning men inte om det gäller underrättelseverksamhet. I underrättelseverksamhet ska i stället SIN underrättas om myndighetsbeslut att inhämta trafikuppgifter.

EU-domstolens domar och frågans fortsatta behandling

Den 8 april 2014 meddelade EU-domstolen dom i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., angående giltigheten av datalagringsdirektivet med anledning av begäran om förhandsavgöranden från nationella domstolar i Irland respektive Österrike. EU-domstolen förklarade i domen datalagringsdirektivet ogiltigt. Domstolen angav att direktivet innebar ett långtgående och synnerligen allvarligt ingrepp i rätten till privatliv och skyddet av personuppgifter. Enligt domstolen hade EU:s lagstiftande församlingar överskridit sina befogenheter då direktivet antogs eftersom regleringen inte ansågs leva upp till den unionsrättsliga proportionalitetsprincipen. Bl.a. framhöll domstolen som en brist i datalagringsdirektivet att tillgången till lagrade uppgifter inte var underkastad någon förhandskontroll av en domstol eller oberoende myndighet som har till uppgift att se till att tillgången begränsas till vad som kan anses vara strikt nödvändigt (punkterna 61 och 62).

De svenska reglerna om datalagring, tillgång till och behandling av datalagrade uppgifter samt bestämmelsernas förhållande till unionsrätten, blev därefter föremål för ingående analys (se Ds 2014:23 och SOU 2015:31). Bland annat analyserades inhämtningslagens förenlighet med unionsrätten, däribland bestämmelsen i 4 § som innebär att uppgifter inhämtas av en myndighet utan föregående prövning av en oberoende instans. Denna förnyade prövning av beslutsordningen ledde dock inte till något förslag till lagändring. Bedömningen gjordes alltså att beslut även i fortsättningen borde fattas av Polismyndigheten, Säkerhetspolisen eller Tullverket. Resonemangen bakom detta kan sägas i stora drag överensstämma med överväganden från förarbetena till inhämtningslagen som redovisats ovan.

Den 21 december 2016 meddelade EU-domstolen förhandsavgörande i de förenade målen C-203/15 och C-698/15, Tele2 Sverige och Watson m.fl., med anledning av begäran från bl.a. Kammarrätten i Stockholm respektive en domstol i Storbritannien. Den svenska begäran om förhandsavgörande framställdes i ett mål mellan Tele2 Sverige AB (Tele2) och Post- och telestyrelsen (PTS) om ett föreläggande från PTS för Tele2 att lagra trafikuppgifter och lokaliseringsuppgifter avseende bolagets abonnenter och registrerade användare. De frågor som ställts av Kammarrätten avsåg om de svenska bestämmelserna om lagring av och tillgång till uppgifter om elektro-

nisk kommunikation är förenliga med unionsrätten. EU-domstolens slutsats i förhandsavgörandet var bl.a. att en generell och odifferentierad lagring av uppgifter om elektronisk kommunikation inte är förenlig med EU-rätten. Vidare påtalade domstolen att unionsrätten utgör hinder för en nationell lagstiftning som reglerar behöriga nationella myndigheters tillgång till lagrade trafik- och lokaliseringsuppgifter och som inte, inom ramen för brottsbekämpning, föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet.

I dom den 7 mars 2017 upphävde Kammarrätten beslutet att förelägga Tele2 att lagra trafikuppgifter m.m. för brottsbekämpande ändamål. I domen anges att det, med hänsyn till EU-domstolens uttalanden, är klarlagt att de svenska bestämmelserna om lagring av trafikuppgifter m.m. för brottsbekämpande ändamål står i strid med unionsrätten och därför inte kan tillämpas. Domen har vunnit laga kraft.

Regeringen har gett en särskild utredare i uppdrag att bl.a. se över bestämmelserna om skyldigheten för leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster att lagra uppgifter om elektronisk kommunikation samt om de brottsbekämpande myndigheternas tillgång till sådana uppgifter, Utredningen om datalagring och EU-rätten (Ju 2017:04). Översynen ska ske i syfte att anpassa det svenska regelverket till EU-rätten såsom den uttolkats av EU-domstolen. Häri ingår bl.a. att se över beslutsordningen för att hämta in lagrade uppgifter. Uppdraget i denna del ska redovisas senast den 9 oktober 2017.

EU:s PNR-avtal med Kanada

Europaparlamentet har begärt EU-domstolens yttrande angående ett planerat nytt avtal mellan Kanada och EU om överföring och behandling av passageraruppgifter. Enligt avtalet ska lufttrafikföretag vid resor mellan Kanada och EU överföra PNR-uppgifter till kanadensiska myndigheter för användning i syfte att förebygga och upptäcka terroristbrottslighet eller andra allvarliga gränsöverskridande brott.

Den 8 september 2016 meddelade generaladvokaten ett förslag till yttrande.² Yttrandet ska inte redovisas närmare här. Av intresse är dock att generaladvokaten fann det utgöra en brist att den i Kanada insamlade myndigheten, CBSA, själv fattar beslut om utlämnande till en annan myndighet i Kanada eller annat tredjeland utan att dess bedömning av skydds nivån för uppgifterna hos mottagaren är underställd någon förhandskontroll av en oberoende myndighet eller en domstol.

EU-domstolen har ännu inte meddelat sitt avgörande i målet.

Våra överväganden och förslag

Våra förslag: En förutsättning för att en överföring av avmaskerade PNR-uppgifter ska vara tillåten är att en åklagare har beslutat att fullständiga uppgifter ska hämtas in i en pågående förundersökning som handläggs hos någon behörig svensk myndighet eller, i alla andra fall, att Polismyndighetens myndighetschef har godkänt överföringen. Rikspolischefen ska med vissa begränsningar kunna delegera beslutanderätten.

Bortsett från fall då en svensk åklagare beslutat om inhämtande av fullständiga uppgifter, ska dataskyddsombudet vid enheten för passagerarinformation informeras och göra en efterhandsutvärdering av varje överföring av avmaskerade uppgifter.

Några utgångspunkter

Bestämmelsen om att utlämnande av avmaskerade PNR-uppgifter kräver tillstånd från en rättslig myndighet eller annan nationell myndighet fanns inte med i kommissionens förslag till PNR-direktiv från år 2011 utan tillkom i de senare förhandlingarna. Enligt kommissionens förslag skulle tillgång till avmaskerade PNR-uppgifter endast kunna beviljas av chefen för enheten för passagerarinformation. Denna justering i direktivet kan, menar vi, inte tolkas på annat sätt än att det byggts in ett krav på något slag av tilläggskontroll av enhetens egen prövning av att förutsättningarna för överföring av av-

² Förslag till yttrande av generadvokat Paolo Mengozzi, föredraget den 8 september 2016.

maskerade PNR-uppgifter är uppfyllda. Ett genomförande som innebär att chefen för enheten för passagerarinformation beslutar om överföringen uppfyller alltså inte kravet på sådant tillstånd (eller godkännande) som föreskrivs i artikel 12.3 b.

Det kan konstateras att det inte finns någon myndighet som är självskriven för tillståndsgivningen. Något system med lagring och tillgång till PNR-uppgifter i viss brottsbekämpning på det sätt som avses ske enligt PNR-direktivet förekommer inte i Sverige. Det finns därför inte någon nuvarande ordning att ta avstamp i vid bedömningen av hur direktivets krav på tillstånd till utlämnande – eller som det uttrycks i den engelska versionen av artikel 12.3 b *approved by* (jfr *godkendt af* i den danska versionen) – ska genomföras. Inte heller finns det någon erfarenhet att falla tillbaka på för att kunna göra antaganden om hur ofta eller i vilka slags situationer man kan förmoda att förfrågningar kommer att göras avseende PNR-uppgifter som avser flygresor längre tillbaka i tiden än sex månader. Någon klar bild av huruvida förfrågningar om överföring av avmaskerade personuppgifter kan komma att bli aktuellt bara under pågående brottsutredningar där det finns eller inte finns någon skäligen misstänkt, dvs. i förundersökningsförfarandet, eller om också underrättelseverksamhet kan komma i fråga finns ännu inte. Över huvud taget framstår det alltså som relativt osäkert exakt hur behöriga myndigheter kommer att nyttja systemet och vilka kvantiteter avmaskerade uppgifter som kan komma att efterfrågas. Vi måste därför ta höjd för att detta kan komma att begäras ut i såväl förundersökningsverksamhet som underrättelseverksamhet så som direktivets bestämmelser förpliktar medlemsstaterna att möjliggöra. Det är dock vår uppfattning att när det handlar om så pass gamla identitetsuppgifter på flygpassagerare, sex månader eller äldre, torde dessa väl så ofta vara av intresse i brottsutredningar som i underrättelseverksamhet. Ett tänkbart exempel är att en kurir, som gripits på Arlanda för grovt narkotikabrott, berättar om tidigare liknande flygresor. För att i förundersökningen kunna nysta i detta och få fram information om den bakomliggande organisationen skulle det då kunna vara av intresse att få fram uppgifter om mellan vilka destinationer dessa resor gått, vem som bokat och betalat, och i så fall vilka ytterligare flygresor som betalats med samma kontouppgifter osv. Men det kan också vara så att ett inkommet tips om brottslig verksamhet ger

anledning att göra förfrågningar till enheten för att skaffa sig mer substans inför ett eventuellt beslut om att inleda förundersökning.

I linje med hur man resonerat i tidigare lagstiftningsärenden om beslutsordning för brottsbekämpande åtgärder som är ingripande för enskilda berörda anser vi att det finns skäl att göra skillnad mellan om behöriga myndigheter begär ut avmaskerade PNR-uppgifter under en pågående förundersökning eller om det handlar om under rättelseverksamhet.

Behörig myndighets begäran sker i en förundersökning

Förundersökning är ett reglerat förfarande, se 23 kap. RB och förundersökningskungörelsen (1947:948). Beslut att inleda förundersökning kan fattas av Polismyndigheten, Säkerhetspolisen eller åklagare. Även Tullverket kan fatta beslut om inledande av förundersökning enligt 19 § lagen (2000:1225) om straff för smuggling (smugglingslagen). De befogenheter och skyldigheter som undersökningsledaren har enligt rättegångsbalken gäller i sådant fall Tullverket.

Har förundersökningen inletts av Polismyndigheten eller Säkerhetspolisen och är saken inte av enkel beskaffenhet, ska ledningen av förundersökningen om brottet övertas av åklagaren så snart någon skäligen kan misstänkas för brottet. Åklagaren ska också i annat fall överta ledningen när det är motiverat av särskilda skäl (23 kap. 3 § RB). Liknande bestämmelser finns i smugglingslagen. En förundersökning kan alltså ledas av en åklagare, en polisiär undersökningsledare eller en tulltjänsteman. När förundersökningen leds av åklagaren, får han eller hon anlita biträde av Polismyndigheten, Säkerhetspolisen eller Tullverket för att genomföra den. Åklagaren får också uppdra åt en polisman eller tjänsteman vid Tullverket att vidta en viss åtgärd som hör till förundersökningen, om det är lämpligt med hänsyn till åtgärdens beskaffenhet.

Enligt 23 kap. 4 § RB ska en förundersökning bedrivas objektivt. Vid förundersökningen ska förundersökningsledaren söka efter, ta till vara och beakta omständigheter och bevis som talar såväl till den misstänktes fördel som till hans eller hennes nackdel. Förundersökningen ska bedrivas så att inte någon onödigt utsätts för misstanke eller orsakas kostnad eller olägenhet.

En mängd olika mer eller mindre ingripande åtgärder kan vidtas under en förundersökning. Vissa för enskilda berörda särskilt ingripande åtgärder under pågående förundersökning regleras som straffprocessuella tvångsmedel i 24–28 kap. RB, exempelvis frågor om frihetsberövande, vissa andra begränsningar i rörelsefriheten, kvarstad, beslag, husrannsakan och kroppsbesiktning. I 27 kap. regleras en specialform av tvångsmedel, nämligen hemliga tvångsmedel, bl.a. hemlig övervakning av elektronisk kommunikation som tidigare omfattades av datalagringsdirektivet, se ovan.

Gemensamt för all tvångsmedelsanvändning enligt rättegångsbalken är att beslutsförfarandet är reglerat. Vid de mera ingripande tvångsmedlen är allmän domstol ensam behörig att fatta beslut (t.ex. häktning, kvarstad, hemlig rumsavlyssning, hemlig avlyssning eller övervakning av elektronisk kommunikation), dock med rätt i vissa fall för åklagare att fatta interimistiskt beslut i brådskande fall.

Beträffande många andra i och för sig ingripande åtgärder under pågående förundersökning finns inte någon motsvarande reglering som den i rättegångsbalken för tvångsmedel. Exempel härpå är användning i förundersökning av vissa spanings- eller utredningsmetoder såsom infiltration eller provokation. Vad gäller just dessa metoder har i stället utfärdats riktlinjer av Åklagarmyndigheten, RÅR 2016:1. Av dessa framgår bl.a. att beslut om användande av sådana metoder alltid ska fattas av den allmänna åklagare som är förundersökningsledare.

Trots den osäkerhet som finns angående hur behöriga myndigheter kommer att använda sig av möjligheten att begära ut PNR-uppgifter är det vår uppfattning att en sådan åtgärd inte är att jämställa med ett sådant hemligt tvångsmedel som bör regleras som ett sådant i rättegångsbalken. Visserligen finns paralleller med utfående av datalagrad elektronisk kommunikation från teleoperatörer, vilket utgör ett hemligt tvångsmedel benämnt hemlig övervakning av elektronisk kommunikation. Beträffande PNR-systemet handlar det emellertid om utfående av uppgifter som redan har samlats in och använts i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra vissa brott genom lagring i databasen och förhandsbedömning av passagerare vid enheten för passagerarinformation. Vi ser därför ingen anledning att införa någon reglering i rättegångsbalken om behöriga myndigheters tillgång till PNR-uppgifter under pågående förundersökning och hur det ska beslutas. Det vore vidare syste-

matiskt inkonsekvent att införa förändringar i det straffprocessuella regelverket som vore kopplade enbart till sådana PNR-uppgifter hos enheten för passagerarinformation som lagrats en viss tid och därför maskerats, medan andra PNR-uppgifter som lagrats under kortare tid inte skulle omfattas av regleringen.

Vid bedömningen av hur tillståndsgivningen enligt PNR-direktivet ska genomföras kan diskuteras om denna har en i övrigt straffrättslig karaktär eller om den innebär en prövning av annat slag. Av direktivets skäl 25 framgår att den maskering av PNR-uppgifter som ska ske efter sex månader syftar till att undvika oproportionell användning av uppgifterna. Åtkomst till de fullständiga PNR-uppgifterna ska därefter endast få ske under mycket strikta och begränsade villkor för att säkerställa högsta möjliga nivå av dataskydd. Syftet med kravet på tillstånd är således att säkerställa att personuppgifter inte används i onödan och att skydda den personliga integriteten. Det är som nyss sagts inte fråga om användande av något tvångsmedel, utan om tillstånd till överföring av fullständiga personuppgifter, i motsats till maskerade sådana. Samtidigt är förutsättningen för en överföring till behöriga myndigheter knuten till vad som kan antas vara nödvändigt för den brottsbekämpande verksamheten i fråga. Den bedömningen har en i allt väsentligt straffrättslig karaktär. Det ter sig därför lämpligast, menar vi, att prövningen görs av någon som har relevant erfarenhet och kunskap för att bedöma behoven i en förundersökning. I linje med vad vi tidigare anfört om att behöriga myndigheters utfående av avmaskerade PNR-uppgifter inte är något tvångsmedel finner vi det dock inte motiverat att i den nya lagen införa bestämmelser om att allmän domstol ska godkänna överföring av avmaskerade PNR-uppgifter.

Enligt vår mening tillgodoses direktivets krav och enskilda registrerade passagerares berättigade anspråk på ett tillfredsställande integritetsskydd om det införs en bestämmelse i den nya lagen som föreskriver att en begäran från en behörig myndighet om utfående av avmaskerade PNR-uppgifter ska ha beslutats av en åklagare, om förundersökning har inletts. Detta menar vi ska gälla oavsett om förundersökningen är i ett så pass inledande skede att den leds av en undersökningsledare som inte är åklagare.

Lydelsen av artikel 12.3 b i direktivet ger vid handen att det är enheten för passagerarinformation som ska inhämta ett tillstånd eller godkännande till utlämnande av avmaskerade PNR-uppgifter. I

praktiken uppnås dock samma resultat om det är den begärande behöriga myndigheten som inhämtar tillståndet eller godkännandet. Vi ser därför inget hinder mot att genomföra direktivets bestämmelse genom ett på så sätt ”omvänt” förfarande där den behöriga myndigheten införskaffar ett åklagarbeslut.

En svensk åklagare uppfyller rekvisiten på att vara en sådan rättslig myndighet som avses i artikel 12.3 b i direktivet. Direktivet ställer i och för sig inga krav på att den rättsliga myndigheten ska vara oberoende. Vi har dock övervägt om det är olämpligt att en förundersökningsledande åklagare själv fattar beslutet och därmed står för den särskilda kontrollmekanism som ska stoppa obefogad användning av äldre PNR-uppgifter. Förundersökningsförfarandet bygger emellertid på att det är förundersökningsledaren som har det övergripande ansvaret för utredningens bedrivande. Han eller hon ska åtnjuta en självständig ställning visavi utomstående. Några författningsreglerade bestämmelser om att annan åklagare än förundersökningsledaren ska besluta eller godkänna åtgärder finns inte. De möjligheter till överordnad åklagares övertagande av uppgifter som följer av 7 kap. 5 § RB skulle inte passa in för att hantera frågor om utfående av PNR-uppgifter. Någon befintlig ordning att lämna över visst beslutsfattande till en utomstående åklagare som PNR-frågorna skulle kunna inordnas i finns alltså inte. Vi ser det inte heller som nödvändigt eller lämpligt att införa någon nyordning för åklagarväsendet i syfte att genomföra artikel 12.3 b i PNR-direktivet. Det ingår i åklagares ordinarie arbete som förundersökningsledare att fatta beslut om ingripande åtgärder på ett rättssäkert sätt och med beaktande av proportionalitetsprincipen avseende alla motstående intressen, inte minst att väga effektiviteten i brottsbekämpningen mot intresset av att värna den personliga integriteten. Det torde vidare vara förundersökningsledaren som bättre än någon annan kan bedöma om förutsättningarna för utfående av avmaskerade PNR-uppgifter är uppfyllda, dvs. om de kan antas vara nödvändiga för brottsutredningen och därmed utgöra en proportionerlig användning. Beslut och åtgärder av detta slag ska dokumenteras i förundersökningsmaterialet vilket som huvudregel blir tillgängligt för den misstänktes insyn och granskning när utredningen är klar. Med tanke på att en begäran till enheten för passagerarinformation ska vara kopplad till ett behov avseende utredning eller lagföring av terroristbrottslighet eller grov brottslighet såsom den definieras i den nya lagen, kom-

mer det att i allmänhet vara erfarna åklagare som är förundersökningsledare. Mot denna bakgrund finner vi att övervägande skäl talar för inte införa något krav på att beslutsfattande åklagare ska vara någon annan än förundersökningsledaren.

Behörig myndighets begäran sker i underrättelseverksamhet

Av beskrivningen ovan om genomförandet av datalagringsdirektivet har framgått att det inte finns någon reglering om att vissa åtgärder i underrättelseverksamhet ska beslutas eller underställas någon rättslig myndighet eller någon oberoende myndighet av annat slag. Frågan har varit mycket omdiskuterad och bl.a. har Polismetodutredningen föreslagit inrättande av en nämnd för prövning av vissa särskilda spaningsmetoder under underrättelsestadiet (SOU 2010:103), vilket dock inte lett till vidare lagstiftningsåtgärder. Vi har inom ramen för vårt utredningsuppdrag inte haft möjligheten att göra sådana mera ingående analyser som skulle krävas för att föra frågan vidare och eventuellt finna någon ny lämplig övergripande ordning för hur frågor av detta slag skulle tas om hand. Med tanke på att det tillsatts en utredning som ska analysera EU-domstolens förhandsavgörande rörande det svenska införandet av datalagringsdirektivet ser vi det vidare som olämpligt att vi överväger någon nyordning av mer generell karaktär såsom t.ex. att föreslå tillskapandet av en ny instans för prövning av frågor av det aktuella slaget.

Våra överväganden och förslag får således anpassas till den befintliga strukturen. Det kan därvid konstateras att det inte finns någon befintlig myndighet som vore självskriven för att ge tillstånd till att behöriga myndigheter får tillgång till avmaskerade PNR-uppgifter i sitt underrättelsearbete.

Fyra olika existerande myndighetsorganisationer, utanför de behöriga myndigheterna själva, framstår som tänkbara för uppgiften. Dessa är domstolsväsendet, åklagarväsendet och de två tillsynsmyndigheter som för närvarande har tillsyn över polisens behandling av personuppgifter. Ingen av dessa har, som tidigare angetts, någon erfarenhet av tillståndsgivning i liknande fall. När det gäller domstolar och åklagarväsendet instämmer vi dock i de argument mot att lägga beslutsfunktioner hos dem som redovisats ovan i förarbetena till inhämtningslagen. Varken allmän domstol eller åklagare bör alltså

ges i uppgift att ta ställning till överföring av avmaskerade personuppgifter för användning i underrättelseverksamhet.

En annan lösning vore att lägga tillståndsgivningen hos någon av de myndigheter som har till uppgift att utöva tillsyn över den brottsbekämpande verksamheten. Datainspektionen och SIN har i dag överlappande tillsynsansvar när det gäller Polismyndighetens behandling av personuppgifter. Utredningen om tillsynen över den personliga integriteten har nyligen föreslagit att Datainspektionen ska utses till svensk nationell tillsynsmyndighet enligt både dataskyddsförordningen och det nya dataskyddsdirektivet (se SOU 2016:65). Vidare har utredningen föreslagit att tillsynen över den öppna polisens personuppgiftsbehandling i brottsbekämpande verksamhet inte längre ska ingå i SIN:s uppdrag utan i fortsättningen utföras endast av Datainspektionen. Enligt förslaget kommer Datainspektionen att bli nationell tillsynsmyndighet för Polismyndighetens behandling av personuppgifter i den brottsbekämpande verksamheten och därmed även för arbetet vid enheten för passagerarinformation.

Det vore olämpligt att använda sig av samma myndighet för tillståndsgivningen som för tillsynen över arbetet inom enheten som för passagerarinformation. Med hänsyn härtill skulle Datainspektionen vara utesluten medan SIN däremot skulle kunna användas som tillståndsmyndighet enligt PNR-direktivet. Vid SIN finns en uppbyggd organisation för att hantera sekretesskyddat material härrörande från förundersökningar och underrättelsearbete. Det som talar mot en sådan lösning är att SIN inte är uppbyggd för att hantera frågor som uppkommer utanför ordinarie arbetstid och att det skulle innebära ett nytt slags aktiv inblandning i myndigheters pågående verksamhet än vad nämnden har i dag. Det är vår bedömning att det skulle medföra alltför stora förändringar i SIN:s organisation och arbetssätt för att det skulle vara lämpligt att göra nämnden till tillståndsgivare för överföring av PNR-uppgifter.

Det alternativ som återstår att överväga är därmed om frågan om tillstånd eller godkännande av en överföring kan beslutas av någon av de behöriga myndigheterna själva förutsatt att det ges av någon utanför enheten. PNR-direktivet föreskriver nämligen inte att det måste vara en oberoende myndighet som ska ge tillstånd som alternativ till en rättslig myndighet när det handlar om överföring av avmaskerade PNR-uppgifter.

Som framgått av ovan nämnda avgöranden från EU-domstolen har avsaknaden av kontroll av en oberoende myndighet i förhållande till brottsbekämpande myndigheters tillgång till uppgifter varit en av flera brister som domstolen riktat mot datalagringsdirektivet. Även när det gäller PNR-avtalet med Kanada har frågan dryftats, se ovan nämnda yttrande av generaladvokaten. Vårt uppdrag är emellertid att föreslå den författningsreglering som krävs för att genomföra PNR-direktivet i svensk rätt. Det ligger alltså inte i uppdraget att särskilt analysera om direktivet som sådant är förenligt med EU-stadgan. Vi kan dock inte se att det skulle vara oförenligt med vare sig PNR-direktivet eller med EU-stadgan att använda motsvarande beslutsordning för överföring av avmaskerade PNR-uppgifter som den som föreskrivs i inhämtningslagen. Utan att vi har kunnat göra någon mera ingående analys av EU-domstolens avgöranden finner vi nämligen att det finns ganska väsentliga skillnader mellan användning i brottsbekämpning av datalagrad elektronisk kommunikation respektive av PNR-uppgifter.

Det som enligt EU-domstolen gör datalagringen särskilt känslig ur integritetssynpunkt är att den innebär en kartläggning som möjliggör mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i. Dessutom sker den senare användningen av uppgifterna utan att den registrerade användaren är underrättad om detta, vilket kan ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning (se punkt 99 och 100 i EU-domstolens dom i de förenade målen C-203/15 och C-698/15).

Behandling, lagring och användning av PNR-uppgifter måste enligt vår bedömning anses som ett jämförelsevis väsentligt mindre allvarligt intrång i enskildas privatliv. Internationella flygresor är inget som flertalet människor normalt gör dagligdags, i vart fall inte för privata syften. Likaså torde flygpassagerare inte ha samma förväntningar på att flyga obemärkt och oregistrerat som den normala användaren av telefoner och datorer har när de samtalat eller använder dessa för att skicka och ta emot sms eller andra meddelanden. Även om den beslutade långtidslagringen av PNR-uppgifter är känslig ur ett integritetsperspektiv innebär den alltså typiskt sett inte ett

lika stort intrång i privatlivet som datalagringen. Av den anledningen anser vi att det finns goda skäl för att inte dra så långtgående slutsatser av EU-domstolens avgörande i datalagringsfrågorna att någon oberoende kontrollinstans måste ges i uppgift att godkänna överföring av avmaskerade PNR-uppgifter trots att detta inte är ett krav enligt PNR-direktivet. Inte heller anser vi att den parallella processen om PNR-avtalet med Kanada och generaladvokatens yttrande påverkar hur PNR-direktivet ska läsas. Vad som kritiseras i det avtalet är nämligen att det inte finns något oberoende kontrollorgan i det tredjelandet som prövar mottagarens skydds nivå vid vidareöverföring inom det tredjelandet, dvs. en något annorlunda frågeställning än den som gäller överföring av PNR-uppgifter till behöriga mottagare enligt PNR-direktivet.

Mot bakgrund av det sagda är det vår bedömning att övervägande skäl talar för att PNR-direktivets krav på tillstånd till överföring av avmaskerade PNR-uppgifter till behöriga myndigheter för användning i underrättelsearbetet i nuläget bör konstrueras på i huvudsak samma sätt som i inhämtningslagen, nämligen att enheten för passagerarinformation ska inhämta tillstånd från myndighetschefen för Polismyndigheten, dvs. rikspolischefen. Vi föreslår därför detta. Motsvarande möjlighet för delegation som i inhämtningslagen bör därvid finnas. Liksom i inhämtningslagen bör delegation inte kunna ske till någon som själv deltar i den verksamhet som har begärt ut informationen, en situation som dock bara kan uppkomma när det är Polismyndigheten som är den begärande behöriga myndigheten. Inte heller ska delegation kunna ges till någon som arbetar vid enheten för passagerarinformation.

Vid valet av en annan tillståndsmyndighet än en rättslig sådan ska enligt direktivets bestämmelser dataskyddsombudet vid enheten för passagerarinformation informeras och göra en efterhandsutvärdering varje gång avmaskerade PNR-uppgifter förs över till en behörig myndighet. Bestämmelser med denna innebörd kan föras in i förordningen. Hur efterhandsutvärderingen ska utföras bör inte närmare regleras. Det är dock givet att den ska gå ut på att kontrollera att de lagliga förutsättningarna för överföring har varit uppfyllda samt att det funnits behörigt tillstånd till överföringen. Vi kommer att i avsnitt 19.5 närmare behandla hur dataskyddsombudet ska utses och vilka uppgifter han eller hon ska ha. Då kommer vi också att närmare beröra vilka åtgärder som dataskyddsombudet bör vidta

om han eller hon vid sin efterhandsutvärdering konstaterar någon brist i hanteringen av överföringen eller liknande.

Bland annat på grund av att dataskyddsombudet alltid ska göra en egen utredning, med möjlighet att anmäla eventuella missförhållanden till tillsynsmyndigheten, har vi inte funnit skäl att överväga att underrättelse om överföring av avmaskerade PNR-uppgifter ska sändas till någon tillsynsmyndighet.

Avslutningsvis vill vi påtala att vi inte är omedvetna om att tillämpningen av beslutsordningen enligt inhämtningslagen i vissa fall föranlett en del kritik från tillsynsmyndigheten SIN. Det inger viss oro och talar för att, i händelse av att en ny ordning för beslutsfattande avseende inhämtning av datalagrade uppgifter eller andra åtgärder i underrättelseförfarande införs som en följd av den översyn av inhämtningslagen som nu genomförs, det kan finnas skäl att i framtiden överväga om också överföring av avmaskerade PNR-uppgifter ska inordnas i ett sådant nytt beslutsförfarande. Det vore dock av värde att kunna göra sådana överväganden först då PNR-systemet kommit igång och funnits en tid för att med erfarenheter från den faktiska hanteringen kunna göra närmare överväganden om vilken beslutsnivå osv. som bör gälla för överföringar enligt den nya lag som genomfört PNR-direktivet.

Begäran från andra länder och Europol

Om det framstår som oklart när, hur och för vilken närmare användning avmaskerade PNR-uppgifter kommer att begäras ut av svenska behöriga myndigheter framstår det som än mer ovisst vad som kommer att bli ett vanligt utbyte mellan medlemsstaterna och med Europol. Vi antar emellertid att det, när det gäller så pass "gamla" uppgifter att de blivit maskerade, kommer att kunna handla om att uppgifterna i den svenska databasen kan vara intressanta i en brottsutredning i en annan medlemsstat. Det hade i och för sig kunnat vara tänkbart att den svenska enheten för passagerarinformation skulle ha kunnat godta ett beslut från en utländsk domstol eller annan utländsk rättslig myndighet som tillåtit inhämtningen i en brottsutredning om terroristbrottslighet eller grov brottslighet i det landet. Vi vet emellertid inte hur andra medlemsstater kommer att genomföra PNR-direktivet och ett sådant omedelbart accepterande

av beslut från andra länders rättsliga myndigheter torde kräva en harmoniserad reglering av något slag.

Enligt direktivet kommer det vidare som huvudregel att vara en enhet för passagerarinformation som begär ut uppgifterna från den svenska enheten. Vilken bakomliggande information som då kommer att göras tillgänglig för den svenska enheten vet vi inte i nuläget, t.ex. om det kommer att bifogas beslut från en åklagare eller undersökningsdomare om att uppgifterna ska inhämtas i en viss brottsutredning eller underrättelseverksamhet. Gissningsvis kommer formulär eller något slags standardiserade ordningar införas för detta uppgiftsutbyte men än så länge finns inga sådana utarbetade. Redan av denna anledning anser vi att övervägande skäl talar för att begäran från andra medlemsstaters enheter och Europol alltid ska behandlas på samma sätt som begäran från svenska myndigheter utanför förundersökningsförfarandet. Det innebär att oavsett om uppgifterna begärs ut från en annan medlemsstat för att användas i en förundersökning eller i underrättelseverksamhet, ska Polismyndighetens myndighetschef fatta beslut om utlämnande och dataskyddsbudet göra en efterhandsutvärdering. Detsamma föreslår vi ska gälla i de absoluta undantagsfall när det kan bli aktuellt att lämna ut avmaskerade PNR-uppgifter till tredjeland enligt artikel 11.

16 Behöriga myndigheters behandling av PNR-information

16.1 Behöriga myndigheters rätt att motta och begära tillgång till PNR-information

PNR-systemet är uppbyggt så att endast sådan PNR-information som har behandlats vid en nationell enhet för passagerarinformation och som där har bedömts vara av intresse för bekämpning av sådan brottslighet som avses i direktivet, ska sändas vidare till utvalda myndigheter i det egna landet för vidare analys och åtgärder. Endast vissa nationella myndigheter kommer att på detta sätt få ta del av PNR-informationen. Dessa myndigheter har även rätt att under vissa förutsättningar ställa egna frågor till enheter för passagerarinformation och kan på så sätt begära att få ta del av sådan PNR-information som är av intresse just för den myndighetens bekämpande av terroristbrottslighet eller grov brottslighet.

PNR-information kommer således att vidarebefordras från enheten för passagerarinformation till de behöriga myndigheterna. Någon möjlighet för de behöriga myndigheterna att få tillgång till enhetens PNR-information genom direktåtkomst är inte tillåten (se avsnitt 10.4.1).

Som tidigare har angetts ska varje medlemsstat utse de myndigheter som ska vara behöriga att ta emot eller begära PNR-information. Dessa myndigheter ska ansvara för den vidare bearbetningen av informationen samt för att vidta lämpliga åtgärder för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Regeringen har den 4 maj 2017 utsett Polismyndigheten, Säkerhetspolisen, Tullverket, Ekobrottsmyndigheten och Försvarsmakten som behöriga myndigheter. Ytterligare myndigheter kan komma att utses i framtiden.

16.1.1 Behöriga myndigheters rätt att motta PNR-information

De behöriga myndigheterna kommer främst att få tillgång till PNR-information avseende sådana passagerare som den nationella enheten för passagerarinformation har valt ut vid de förhandsbedömningar som görs av passagerare före deras beräknade ankomst till eller avresa från Sverige (artikel 6.2 a och 6.6). Aktuella myndigheter kommer även att få tillgång till motsvarande uppgifter som har tagits fram av andra medlemsstaters enheter för passagerarinformation vid deras förhandsbedömningar och som i vissa fall därefter har överförs till den svenska enheten för vidare befordran till svenska behöriga myndigheter (se artikel 9.1 och 6.6).

Vidare kommer de behöriga myndigheterna att få tillgång till PNR-information som svar på sådana särskilda förfrågningar som myndigheterna har ställt till enheten för passagerarinformation (artikel 6.2 b). Även i dessa fall kan informationen komma från en motsvarande enhet i en annan medlemsstat och vidarebefordras till den behöriga myndigheten av den nationella enheten.

I undantagsfall kan PNR-information även överföras direkt till en behörig myndighet från en enhet för passagerarinformation i en annan medlemsstat som svar på en särskild begäran, se nedan i avsnitt 16.1.2.

16.1.2 Behöriga myndigheters möjlighet att begära tillgång till PNR-information

De behöriga myndigheterna har, som framgått ovan, en möjlighet att ställa egna frågor till enheten för passagerarinformation och på så sätt få tillgång till sådan PNR-information som myndigheten bedömer är nödvändig i dess verksamhet. För att en sådan begäran ska besvaras krävs, enligt artikel 6.2 b, att den är vederbörligen motiverad och bygger på tillräckliga skäl. Förfrågan ska vidare avse ett specifikt fall och syfta till att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Det finns enligt direktivet även en möjlighet för de behöriga myndigheterna att vända sig direkt till en enhet för passagerarinformation i en annan medlemsstat för att få ta del av sådan PNR-information som finns lagrad hos den enheten. Denna möjlighet, som regleras i artikel 9.3, ska dock endast användas i nödfall och

i övrigt enligt de villkor som fastställts i artikel 9.2 (se avsnitt 15.3.3). Även i dessa fall ska begäran vara motiverad. En kopia av begäran ska alltid skickas till enheten för passagerarinformation i den begärande medlemsstaten. Möjligheten för en behörig myndighet att vända sig direkt till en enhet för passagerarinformation i en annan medlemsstat ska endast användas i undantagsfall. I alla andra fall ska, enligt artikel 9.3, de behöriga myndigheterna översända sina framställningar via enheten för passagerarinformation i den egna medlemsstaten.

16.1.3 Våra överväganden och förslag

Våra förslag: En behörig myndighet som önskar ta del av PNR-information som lagras hos en enhet för passagerarinformation i en annan medlemsstat ska framställa begäran till enheten för passagerarinformation vid Polismyndigheten för vidare förmedling till den andra medlemsstaten.

Endast om det i ett enskilt brådskande fall är absolut nödvändigt får en behörig myndighet vända sig direkt till enheten för passagerarinformation i en annan medlemsstat med en begäran om att ta del av PNR-information som lagras hos den enheten. En behörig myndighet som har framställt en sådan begäran ska skicka en kopia av begäran till enheten för passagerarinformation vid Polismyndigheten.

Frågorna kan regleras i förordning.

Införandet av en bestämmelse som innebär att PNR-information ska överföras från enheten för passagerarinformation till de behöriga myndigheterna har föreslagits i avsnitt 15.2.2. Det saknas anledning att därutöver även reglera i vilka situationer de behöriga myndigheterna har rätt att motta den överförda PNR-informationen. Detsamma gäller för det fall PNR-information skulle komma myndigheten till del från en enhet för passagerarinformation i en annan medlemsstat. Det får nämligen förutsättas att den översändande medlemsstaten tillser att överföringen sker i enlighet med direktivets bestämmelser.

Vidare saknas det enligt vår bedömning anledning att författningsreglera de närmare förutsättningarna för att en behörig myn-

dighet ska få tillgång till PNR-information från enheten för passagerarinformation. Enligt vår mening bör det i stället vara upp till enheten att bedöma vilka förfrågningar som får och ska besvaras. Således är det upp till enheten för passagerarinformation att bedöma t.ex. huruvida en begäran är tillräckligt motiverad för att den efterfrågade PNR-informationen ska föras över till den efterfrågande myndigheten. När det gäller en begäran om att få ta del av PNR-information som lagras hos en enhet för passagerarinformation i en annan medlemsstat har vi i avsnitt 15.3.4 redan föreslagit en bestämmelse i förordningen som innebär att en sådan begäran får göras endast om syftet därmed faller inom ramen för när PNR-information alls får behandlas enligt lagens portalparagraf som bl.a. genomför artikel 1.2 i direktivet, dvs. för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Den bestämmelsen bör vara tillämplig även när en behörig myndighet begär tillgång till PNR-information.

Vidare bör det av författning framgå att en begäran från en behörig myndighet om att få ta del av PNR-information som lagras hos en enhet för passagerarinformation i en annan medlemsstat som huvudregel ska framställas till enheten för passagerarinformation vid Polismyndigheten för vidare förmedling till den andra medlemsstaten (jfr artikel 9.3). Denna fråga kan regleras i förordning. Det bör också i förordning regleras att en behörig myndighet endast i undantagsfall har rätt att vända sig direkt till en enhet för passagerarinformation i en annan medlemsstat med en begäran om att få ta del av sådan information som finns bevarad vid den enheten. Enligt artikel 9.3 får en sådan begäran endast framställas i nödfall. Med nödfall torde menas detsamma som om det absolut krävs eller är absolut nödvändigt. Enligt vår mening passar uttrycket absolut nödvändigt bättre in i svensk lagstiftning. Vi föreslår därför att detta uttryck används i författningstexten.

En situation där det skulle kunna anses absolut nödvändigt för en behörig myndighet att vända sig direkt till en enhet för passagerarinformation i en annan medlemsstat skulle kunna uppstå om myndigheten finner att det finns risk för ett nära förestående terroristattentat och det är nödvändigt att så snabbt som möjligt få information om en misstänkts resväg. Enligt vår bedömning kommer dock bestämmelsen troligen inte att användas i praktiken. För de behöriga myndigheterna kommer det sannolikt att gå snabbare att begära in

den önskade informationen via den nationella enheten för passagerarinformation, som har upparbetade vägar för utbyte med motsvarande enheter, i stället för att myndigheterna själva ska ta dessa kontakter.

För det fall en behörig myndighet har begärt PNR-information direkt från en enhet för passagerarinformation i en annan medlemsstat, ska en kopia av begäran skickas till den nationella enheten för passagerarinformation. Även denna fråga kan regleras i förordning.

16.2 Behandling av PNR-information vid de behöriga myndigheterna

PNR-direktivet innehåller endast ett fåtal bestämmelser som rör behandlingen av den PNR-information som har vidarebefordrats från enheten för passagerarinformation till de behöriga myndigheterna. Bestämmelserna, som finns i direktivets artikel 7, kommer att beröras i det följande. Först följer dock en kort beskrivning av gällande dataskyddsbestämmelser på området och våra allmänna överväganden gällande de behöriga myndigheterna.

16.2.1 Tillämpliga dataskyddsbestämmelser hos de behöriga myndigheterna

Polisdatalagen är för närvarande tillämplig vid behandling av personuppgifter i brottsbekämpande verksamhet vid Polismyndigheten och Säkerhetspolisen. Lagen gäller även för den polisiära verksamheten vid Ekobrottsmyndigheten. Enligt vad vi erfarit är det endast till Ekobrottsmyndighetens polisiära del som det kommer att bli aktuellt att överföra PNR-information. Polisdatalagen beskrivs kortfattat i avsnitt 6.4.1.

För Tullverkets del kommer från den 1 juli 2017 en ny lag om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet, tullbrottsdatalagen, att bli tillämplig för Tullverkets personuppgiftsbehandling i den brottsbekämpande verksamheten. Den ersätter den nu gällande lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. För en kortfattad beskrivning av den nya lagen, se avsnitt 6.4.2.

Som tidigare har framgått har Utredningen om 2016 års dataskyddsdirektiv lämnat förslag till en brottsdatalog med bestämmelser om skydd av personuppgifter på det brottsbekämpande området. Förslaget innehåller bestämmelser som i princip genomför samtliga bestämmelser i det nya dataskyddsdirektivet. Utredningen kommer senast den 30 september 2017 att lämna förslag till de författningsändringar som krävs för att anpassa bl.a. polisdatalagen och tullbrottsdatalagen till de nya förutsättningarna.

För Försvarsmakten gäller bl.a. lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst med anslutande förordning (SFS 2007:260). Lagen gäller för verksamheten vid den del av Försvarsmakten som kallas Must och i vilken PNR-information med personuppgifter kan komma att mottas från enheten för passagerarinformation för fortsatt behandling i verksamhet med att förebygga, upptäcka eller förhindra terroristbrottslighet eller grov brottslighet. Regleringen är en s.k. heltäckande registerlagstiftning som varken gäller utöver eller hänvisar till personuppgiftslagen. Den innehåller dock likadana eller liknande bestämmelser som personuppgiftslagen, t.ex. om förhållandet till offentlighetsprincipen och definitioner men även bestämmelser rörande information, rättelse, skadestånd, säkerhet och personuppgiftsombud. Tillsyn över personuppgiftsbehandlingen enligt lagen utövas av Datainspektionen (10 § förordningen). En utredning har nyligen getts i uppdrag att se över regleringen av behandlingen av personuppgifter inom bl.a. Försvarsmakten (dir. 2017:42). Det uppdraget ska redovisas senast den 31 maj 2018.

16.2.2 Våra generella överväganden i denna del

Som vi anfört redan i avsnitt 8.5 hade de fåtaliga bestämmelserna om hur PNR-information får behandlas hos de behöriga myndigheterna lämpligen kunnat placeras i respektive behörig myndighets registerförfattning. Det föreligger dock för närvarande en stor osäkerhet kring hur den aktuella dataskyddsregleringen kommer att se ut efter genomförandet av dataskyddsreformen. Vad gäller de brottsbekämpande myndigheternas personuppgiftsbehandling kommer den till stor del att regleras av brottsdatalagen och det är i nuläget oklart hur de myndighetsspecifika registerförfattningarna kommer

att se ut. Förslaget till brottsdatalag tyder på att dess bestämmelser inte kommer att vara direkt tillämpliga för Säkerhetspolisens verksamhet. Utredningen om 2016 års dataskyddsdirektiv har dock angett att vissa bestämmelser i brottsdatalagen kommer att vara tillämpliga på motsvarande sätt som vissa bestämmelser i personuppgiftslagen i dag (SOU 2017:29 s. 176). Vilka bestämmelser i brottsdatalagen och hur Säkerhetspolisens personuppgiftsbehandling ska regleras kommer utredningen att återkomma till i sitt slutbetänkande. Vidare omfattas inte Försvarsmaktens personuppgiftsbehandling av den dataskyddsreglering som föreslagits eller kommer att föreslås för brottsbekämpande myndigheter. Med hänsyn till dessa förhållanden föreslår vi, som framgått av avsnitt 8.5, att PNR-direktivets bestämmelser om PNR-uppgifternas behandling hos de behöriga myndigheterna, i vart fall tills vidare, förs in i den av oss föreslagna nya lagen. En fördel med denna samlade lösning är att det inte krävs ändringar i olika registerförfattningar om nya behöriga myndigheter utses eller någon faller ifrån.

Vidare föreslår vi att det i de aktuella registerförfattningarna förs in bestämmelser om att det i den av oss föreslagna lagen och i föreskrifter som har meddelats med stöd av den lagen finns bestämmelser om personuppgiftsbehandling som ska tillämpas i stället för bestämmelserna i aktuell registerförfattning (se avsnitt 8.5).

Utöver de bestämmelser som kommer att föreslås i detta avsnitt föreslår vi även att det i den nya lagen tas in bestämmelser om gallring vid de behöriga myndigheterna av sådan PNR-information som visar sig sakna betydelse för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet (se avsnitt 18.8) eller som avslöjar känsliga personuppgifter (se avsnitt 18.5). Det kan här också erinras om att vi i avsnitt 9.5 föreslagit en inledande allmän portalbestämmelse som genomför bl.a. artikel 1.2 i direktivet och som innebär en yttre ram för vilken behandling som alls är tillåten vad gäller PNR-information. Enligt den bestämmelsen, som även behöriga myndigheter är skyldiga att följa, får PNR-information inte behandlas för andra syften än att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

I övriga frågor kommer behandlingen av den PNR-information som har överförts till de behöriga myndigheterna från en enhet för passagerarinformation att styras av de dataskyddsbestämmelser som

är tillämpliga för de behöriga myndigheterna. I praktiken innebär detta brottsdatalagen, avvikande eller kompletterande bestämmelser i polisdatalagen, tullbrottsdatalagen, lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst eller de nya författningar som kan komma att genomföras på grundval av förslag från Utredningen om 2016 års dataskyddsdirektiv eller den nyss nämnda utredning som ser över behandlingen av personuppgifter inom Försvarsmakten.

För att skyddet för enskilda ska bli effektivt krävs att de myndigheter som hanterar PNR-information är medvetna om uppgifternas ursprung och att det på grund av ursprunget kan göras särskilda begränsningar för behandlingen. Det kan därför vara lämpligt att PNR-informationen förses med någon form av märkning redan i samband med att den erhålls från en enhet för passagerarinformation. En sådan märkning skulle göra det enklare för de behöriga myndigheterna att leva upp till lagens krav på hantering av informationen. Det har i tidigare lagstiftningssammanhang diskuterats huruvida det i lag eller förordning bör regleras om en märkning ska göras av varifrån vissa uppgifter härstammar. Regeringen har då funnit att frågan om hur en eventuell märkning ska utformas inte bör regleras på lag- eller förordningsnivå, eftersom en sådan reglering skulle kunna innebära en onödig begränsning i myndigheternas arbete med moderna tekniklösningar (se prop. 2012/13:73 s. 113). Vi delar den bedömningen. Frågan om märkning av den PNR-information som har överförts till de behöriga myndigheterna från en enhet för passagerarinformation bör därför lösas på myndighetsnivå, eventuellt i samarbete mellan myndigheterna.

16.2.3 Myndigheternas behandling av den överförda PNR-informationen

Vårt förslag: Om det har kommit fram uppgifter om annat brott än terroristbrottslighet eller grov brottslighet i samband med en behörig myndighets insats som görs till följd av behandling av PNR-information, får – utöver vad som anges i lagens portalbestämmelse – informationen användas för att förhindra, utreda eller lagföra brottet.

Behandling endast för direktivets syften

Av artikel 7.4 framgår att de behöriga myndigheterna endast får vidarebehandla sådan PNR-information som de har mottagit av enheten för passagerarinformation om det specifika syftet är att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet.

Artikel 7.4 utgör såvitt avser PNR-uppgifter en upprepning av den för direktivet grundläggande bestämmelsen i artikel 1.2 om att PNR-uppgifter endast får behandlas för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Enligt vårt förslag kommer en portalbestämmelse med denna innebörd att föras in i lagens inledande kapitel. Vi föreslår att den också ska omfatta resultaten av en enhet för passagerarinformations behandling av PNR-uppgifter, dvs. PNR-information. Det saknas enligt vår bedömning skäl att därutöver införa en särskild bestämmelse med detta innehåll för de behöriga myndigheterna. För det fall bestämmelserna om hur PNR-information får behandlas hos de behöriga myndigheterna skulle föras in i varje behörig myndighets registerförfattning hade dock en särskild bestämmelse som genomför artikel 7.4 varit nödvändig i respektive lag.

Behandling för att förhindra, utreda eller lagföra annan upptäckt brottslighet

Enligt artikel 7.5 ska punkten 4 inte påverka de brottsbekämpande eller rättsliga myndigheternas befogenheter på nationell nivå, om andra brott eller indikationer på sådana upptäcks i samband med brottsbekämpande insatser som görs till följd av sådan behandling av PNR-uppgifter. Om PNR-informationen leder till att en behörig myndighet genomför en brottsbekämpande insats avseende terroristbrottslighet eller grov brottslighet och det vid denna insats framkommer misstankar om sådan brottslighet som faller utanför direktivet, har myndigheterna således rätt att agera även på dessa misstankar. Bestämmelsen innebär en möjlighet att förhindra, utreda och lagföra mindre allvarlig brottslighet som upptäcks i samband med en brottsbekämpande insats gällande allvarlig brottslighet, inklusive terrorism. Vad som menas med en brottsbekämpande insats anges inte i direktivet. Enligt vår mening bör med en sådan insats avses

olika möjliga åtgärder som kan ske till följd av sådan misstänkt brottslighet som omfattas av direktivet. Man kan t.ex. tänka sig ett förhör, en husrannsakan, en brottsplatsundersökning eller ett beslag. Man kan också tänka sig en spaningsoperation. Huruvida en förundersökning har inletts bör inte vara avgörande.

En bestämmelse som genomför artikel 7.5 bör föras in i lag. Av bestämmelsen bör framgå att den utgör ett undantag från huvudregeln om att PNR-information endast får användas för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

16.2.4 Automatiserade beslut

Vårt förslag: Ett beslut som har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne, får inte enbart grundas på en automatiserad behandling av PNR-uppgifter eller på känsliga personuppgifter.

Med automatiserade beslut avses beslut som inte fattas av någon tjänsteman utan som blir den automatiska följden av t.ex. att en viss handling ges in eller inte inkommer inom viss tid (SOU 2017:29 s. 288). En bestämmelse med liknande innehåll finns i artikel 11 i det nya dataskyddsdirektivet. I brottsdatalagen har den aktuella artikeln genomförts i 2 kap. 19 §. Av den bestämmelsen framgår att om ett beslut, som har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne, enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen ha möjlighet att på begäran få beslutet omprövat av någon person. I bestämmelsen anges också att automatiserade beslut inte får enbart grundas på känsliga personuppgifter.

I artikel 7.6 i PNR-direktivet anges att de behöriga myndigheterna inte får fatta några beslut som har negativa rättsliga konsekvenser för en person eller på annat sätt allvarligt påverkar en person endast på grund av den automatiska behandlingen av PNR-uppgifter. Besluten (*such decisions* i den engelska respektive *sådanne afgørelser* i den danska versionen) får inte heller grunda sig på känsliga personuppgifter.

Bestämmelsen innebär alltså att en behörig myndighet inte får fatta några beslut som har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne enbart till följd av en automatiserad behandling av PNR-uppgifter. Ett beslut baserat på PNR-uppgifter måste således alltid föregås av en bedömning gjord av en tjänsteman vid myndigheten. Vidare får ett sådant beslut inte grundas på känsliga personuppgifter. Direktivets bestämmelse uppvisar alltså vissa likheter med förbudet mot automatiserade beslut i brottsdatalagen.

Vi föreslår att det tas in en bestämmelse i den nya lagen om automatiserade beslut som genomför artikel 7.6 i PNR-direktivet. Liksom på övriga ställen i vår lag där känsliga personuppgifter är aktuella bör det i vår bestämmelse föras in en hänvisning till den bestämmelse i brottsdatalagen där de känsliga personuppgifterna i här aktuellt hänseende definieras.

För de brottsbekämpande myndigheter som i sin verksamhet tillämpar brottsdatalagen, kommer 2 kap. 19 § BDL att gälla utöver den av oss föreslagna bestämmelsen om automatiserade beslut. En viss dubbelreglering kommer därmed att uppstå avseende automatiserade beslut baserade på känsliga personuppgifter. Det sagda gäller dock bara för sådana behöriga myndigheter som annars har att tillämpa 2 kap. 19 § BDL, inte t.ex. Försvarsmakten.

Enligt vår bedömning torde bestämmelsen inte komma att få någon praktisk betydelse för de behöriga myndigheternas behandling av PNR-information. Denna information kommer alltid att granskas individuellt av någon tjänsteman innan den används på ett sådant sätt att den leder till ett beslut som påverkar den person som PNR-uppgifterna avser. Vidare får PNR-uppgifter som avslöjar känsliga personuppgifter över huvud taget inte behandlas av enheten för passagerarinformation eller de behöriga myndigheterna. Sådana uppgifter kommer därför inte att ligga till grund för några beslut.

17 Överföring till tredjeland

17.1 Direktivets bestämmelser

Överföringar från enheten för passagerarinformation till tredjeland behandlas i artikel 11 i PNR-direktivet. Av bestämmelsen framgår att det är tillåtet för en medlemsstat att överföra sådan PNR-information som lagras av enheten för passagerarinformation till ett tredjeland (artikel 11.1). En överföring får dock endast ske efter en bedömning i det enskilda fallet och under förutsättning att

1. de villkor som fastställs i artikel 13 i dataskyddsrambeslutet är uppfyllda,
2. överföringen är nödvändig för direktivets syften enligt artikel 1.2, dvs. för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet,
3. det berörda tredjelandet godtar att överföra uppgifterna till ett annat tredjeland endast om det är strikt nödvändigt för direktivets ändamål enligt artikel 1.2 och endast efter uttryckligt samtycke av medlemsstaten, och
4. samma villkor för överföring till en annan medlemsstat som anges i artikel 9.2 är uppfyllda.

I artikel 11.2 behandlas överföringar av sådan PNR-information som enheten för passagerarinformation har mottagit från en annan medlemsstats motsvarande enhet. Överföring av personuppgifter som en svensk myndighet har fått från en annan medlemsstat kräver normalt samtycke från den medlemsstat från vilken uppgifterna har hämtats. I artikel 13.2 i dataskyddsrambeslutet finns det intaget ett undantag från denna huvudregel. Även i PNR-direktivet finns ett sådant undantag, som enligt bestämmelsen ska gälla i stället för motsvarande bestämmelse i dataskyddsrambeslutet. Således anges i arti-

kel 11.2 att överföring av PNR-uppgifter utan förhandssamtycke från den medlemsstat från vilken uppgifterna hämtades får ske i undantagsfall och endast om överföringen är absolut nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet samt förhandssamtycke inte kan erhållas i tid. Den myndighet som ansvarar för att ge samtycke i den ursprungliga medlemsstaten ska informeras utan dröjsmål och överföringen ska vederbörligen registreras samt genomgå efterhandskontroll.

Enligt artikel 11.3 ska medlemsstaterna överföra PNR-uppgifter till behöriga myndigheter i tredjeländer på villkor som är förenliga med direktivet endast efter att ha förvissat sig om att mottagarnas planerade användning av uppgifterna är förenlig med dessa villkor och skyddsåtgärder. Dataskyddsombudet vid enheten för passagerarinformation i den medlemsstat som har överfört PNR-uppgifterna ska enligt artikel 11.4 informeras om varje överföring.

17.2 Bakgrund

17.2.1 Dataskyddsrambeslutet och 2013 års lag

I dataskyddsrambeslutet anges gemensamma regler för behandling av personuppgifter inom ramen för polisiärt och straffrättsligt samarbete när personuppgifter överförs eller görs tillgängliga mellan EU-medlemsstater, Island, Liechtenstein, Norge och Schweiz och EU-organ och EU:s informationssystem. Dataskyddsrambeslutet innehåller även bestämmelser om dataskydd vid överföringar till tredjeland. I rambeslutets artikel 13 finns således regler om överföring av personuppgifter från en medlemsstat till ett tredjeland i de fall där uppgifterna har överförts från eller gjorts tillgängliga för medlemsstaten av en behörig myndighet i en annan medlemsstat.

I artikel 13.1 anges vissa förutsättningar för att personuppgifter ska få överföras. En sådan överföring får göras bara om den stat från vilken uppgifterna har erhållits har gett samtycke till överföringen, överföringen är nödvändig för att förebygga, utreda, upptäcka eller lagföra brott eller för verkställighet av en straffrättslig påföljd och om mottagaren har ansvar för sådan verksamhet, samt det finns en adekvat skyddsnivå för databehandling i den stat i vilken mottagande myndighet eller mottagande internationellt organ finns. För att det

ska vara tillåtet att föra över uppgifter eller göra dessa tillgängliga måste samtliga dessa villkor som huvudregel vara uppfyllda.

Enligt artikel 13.2 finns dock möjlighet att överföra personuppgifter i förväg. Enligt artikeln krävs då att överföringen är absolut nödvändig, antingen för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller en tredjestat eller för att tillgodose en medlemsstats väsentliga intressen samt att ett förhandsmedgivande inte hinner utverkas i tid. Om överföringen sker utan medgivande ska enligt artikel 13.2 sista meningen den myndighet, vars medgivande till överföring krävs, underrättas utan dröjsmål.

Artikel 13.3 innehåller en möjlighet att överföra personuppgifter trots att kravet på adekvat skyddsnivå inte är uppfyllt. I artikel 13.4 anges vilka faktorer som ska beaktas vid bedömningen av om mottagaren har en adekvat skyddsnivå.

Artikel 13 i dataskyddsrambeslutet har i svensk rätt genomförts i lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag) och i en tillhörande förordning (2013:343) med i övrigt samma namn. 2013 års lag gör det således möjligt för en svensk myndighet att föra över personuppgifter till ett tredjeland. Den tillämpas dock bara på personuppgifter som en svensk myndighet har fått från en annan stat som är medlem i EU, Island, Liechtenstein, Norge eller Schweiz, ett EU-organ eller ett EU-informationssystem. I lagens 7 § anges att personuppgifter får överföras till ett tredjeland om den som har överfört eller gjort uppgifterna tillgängliga för den svenska myndigheten har medgett att de överförs, överföringen är nödvändig för något av de ändamål som omfattas av lagens tillämpningsområde och mottagaren har ansvar för ett sådant ändamål. Därtill ska staten där den mottagande myndigheten eller organet finns ha en adekvat skyddsnivå för den avsedda behandlingen. Undantag från kravet på adekvat skyddsnivå görs i vissa enskilda fall som framgår av paragrafen. På samma sätt föreskrivs undantag från kravet på medgivande i förväg.

Artikel 13 i dataskyddsrambeslutet och 2013 års lag är som angetts enbart tillämplig vid överföring av personuppgifter som härrör från andra medlemsstater eller från vissa andra stater, organ och informationssystem. Personuppgiftslagen blir därför tillämplig för andra överföringar, bl.a. genom hänvisningar dit i myndigheters

registerförfattningar. Vad gäller bestämmelserna i personuppgiftslagen hänvisas till redogörelsen i avsnitt 6.3.2.

17.2.2 Brottsdatalagen

Dataskyddsrambeslutet upphör att gälla den 6 maj 2018, då det kommer att ersättas av det nya dataskyddsdirektivet. Av PNR-direktivets skäl 27 framgår att hänvisningar till dataskyddsrambeslutet bör ses som hänvisningar till såväl nuvarande lagstiftning som de framtida bestämmelser som kommer att ersätta denna. Eftersom det nya dataskyddsdirektivet ska genomföras i nationell rätt ungefärligen samtidigt som PNR-direktivet, får hänvisningarna till dataskyddsrambeslutet läsas som hänvisningar till det nya dataskyddsdirektivet. Som tidigare framgått föreslås det nya dataskyddsdirektivet genomföras i svensk rätt genom brottsdatalagen.

Bestämmelserna om överföring till tredjeland har tagits in i 8 kap. brottsdatalagen. I 8 kap. 1 och 2 §§ anges de grundläggande förutsättningarna för en sådan överföring. Enligt 1 § får en behörig myndighet överföra personuppgifter som behandlas till ett tredjeland eller en internationell organisation. Det gäller även överföring av personuppgifter för behandling i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet, och
3. omfattas av
 - a) ett beslut om adekvat skyddsnivå enligt 3 §, eller
 - b) tillräckliga skyddsåtgärder enligt 4 §, eller
 - c) ett undantag för särskilda situationer enligt 5 §.

Enligt andra stycket ska en behörig myndighet som avser att överföra personuppgifter till ett tredjeland särskilt beakta risken för att enskilda får försämrat skydd för sina personuppgifter.

Personuppgifter som en svensk myndighet har fått från en annan medlemsstat får, enligt 8 kap. 2 §, överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs. Om medgivande på grund av tidsbrist inte kan inhämtas i förväg, får, enligt andra stycket, personuppgifter ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för andra väsentliga intressen för Sverige eller annan medlemsstat.

I 8 kap. 3 § anges att om kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit.

Om det inte finns ett beslut om adekvat skyddsnivå får, enligt 8 kap.4 §, personuppgifter ändå överföras om

1. skyddsåtgärder för personuppgifter har fastställts i ett avtal som ger tillräckliga garantier till skydd för registrerades rättigheter, eller
2. den behöriga myndighet som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

Enligt 8 kap. 5 § kan överföring vara tillåten i vissa särskilda situationer även om det inte finns ett beslut om adekvat skyddsnivå enligt 3 § eller tillräckliga skyddsåtgärder enligt 4 §. I sådant fall får en överföring, eller en samling av överföringar, göras endast om överföringen är nödvändig för att

1. skydda den registrerades eller en annan fysisk persons vitala intressen, eller andra berättigade intressen för den registrerade,
2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller
4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får, enligt andra stycket, inte överföras om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

I 8 kap. 6 och 7 §§ finns bestämmelser om vidareöverföring till ett annat tredjeland eller internationell organisation. Enligt 6 § får en svensk myndighet inte tillåta att sådana personuppgifter som en myndighet har fått från en annan medlemsstat, och som överförts till ett tredjeland, vidareöverförs till ett annat tredjeland eller en internationell organisation, om inte den behöriga myndigheten i den medlemsstat som ursprungligen lämnade uppgiften, har medgett att uppgifterna får vidareöverföras. I 7 § anges vad en behörig myndighet ska beakta när den ska ta ställning till om personuppgifter som behandlats i Sverige får vidareöverföras.

I 8 kap. 8 § finns en möjlighet att i vissa fall överföra personuppgifter till andra än behöriga myndigheter. Enligt 9 § ska svenska myndigheter följa uppställda villkor för att använda personuppgifter som har överförts från ett tredjeland. I 10 § anges att en svensk behörig myndighet får, vid överföring av personuppgifter till tredjeland, ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt.

Enligt 7 kap. 1 § BDF ska den som har överfört personuppgifter till ett tredjeland utan förhandsmedgivande enligt 8 kap. 2 § andra stycket BDL, utan dröjsmål informera den medlemsstat som lämnat uppgifterna till en svensk myndighet om överföringen.

17.3 Våra överväganden och förslag

17.3.1 Grundläggande begrepp

Vårt förslag: Tredjeland ska i lagen definieras som en stat som inte är en medlemsstat.

PNR-direktivet innehåller inte någon definition av tredjeland. Med tredjeland avses i EU-sammanhang vanligtvis ett land som inte är medlem i unionen och som därmed står utanför medlemsstaternas samarbete. Alla EU-medlemsstater är dock inte bundna av PNR-

direktivet. Som tidigare har angetts ska direktivet inte tillämpas av Danmark. Överföringar av PNR-uppgifter till Danmark får därmed uppfattas som överföringar till ett tredjeland. Med hänsyn härtill blir en definition av begreppet tredjeland nödvändig i vår lag. Utgångspunkten för en sådan definition bör enligt utredningen vara hur medlemsstat definieras. Som framgått av avsnitt 15.3.1 avses med medlemsstat i lagförslaget en stat som är medlem i EU, med undantag för Danmark. Stater som inte är medlemsstater enligt direktivet ska betraktas som tredjeländer. Definitionen av tredjeland bör därför vara en stat som inte är en medlemsstat enligt lagens definition av en sådan.

17.3.2 Förutsättningar för överföring till tredjeland

Vårt förslag: Enheten för passagerarinformation får överföra PNR-information till en myndighet i ett tredjeland som där är behörig att bedriva verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra sådan brottslighet som motsvarar terroristbrottslighet eller grov brottslighet. Uppgifterna får dock endast överföras om

1. de grundläggande förutsättningarna för överföring av personuppgifter enligt 8 kap. 1 § första stycket 3 och 2 § första stycket BDL är uppfyllda och under i övrigt samma förutsättningar som överföringar får ske mellan medlemsstaterna,
2. överföringen är nödvändig för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet, och
3. det tredjelandet godtar att vidareöverföra uppgifterna till ett annat tredjeland endast om det är absolut nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet och enheten för passagerarinformation har lämnat ett uttryckligt medgivande till överföringen.

PNR-information får överföras till vissa myndigheter i tredjeland

PNR-direktivets bestämmelser om överföring till tredjeland bör i huvudsak genomföras i den av oss föreslagna lagen. Vissa detaljbestämmelser kan dock tas in i den anslutande förordningen.

Det bör av lagen framgå att enheten för passagerarinformation får överföra PNR-information till ett tredjeland. Det är således enligt direktivet inte möjligt att, såsom får ske enligt brottsdatalagen, överföra PNR-information även till internationella organisationer.

Enligt PNR-direktivet får överföringar endast ske till en behörig myndighet i tredjeland (artikel 11.3). Även i brottsdatalagen anges att överföringar får ske till en behörig myndighet i tredjeland. En behörig myndighet definieras i brottsdatalagen som en myndighet eller en annan aktör som har i uppdrag att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet (1 kap. 6 §). Enligt vår mening bör med behörig myndighet i PNR-direktivet dock avses en myndighet som i det tredjelandet är behörig att bedriva verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra brott motsvarande terroristbrottslighet eller grov brottslighet. Det bör av lagen framgå att överföringar endast får ske till en sådan myndighet i tredjeland. Så kan ske genom en hänvisning till lagens portalbestämmelse där dessa syften anges.

Det bör vidare av lagen framgå att en överföring endast får ske om vissa särskilt uppräknade villkor är uppfyllda. En bestämmelse om överföring bör utformas så att det framgår att samtliga villkor ska vara uppfyllda för att enheten ska få överföra PNR-information till ett tredjeland. Vilka dessa villkor bör vara diskuteras i det följande.

Grundläggande bestämmelser om överföring av personuppgifter till tredjeland ska vara uppfyllda

PNR-direktivet innehåller inte några grundläggande bestämmelser med allmänna principer för överföring av personuppgifter till tredjeland. T.ex. saknas i direktivet bestämmelser om krav på adekvat skyddsnivå för personuppgifterna i det tredjelandet. I stället anges att villkoren i artikel 13 i dataskyddsrambeslutet ska vara uppfyllda vid överföringar av PNR-information till tredjeland. Som tidigare

har angetts upphävs dataskyddsrambeslutet i samband med genomförandet av det nya dataskyddsdirektivet. PNR-direktivets hänvisningar till dataskyddsrambeslutet får därför läsas som hänvisningar till det nya dataskyddsdirektivet.

Artikel 13 i dataskyddsrambeslutet innehåller rambeslutets samtliga bestämmelser om överföring till tredjeland. Den allmänna hänvisningen till rambeslutets samtliga bestämmelser i frågan får därför tolkas som en hänvisning även till samtliga bestämmelser om överföring till tredjeland i det nya dataskyddsdirektivet. I något fall innehåller det direktivet dock bestämmelser som inte kan tillämpas vid överföringar till tredjeländer från enheten för passagerarinformation, eftersom PNR-direktivet innehåller andra regler. Dessa bestämmelser kommer vi att återkomma till nedan.

Som tidigare har angetts föreslås det nya dataskyddsdirektivets samtliga bestämmelser om överföring till tredjeland genomföras i brottsdatalagen med tillhörande förordning. Brottsdatalagen innehåller således de grundläggande bestämmelserna med allmänna principer för överföring av personuppgifter till tredjeland inom det brottsbekämpande området. Enligt vår mening är det viktigt att dessa grundläggande bestämmelser tillämpas även vid överföring av PNR-information för att den skyddsnivå som säkerställs genom det direktivet inte ska undergrävas. Dessa bestämmelser i brottsdatalagen bör därmed vara tillämpliga även vid överföring av PNR-information.

De grundläggande förutsättningarna för att överföringar alls ska få ske till tredjeländer framgår för det första av 8 kap. 1 § första stycket 3 BDL. Bestämmelsen hänvisar till 3, 4 och 5 §§, som anger förutsättningarna för att en överföring ska omfattas av beslut om adekvat skyddsnivå, av tillräckliga skyddsåtgärder eller vara föremål för ett undantag för särskilda situationer. Dessa bestämmelser bör således tillämpas även vid överföringar av PNR-information från enheten för passagerarinformation. Det kan dock sägas att 8 kap. 5 § inte torde kunna ha något tillämpningsutrymme i praktiken med tanke på det snäva användningsområdet och detaljregleringen av hur PNR-uppgifter får användas enligt vårt förslag till lagstiftning.

Vidare finns i 8 kap. 2 § första stycket intaget den huvudregel som anger att personuppgifter som har erhållits från en annan medlemsstat endast får överföras om den medlemsstat som har lämnat uppgifterna har medgett att de överförs. Även denna huvudregel bör gälla vid överföring av PNR-uppgifter.

Förutsättningarna för överföring till en annan medlemsstat ska vara uppfyllda

Enligt artikel 11.1 d ska de villkor som fastställs i artikel 9.2 vara uppfyllda även vid en överföring av PNR-information till tredjeland. Av artikel 9.2, som har behandlats i avsnitt 15.3.2, framgår vad som ska iakttas vid överföring av PNR-information till en annan medlemsstat på särskild förfrågan. Således ska samma villkor som gäller vid överföring av PNR-information till en annan medlemsstat på särskild begäran vara uppfyllda även när sådan information överförs till ett tredjeland.

Bestämmelsen i artikel 11.1 d bör genomföras i lagen genom en hänvisning till de paragrafer som genomför artikel 9.2. Det innebär att för det fall överföringen avser PNR-uppgifter som är äldre än sex månader och därmed maskerade, får fullständiga, avmaskerade, PNR-uppgifter endast överföras om även de bestämmelser som genomför artikel 12.3 är uppfyllda, se vidare i avsnitt 15.5.

Överföringen ska vara nödvändig för direktivets syften

Av artikel 11.1 b framgår att en överföring av PNR-information till tredjeland endast får ske om den är nödvändig för direktivets syften enligt artikel 1.2. Således krävs enligt PNR-direktivet att en överföring till tredjeland är nödvändig för just de syften som anges i direktivet, dvs. för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. I brottsdatalagen anges i stället att överföringar endast får ske om de ändamål som anges i dataskyddsdirektivet, och som är mer allmängiltiga, är uppfyllda (8 kap. 1 § 1). PNR-direktivets syften innefattas i de syften som anges i brottsdatalagen. Det behöver därför inte i den lag som vi föreslår införas någon bestämmelse som anger att 8 kap. 1 § 1 inte ska vara tillämplig. Dock krävs det i lagen en bestämmelse som anger att en överföring till tredjeland endast får ske om syftena i PNR-direktivet är uppfyllda. Den bestämmelsen är en sådan avvikande bestämmelse i annan författning som enligt 1 kap. 5 § BDL gäller före brottsdatalagen.

Bestämmelsen bör föras in i lagen genom en hänvisning till ett eller flera av de syften som anges i den portalbestämmelsen i lagen som genomför artikel 1.2 i direktivet och som innebär att uppgift-

erna endast får behandlas för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Visserligen hade bestämmelsen blivit tydligare om dessa syften skrevs ut i bestämmelsen. Dessa syften återkommer emellertid så pass frekvent i lagen, sedd som helhet, att hänvisningar i allmänhet bör väljas för att lagtexten inte i ska bli onödigt ordrik. Med terroristbrottslighet och grov brottslighet bör i sammanhanget avses motsvarande brottslighet i det tredjelandet.

Direktivets krav på att överföringen ska vara nödvändig bör också föras in i lagen. Enligt vår mening bör nödvändigheten tolkas på samma sätt som i allmänt språkbruk, dvs. att det är fråga om något som behövs. De PNR-uppgifter som överförs ska således behövas av ett tredjeland i dess bekämpning av aktuell brottslighet.

Villkor för vidareöverföring från det tredjelandet

Artikel 11.1 c behandlar frågan om vidareöverföring från ett tredjeland till ett annat tredjeland av sådan PNR-information som härstammar från den svenska enheten för passagerarinformation. Enligt bestämmelsen ska det tredjeland som vill motta PNR-information godta att de överförda uppgifterna endast får föras vidare till ett annat tredjeland om det är strikt nödvändigt för detta direktivs ändamål och efter uttryckligt samtycke av medlemsstaten.

I brottsdatalagen anges endast att en svensk behörig myndighet får ställa upp villkor som begränsar möjligheten att använda de överförda uppgifterna, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt (8 kap. 10 §). Bestämmelsen i direktivet bör därför genomföras i vår lag. På samma sätt som angetts ovan föreslår vi att det i bestämmelsen ska framgå de syften för vilka en överföring ska vara nödvändig. Så bör, på samma sätt som angetts ovan, ske genom en hänvisning till ett eller flera av de syften som anges i lagens portalbestämmelse.

Enligt direktivet får en vidareöverföring endast ske om det är strikt nödvändigt (i den engelska versionen *strictly necessary*, i den danska *strengt nødvendigt*). I svensk lag brukar begreppet absolut nödvändigt användas för att markera ett undantagsfall som ska tillämpas restriktivt. Vi föreslår därför att det i lagen anges att det tredjelandet

ska godta att överföra uppgifterna till ett annat tredjeland endast om det är absolut nödvändigt för direktivets ändamål.

Vidare får en vidareöverföring enligt direktivet endast ske efter uttryckligt samtycke av medlemsstaten. I 2013 års lag och i brottsdatalogen används ordet medgivande i stället för samtycke. För att bättre korrespondera med denna lagstiftning föreslår vi att ordet medgivande används även i vår lag. Medgivandet bör lämpligen lämnas av enheten för passagerarinformation.

Medgivandet ska enligt direktivet vara uttryckligt. Det framgår dock inte närmare hur ett sådant medgivande ska manifesteras. Man skulle kunna tänka sig att ett uttryckligt medgivande sker såväl muntligt som skriftligt och vi ser inga principiella eller praktiska problem med en sådan ordning. Vi föreslår därför att endast ett krav på uttrycklighet införs i lagen. Det säger sig dock självt att oavsett på vilket sätt ett samtycke getts, måste det dokumenteras på något sätt.

17.3.3 Överföring utan medgivande

Våra förslag: Om medgivande till överföring av PNR-information på grund av tidsbrist inte kan inhämtas i förväg från den medlemsstat som har lämnat informationen till enheten för passagerarinformation får, i stället för vad som anges i 8 kap. 2 § andra stycket BDL, informationen ändå överföras om det är absolut nödvändigt för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet.

I förordning ska regleras att om PNR-information, som kommer från en annan medlemsstat, har överförts till ett tredjeland utan förhandsmedgivande, ska enheten för passagerarinformation utan dröjsmål informera den andra medlemsstaten om överföringen. Det ska i förordning också regleras att överföringar utan förhandsmedgivande ska genomgå efterhandskontroll av dataskyddsombudet vid enheten för passagerarinformation.

Som tidigare har angetts får, enligt 8 kap. 2 § första stycket BDL, personuppgifter som en svensk myndighet har fått från en annan medlemsstat överföras till ett tredjeland endast om den medlemsstat som lämnat personuppgifterna i förväg har medgett att de överförs till tredjelandet. Bestämmelsen ska enligt vårt förslag

tillämpas även vid överföring av PNR-uppgifter. I bestämmelsens andra stycke finns intaget ett undantag från denna huvudregel. Även i artikel 11.2 i PNR-direktivet finns ett undantag från kravet på förhandsmedgivande, som är snävare än det undantag som föreslås i brottsdatalagen. För att en överföring av PNR-information ska få ske krävs enligt bestämmelsen att överföringen är absolut nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet i en medlemsstat eller tredjeland och att ett förhandssamtycke inte kan erhållas i tid. En bestämmelse bör därför föras in i vår lag som ska gälla i stället för undantaget i 8 kap. 2 § andra stycket BDL.

För förutsebarhetens skull bör bestämmelsen i vår lag genomföras på liknande sätt som den angivna bestämmelsen i brottsdatalagen. Ordet medgivande bör därför, som angetts ovan, användas i stället för samtycke. I brottsdatalagen och i 2013 års lag används också ordet fara i stället för hot. Med hänsyn härtill och eftersom svensk lagstiftning brukar utformas på det sättet, föreslår vi att ordet fara används i stället för hot även vid genomförandet av PNR-direktivet. Av samma anledning bör det i de andra lagarna använda ordet avvärja användas också i vår lag i stället för begreppet reagera på, som används i direktivet. Således bör det i lagen anges att en överföring utan förhandsmedgivande får ske om det är absolut nödvändigt för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet. Med uttrycket absolut nödvändigt markeras att undantaget ska tillämpas restriktivt och att det kan bli fråga om överföring utan förhandssamtycke endast i undantagsfall. Tillägget att det ska gälla brott i en medlemsstat eller tredjeland innebär att tillämpningsområdet omfattar alla stater och saknar därför egentligt innehåll. Tillägget bör således inte föras in i vår lag.

Bestämmelsen skulle exempelvis kunna användas om överföringen är nödvändig för att avvärja ett terroristattentat i en medlemsstat eller tredjeland. Eftersom det typiskt sett är fråga om en överhängande fara för att något ska hända får prövningen i dessa fall göras utifrån att åtgärden kan antas vara nödvändig för att avvärja faran. Att faran inte förverkligas behöver inte innebära att överföringen har varit otillåten. Bedömningen måste göras med hänsyn till vad som är känt när prövningen görs.

Enligt andra stycket i artikel 11.2 ska den myndighet som ansvarar för att ge samtycke informeras om överföringen utan dröjsmål. En liknande bestämmelse finns i dag i 1 § i 2013 års förordning och föreslås införas i 7 kap. 1 § BDF. Vi föreslår att en liknande bestämmelse förs in i den till vår lag hörande förordningen. I bestämmelsen bör anges att om PNR-information, som kommer från en annan medlemsstat, har överförts till ett tredjeland utan förhandsmedgivande, ska enheten för passagerarinformation utan dröjsmål informera den andra medlemsstaten om överföringen.

Vidare ska enligt artikel 11.2 överföringar utan samtycke registreras och genomgå efterhandskontroll. Att överföringar till tredje länder ska registreras anges även i artikel 13.5 c. Vi kommer därför att behandla frågan i samband med våra förslag till genomförande av den artikeln (se avsnitt 19.3). Hur en efterhandskontroll ska gå till eller av vem anges inte i direktivet. Enligt vår bedömning bör denna kontroll utföras av dataskyddsombudet vid enheten för passagerarinformation (se vidare om dataskyddsombudets uppgifter i avsnitt 19.5). Även denna fråga kan regleras i förordning.

17.3.4 Säkerställande av direktivets bestämmelser

Våra förslag: Det ska vara obligatoriskt för enheten för passagerarinformation att uppställa villkor om användningsbegränsning för den som ska ta emot PNR-information. Begränsningarna ska syfta till att skydda PNR-informationen från användning i strid med PNR-direktivet. Frågan kan regleras i förordning. Där kan även regleras att dataskyddsombudet vid enheten för passagerarinformation ska informeras om varje överföring av PNR-uppgifter till tredjeland.

När enheten för passagerarinformation överför PNR-information till ett tredjeland ska vad som anges i 8 kap. 8 § BDL inte gälla.

Enligt artikel 11.3 ska medlemsstaterna överföra PNR-uppgifter till behöriga myndigheter i tredjeländer på villkor som är förenliga med direktivet endast efter att ha förvässat sig om att mottagarnas planerade användning av uppgifterna är förenlig med dessa villkor och skyddsåtgärder. Bestämmelsen innebär i huvudsak att medlemsstaterna ska säkerställa att direktivets bestämmelser om överföring

till tredjeländer sker i enlighet med direktivets bestämmelser och att den överförda informationen är planerad att användas i överensstämmelse med direktivets syften och begränsningar. Vid en överföring till ett tredjeland fordras således att enheten för passagerarinformation försäkras sig om att den planerade användningen av informationen inte kommer att strida mot lagens grundläggande bestämmelser, framför allt att informationen bara används för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

I brottsdatalagen föreslås en bestämmelse, 8 kap. 10 §, som anger att en svensk behörig myndighet får ställa upp villkor som begränsar mottagarens möjlighet att använda överförda uppgifter. Det är dock inte obligatoriskt för en myndighet att ställa upp villkor. I 9 § 2013 års lag, som bl.a. genomför artikel 12 i dataskyddsrambeslutet, föreskrivs att om en svensk myndighet överför personuppgifter, ska myndigheten underrätta mottagaren om de särskilda villkor som gäller för användningen av uppgifterna. Det finns även i andra lagar bestämmelser som anger att svenska myndigheter under vissa förutsättningar får ställa upp villkor som begränsar möjligheten att använda uppgifter som lämnas till en annan stat, se t.ex. 3 a § lagen (2000:343) om internationellt polisiärt samarbete eller 5 kap. 2 § lagen (2000:562) om internationell rättslig hjälp i brottmål.

Enligt vår mening bör det, för ett korrekt genomförande av artikel 11.3 i PNR-direktivet, vara obligatoriskt för enheten att ställa upp villkor om användningsbegränsningar. Vi föreslår därför en bestämmelse som anger att enheten för passagerarinformation, i samband med en överföring av PNR-information till ett tredjeland, ska ställa upp sådana villkor om användningsbegränsningar som avses i 8 kap. 10 § BDL. Det ska vidare anges att sådana villkor ska syfta till att skydda informationen från användning i strid med PNR-direktivet. Sådana villkor kan exempelvis avse för vilket eller vilka specifika syften den överförda informationen får behandlas av den som tar emot den, att spridningen inom den mottagande myndigheten eller mottagarlandet ska begränsas eller om, och i så fall under vilka förutsättningar, den får vidareöverföras. Bestämmelsen bör kunna regleras i förordning. Det ligger i sakens natur att det inte går att i övrigt i svensk rätt föreskriva hur uppgifterna ska behandlas i det tredjelandet. Det får beaktas av enheten vid bedömningen av om PNR-information alls ska överföras till det tredjelandet.

I 8 kap. 8 § BDL anges en möjlighet att i enskilda fall överföra personuppgifter till andra organ än behöriga myndigheter eller internationella organisationer. Som tidigare har angetts får PNR-information enligt direktivet endast överföras till tredjeland och inte till någon internationell organisation. Inte heller ger direktivet någon möjlighet att överföra personuppgifter till andra organ. Bestämmelsen i 8 kap. 8 § BDL, som inte motsvaras av någon bestämmelse i dataskyddsrambeslutet, kan därför inte vara tillämplig vid överföring av PNR-information. Detta bör framgå av vår lag.

Övriga, inte här särskilt angivna bestämmelser om överföring till tredjeland i brottsdatalagen kommer att bli generellt tillämpliga vid enheten för passagerarinformations överföring av PNR-uppgifter. Detta behöver inte särskilt anges i vår lag.

Enligt artikel 11.4 i PNR-direktivet ska dataskyddsombudet vid enheten för passagerarinformation informeras om varje överföring enligt artikeln. Frågan kan regleras i förordning.

18 Lagringstid och gallring

18.1 Inledning

I detta avsnitt behandlar vi PNR-direktivets bestämmelser som har betydelse för bevarande och gallring av PNR-information. I artikel 6.1 finns en inledande bestämmelse som ska säkerställa att endast sådana PNR-uppgifter som omfattas av direktivet får behandlas vid enheten för passagerarinformation. För det fall enheten tar emot andra PNR-uppgifter ska de omedelbart raderas. Enligt artikel 13.4 ska enheten för passagerarinformation även radera sådana PNR-uppgifter som avslöjar känsliga personuppgifter. I artikel 12 finns vidare bestämmelser om hur länge PNR-uppgifterna ska och får lagras i databasen hos enheten för passagerarinformation. Avsnittet inleds dock med en beskrivning av relevant reglering på området såsom en rättslig bakgrund till våra överväganden.

18.2 Rättslig bakgrund

När stora mängder personuppgifter samlas hos myndigheter uppstår onekligen integritetsrisker, i synnerhet då informationsteknikens utveckling inneburit ständigt förbättrade möjligheter att söka och sammanställa uppgifter. Frågor om hur länge personuppgifter ska få behandlas i datoriserade myndighetsregister har därför, alltsedan datoriseringen inleddes, varit en central fråga i all dataskyddsreglering. Efter hand som myndigheter övergått till att behandla i princip all verksamhetsinformation med hjälp av elektronisk informationsteknik har frågeställningarna blivit alltmer komplexa. Mot den dataskyddsrättsliga principen står nämligen de intressen som bär upp offentlighetsprincipen i form av handlingsoffentligheten, dvs. var och ens rätt att ta del av allmänna handlingar, se 2 kap. 1 § TF. Av bestämmelsen framgår att syftet härmed är att främja ett fritt menings-

utbyte och en allsidig upplysning. Myndigheter kan också från verksamhetssynpunkt ha legitima intressen av att lagra information en längre tid. Även för den enskilde registrerade kan ett långsiktigt bevarande av information om honom eller henne vara mycket viktigt i vissa fall.

För att handlingsöfentligheten och andra bevarandebestånden ska kunna få genomslag i praktiken förutsätts att allmänna handlingar bevaras och hålls ordnade. I den svenska dataskyddsregleringen på myndighetsområdet har därför genomgående gjorts avvägningar mellan dessa ofta motstående intressen.

18.2.1 Gällande rätt

Begreppet allmän handling

Med begreppet allmänna handlingar förstås inte bara traditionella handlingar. Även upptagningar som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel, t.ex. datorlagrad information, är enligt 2 kap. 3 § TF att se som handlingar. Det är informationsinnehållet, dvs. de lagrade uppgifterna, som konstituerar handlingen (se SOU 2012:90 s. 60 f.). En sådan upptagning är en allmän handling om den förvaras hos myndigheten samt är inkommen eller upprättad där.

I fråga om upptagningar anses en sådan som en förvarad handling hos myndigheten om den är tillgänglig för den med sådana tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (2 kap. 3 § andra stycket TF). En hos myndigheten förvarad handling blir alltså allmän om den är att betrakta som inkommen till myndigheten. I fråga om upptagningar gäller att en sådan anses som inkommen till en myndighet i samma ögonblick som den är att anse som förvarad hos myndigheten på sätt som anges i 2 kap. 3 § andra stycket TF. Detta gäller under förutsättning att det är någon utanför myndigheten, dvs. en annan myndighet eller en enskild som har vidtagit den åtgärd som gjort handlingen tillgänglig för myndigheten (2 kap. 6 § första stycket andra meningen TF). Vad gäller en förvarad upptagning som myndigheten själv framställt i sin verksamhet blir den att betrakta som allmän handling när den enligt en relativt komplicerad reglering i 2 kap. 7 § TF är att anse som upp-

rättad hos myndigheten. Huvudregeln är att en handling anses upp-
rättad och därmed allmän när den har expedierats, dvs. lämnats till
annan myndighet eller enskild, eller annars föreligger i slutligt skick.

Arkivlagstiftningen

Handlingsoffentligheten förutsätter som ovan nämnts att allmänna
handlingar hålls ordnade och bevaras. Myndigheterna har därför
grundläggande skyldigheter att bevara och vårda sina allmänna hand-
lingar i arkiv. Bestämmelser om bevarande och gallring av allmänna
handlingar hos bl.a. de statliga myndigheterna finns i arkivlagen
(1990:782). Lagen är en ramlag som innehåller allmänna och över-
gripande bestämmelser om myndigheternas arkiv. Lagen fylls ut av
arkivförordningen (1991:446) samt de myndighetsspecifika beslut
eller generella föreskrifter som arkivmyndigheterna utfärdar. Riks-
arkivet är statlig arkivmyndighet.

Huvudprincipen enligt arkivlagen är att allmänna handlingar –
konventionella handlingar likväl som upptagningar – ska bevaras i
myndigheternas arkiv. Gallring av allmänna handlingar får dock ske,
vilket anges i lagens 10 §. Vid gallring ska alltid beaktas att arkiven
utgör en del av kulturarvet och att det arkivmaterial som återstår ska
kunna tillgodose rätten att ta del av allmänna handlingar, behovet av
information för rättskipningen och förvaltningen samt forskningens
behov. Arkivlagens bestämmelser om gallring syftar således primärt
inte till att tillgodose integritetsskyddsintressen.

I 10 § tredje stycket arkivlagen anges att avvikande bestämmelser
om gallring av vissa allmänna handlingar i annan lag eller förordning
har företräde framför arkivlagens gallringsregler. Avvikande bestäm-
melser om bevarande och gallring finns i de flesta registerförfatt-
ningar. Bestämmelserna kan syfta till att skydda den personliga inte-
griteten hos de som uppgifterna rör. Det kan dock finnas bestäm-
melser om gallring, eller som i vart fall i praktiken får till följd att
gallring sker, som tillkommit av andra skäl än integritetsskäl. Även
sådana bestämmelser går före arkivlagens regler enligt detta stycke.

Med gallring av elektronisk information avses normalt att viss
information raderas från databäraren. Gallring kan dock även inne-
bära en partiell gallring där information tas bort från ett register eller
ett ärendehanteringssystem men kommer att bevaras i annan form,

t.ex. på pappersutskrifter eller i elektronisk form men med försämrade sök- eller sammanställningsmöjligheter (se SOU 2015:39 s. 526 f.).

Personuppgiftslagen

I 9 § första stycket PUL framgår att det är ett grundläggande krav att den personuppgiftsansvarige ska se till att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det är alltså ändamålen för en personuppgiftsbehandling som avgör hur länge uppgifterna får bevaras. Ospecificerad lagring av personuppgifter som kan vara ”bra att ha” är inte tillåten. Behövs uppgifterna inte längre för ändamålen ska de förstöras eller avidentifieras (se SOU 1997:39 s. 356). Dock får uppgifterna bevaras även därefter så länge det behövs för historiska, statistiska eller vetenskapliga ändamål (9 § tredje stycket).

För myndigheter gäller enligt 8 § andra stycket PUL särskilda regler om förhållandet till arkivbildning. Enligt 8 § andra stycket första meningen hindrar bestämmelserna i personuppgiftslagen inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

Bestämmelsen i 10 § arkivlagen om att avvikande bestämmelser om gallring av vissa allmänna handlingar i annan lag eller förordning ska ha företräde framför arkivlagens gallringsregler syftar inte på personuppgiftslagens bestämmelser om hur länge personuppgifter får bevaras. Arkivlagstiftningen har alltså i fråga om allmänna handlingar företräde framför personuppgiftslagens bestämmelser om längsta bevarandetid. I detta avseende kan alltså sägas att intresset av att bevara allmänna handlingar har prioriterats framför integritets- och skyddsintresset.

Bevarande och gallring i särreglering för brottsbekämpande verksamhet

I så gott som all särreglering för de behöriga myndigheterna finns regler om bevarande och gallring av uppgifter. Endast ett mycket begränsat urval nämns i det följande.

I polisdatalagen, som gäller generellt för brottsbekämpande verksamhet vid Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndighetens polisiära verksamhet, finns ett omfattande regelverk om bevarande och gallring. Detta tar sikte på dels uppgifter i särskilda register som regleras i lagen, t.ex. penningtvätsregistret eller DNA-registret, dels uppgifter som mer allmänt behandlas i den brottsbekämpande verksamheten, se 2 kap. 12 § PDL med där angivna hänvisningar. Huvudprincipen kan sägas vara att personuppgifter inte får bevaras under längre tid än vad som behövs för det aktuella ändamålet. Därutöver finns bestämmelser om hur länge uppgifter får bevaras som längst. Regeringen eller den myndighet som regeringen bestämmer kan också meddela avvikande föreskrifter om längre tids bevarande för historiska, statistiska eller vetenskapliga ändamål. I 20–26 §§ PDF finns sådana närmare föreskrifter med längre bevarandetider avseende vissa slags uppgifter hänförliga till verksamhet med utredande och beivrande av brott. I 27 § finns vidare ett bemyndigande för Riksarkivet att meddela föreskrifter i övrigt om längre tids bevarande för historiska, statistiska eller vetenskapliga syften. Hur gallring ska ske regleras inte närmare i de nämnda författningarna.

I den nya tullbrottsdatalagen som träder i kraft den 1 juli 2017 finns bestämmelser om bevarande och gallring samlade i lagens 4 kap. De påminner i stora drag om regleringen i polisdatalagen med gallring som huvudregel och bevarande som undantag genom möjlighet att meddela särskilda föreskrifter.

I 4 kap. 8 § tullagen (2016:253) och 16 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränslagen) finns bestämmelser om lagring och förstöring av vissa uppgifter från transportföretag. Där framgår att uppgifter från transportföretag som Tullverket tar del av genom terminalåtkomst inte får ändras eller på annat sätt bearbetas eller lagras. Uppgifter om enskilda personer som lämnats på annat sätt än genom terminalåtkomst ska förstöras omedelbart om de visar sig sakna betydelse för utredning och lagföring av brott. Motsvarande bestämmelser finns i 26 § polislagen (1984:387). Huvudregeln är alltså att uppgifterna inte alls ska bevaras utan gallras så fort de visar sig inte behövas för det primära ändamål för vilka de togs fram. I 2 kap. 8–9 §§ TBL finns ytterligare bestämmelser om behandling av personuppgifter från transportföretag. Bestämmelserna innebär bl.a. att

bokningsuppgifterna i vissa fall får göras gemensamt tillgängliga och därmed omfattas av lagens gallringsbestämmelser.

Enligt 9 § lagen (2006:444) om passagerarregister ska en uppgift i passagerarregistret gallras inom 24 timmar efter överföringen till Polismyndigheten. Om uppgifter i registret behövs för att Polismyndigheten, Säkerhetspolisen eller Tullverket ska kunna verkställa personkontroller enligt 4 § samma lag, får uppgifterna i registret dock stå kvar till dess att myndighetens kontroller är slutförda. Vidare får regeringen meddela föreskrifter om att uppgifter i registret får stå kvar till dess att någon annan myndighet, som behöver uppgifterna för att kunna verkställa personkontroller enligt 4 §, har slutfört kontrollerna. Även här är huvudregeln således att i princip omedelbar gallring ska ske så fort uppgifterna inte längre behövs för sitt primära syfte.

Slutligen ska nämnas att det även i lagstiftningen om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst finns regler om bevarande och gallring i lagen (2007:258) och den anslutande förordningen (2007:260).

18.2.2 Brottsdatalagen

I 2 kap. 17 § BDL anges att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Detta gäller dock inte om det finns avvikande bestämmelser i lag eller förordning. Inte heller finns hinder mot att en myndighet bevarar allmänna handlingar för arkivändamål.

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande uttalat att begreppen bevarande och gallring enbart bör användas i den betydelse de har i arkivlagstiftningen för att tydligare skilja mellan arkivrättsliga regler och regler om skydd för personuppgifter. Brottsdatalagen och myndigheternas registerförfattningar bör därför i stället utgå från hur länge personuppgifter får behandlas för andra ändamål än arkivändamål (SOU 2017:29 s. 284). Detta kommer att behandlas närmare för registerförfattningarnas del i utredningen slutbetänkande.

18.3 Inledande radering hos enheten för passagerarinformation

Vårt förslag: I den nya förordning som ansluter till lagen ska föreskrivas att om lufttrafikföretagen skickat in andra PNR-uppgifter än de som anges i bilagan till lagen, ska dessa omedelbart gallras genom att raderas redan då de kommer in till enheten för passagerarinformation.

18.3.1 Direktivets bestämmelser

PNR-direktivet ålägger lufttrafikföretagen att överföra sådana PNR-uppgifter som räknas upp i bilaga I till direktivet, förutsatt att de redan samlar in sådana i sin verksamhet som en del av sin normala verksamhet. Några andra uppgifter är lufttrafikföretagen inte skyldiga att skicka till enheterna för passagerarinformation. Det finns å andra sidan inte något förbud mot att skicka fler uppgifter (så länge de inte utgör känsliga personuppgifter, se avsnitt 18.5) eller något åliggande för lufttrafikföretagen att skilja ut de PNR-uppgifter som enheterna för passagerarinformation ska motta från eventuella andra PNR-uppgifter som måhända behandlas gemensamt i passageraruppgiftssamlingen. I direktivet har därför förutsetts att lufttrafikföretagen kan komma att överföra även sådana PNR-uppgifter som enheterna inte ska ha rätt att behandla. I artikel 6.1 föreskrivs därför att för det fall de överförda PNR-uppgifterna avser andra uppgifter än de som framgår av direktivets bilaga I, ska enheten för passagerarinformation omedelbart och slutgiltigt radera dessa vid mottagandet.

18.3.2 Våra överväganden och förslag

De PNR-uppgifter som överförs till enheten för passagerarinformation blir inkomna allmänna handlingar hos Polismyndigheten när de har översänts elektroniskt från lufttrafikföretagen och enheten kan ta fram dem i läsbart skick.

Vi uppfattar direktivets artikel 6.1 som utgörande en i arkivrättsligt hänseende omedelbar gallringsskyldighet, där de uppgifter

som inte omfattas av bilaga I till direktivet inte alls ska få föras in i databasen vid enheten för passagerarinformation.

Bestämmelsen bör genomföras i stort sett i enlighet med dess ordalydelse. Av vår bestämmelse bör således framgå att de aktuella uppgifterna ska raderas omedelbart vid mottagandet. Enligt vår mening bör dock det i svensk lagstiftning vedertagna begreppet gallring användas. För att klargöra att det är fråga om en definitiv och inte endast en partiell gallring av dessa PNR-uppgifter bör det i bestämmelsen också anges att uppgifterna ska gallras genom att raderas. Ordet utplåning eller förstöras vore ett alternativt sätt att uttrycka samma sak. Med tanke på den osäkerhet om kommande begreppsapparat som för närvarande finns på grund av den pågående dataskyddsreformen, anser vi dock att begreppet radering, som förekommer i såväl dataskyddsförordningen som i det nya dataskyddsdirektivet, är att föredra. Det kan anmärkas att vi inte utesluter att den kommande utvecklingen kan medföra såväl en utmönstring av det arkivrättsliga begreppet gallring ur registerförfattningar som att annan vokabulär kommer att bli vanlig när det närmare ska beskrivas hur personuppgiftsbehandlingen ska avslutas. Det är viktigt att detta uppmärksammas i den fortsatta beredningen då en enhetlig begreppsapparat bör eftersträvas. Vi vill dock understryka att vi här och i de fortsatta delavsnitten använder begreppet gallring i dess arkivrättsliga hänseende, oaktat att motiven till gallringen syftar till att skydda enskildas personliga integritet. Den omedelbara gallringen i detta delavsnitt har integritetsskyddande syfte, men innebär samtidigt att regleringsmetoden för det är att "överskottsinformation" från lufttrafikföretagen aldrig ska bli en del av myndighetens arkiv.

Enligt vår mening kan och bör bestämmelsen om gallring genom radering tas in i den till den nya lagen anslutande förordningen.

När det gäller tillämpningen av denna omedelbara gallringsskyldighet är vi givetvis medvetna om att det dagligen kommer att komma in mycket stora mängder PNR-uppgifter till enheten, så stora mängder att det vore en orimlig tanke att personal vid enheten skulle kunna granska de inkomna uppgifterna och manuellt separera "överskottsinformation" från sådan som enheten ska ta emot. Det får dock förutsättas att enhetens tekniska lösningar programmeras och utformas på så sätt att de genom automatiserade processer kan känna av och sortera bort sådana PNR-uppgifter som omedelbart ska gallras.

18.4 Lagringstiden hos enheten för passagerarinformation för PNR-uppgifter som mottagits från lufttrafikföretag

Vårt förslag: I lagen föreskrivs att PNR-uppgifter som mottagits från lufttrafikföretagen ska lagras i databasen vid enheten för passagerarinformation i fem år. Därefter ska de gallras genom att uppgifterna raderas.

18.4.1 Direktivets bestämmelser

Lagringstiden för PNR-uppgifterna har bestämts till fem år i direktivet. Av skäl 25 framgår att denna tidsrymd ansetts dels stå i rimlig proportion till ändamålen att bekämpa terroristbrott och grov brottslighet, dels vara tillräckligt lång för att möjliggöra att PNR-uppgifterna kan användas i samband med analyser och utredningar.

I artikel 12.1 anges således att medlemsstaterna ska se till att PNR-uppgifter som lämnas till enheten för passagerarinformation från lufttrafikföretag lagras i en databas vid enheten under en period på fem år efter överföringen till enheten för passagerarinformation i den medlemsstat på vars territorium flygningen ankom eller avgick. Vid utgången av femårsperioden ska medlemsstaterna, enligt artikel 12.4 första meningen, se till att PNR-uppgifterna slutgiltigt raderas. PNR-uppgifterna ska således bevaras i databasen vid enheten för passagerarinformation i fem år, varken längre eller kortare tid.

18.4.2 Våra överväganden och förslag

PNR-direktivet är dels en verksamhetsreglering som sätter upp ett system för informationsförsörjning och -utbyte i brottsbekämpning av visst slag, dels en dataskyddsreglering som sätter upp ramar och vissa absoluta krav som ska uppfyllas i syfte att kringgärda verksamheten med tillfredsställande skydd för registrerades integritet. Regleringen är i dessa avseenden mycket sammanflätad. Bestämmelserna i artikel 12.1 och 12.4 om lagring och slutgiltig radering av de PNR-uppgifter som har överförts till enheten för passagerarinformation från lufttrafikföretagen är ett exempel på detta. Lagrings-

tiden på fem år är ett åliggande som medlemsstaterna ska genomföra i linje med sin skyldighet att bedriva sitt lands del i PNR-systemet. Även den slutliga raderingen efter fem år är ett åliggande för medlemsstaterna men är motiverad utifrån ett dataskyddsrättsligt intresse.

Vi föreslår att det i den nya lagen tas in en bestämmelse som anger att sådana PNR-uppgifter som har tagits emot, dvs. kommit in från lufttrafikföretagen, ska lagras i enhetens PNR-databas och bevaras där i fem år.

I skäl 30 till direktivet anges att direktivet inte påverkar tillämpningen av nationell rätt om principen om allmänhetens tillgång till officiella handlingar, varmed för svenskt vidkommande avses allmänna handlingar. Vi anser emellertid att det inte bör komma i fråga att utifrån de intressen som bär upp handlingsoffentligheten och med åberopande av vår grundlag och skäl 30 föreslå en längre tids lagring än den i direktivet stipulerade absoluta tidsgränsen. Något bärande insynsintresse i den stora massan PNR-uppgifter som kommer att lagras i PNR-databasen kan vi inte identifiera. I den mån PNR-uppgifter verkligen kommer att användas i den brottsbekämpande verksamheten hos behöriga myndigheter – i vilken allmänheten i och för sig har ett tungt vägande insynsintresse – rör det sig om ett proportionellt sett ytterst litet antal uppgifter för vilka andra regler för bevarande och gallring än den nu aktuella artikeln kommer att aktiveras. Vi bedömer därför att det framstår som oproblematiskt att PNR-uppgifter i PNR-databasen efter denna föreskrivna femårsperiod ska gallras definitivt.

Vi föreslår alltså en bestämmelse i den nya lagen som anger att PNR-uppgifter ska gallras fem år efter att uppgifterna kommit in till enheten från lufttrafikföretagen. Hur gallring ska ske bör också anges i lagen genom att det föreskrivs att gallringen i detta avseende ska ske genom radering. Härmed avses i praktiken att uppgifterna utplånas. Bestämmelsen, som måste införas enligt direktivet, medför att successiv gallring måste ske kontinuerligt. Det får förutsättas att de tekniska lösningarna utformas så att detta kan skötas genom förprogrammerade processer.

18.5 Radering av PNR-uppgifter som utgör känsliga personuppgifter

Våra förslag: Bland lagens inledande bestämmelser tas in en bestämmelse som förbjuder behandling av PNR-uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, eller som rör hälsa, sexualliv eller sexuell läggning. I bestämmelsen ska detta framgå genom att det hänvisas till relevant bestämmelse i brottsdatalagen som närmare räknar upp dessa slags uppgifter såsom känsliga personuppgifter. I den nya lagen kommer alltså dessa uppgifter inte att närmare definieras.

Det förs i lagen in en bestämmelse som anger att enheten för passagerarinformation omedelbart ska gallra PNR-uppgifter som utgör känsliga personuppgifter genom att radera dem om enheten mottar sådana uppgifter från lufttrafikföretag eller från en enhet för passagerarinformation i en annan medlemsstat. Vidare förs det in en bestämmelse som anger att även behöriga myndigheter omedelbart ska gallra sådana uppgifter genom att radera dem för det fall de skulle motta sådana.

18.5.1 Direktivets bestämmelser

Enligt artikel 13.4 ska medlemsstaterna förbjuda behandling av PNR-uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religion eller filosofiska övertygelse, fackförenings-tillhörighet, hälsotillstånd, sexualliv eller sexuella läggning. Om enheten för passagerarinformation mottar PNR-uppgifter som avslöjar sådana uppgifter, ska dessa uppgifter omedelbart raderas.

18.5.2 Allmänt om känsliga personuppgifter

De i artikel 13.4 uppräknade uppgifterna utgör vad som i dataskyddssammanhang brukar betecknas som känsliga personuppgifter, se t.ex. 13 § PUL. Också det nya dataskyddsdirektivet innehåller en bestämmelse om känsliga personuppgifter (artikel 10). Enligt den bestämmelsen får sådana personuppgifter behandlas endast om det är absolut

nödvändigt och om vissa närmare angivna förutsättningar i övrigt är uppfyllda. Bestämmelsen är genomförd i 2 kap. 11–14 §§ BDL. Även i artikel 9 i dataskyddsförordningen – som framöver kommer att vara tillämplig exempelvis hos lufttrafikföretagen – finns ett principiellt förbud mot behandling av känsliga personuppgifter samt vissa undantagsgrunder.

Uppräkningen av vilka personuppgifter som är att se som känsliga har tidigare varit densamma i olika instrument på dataskyddsområdet. Det nya dataskyddsdirektivet och dataskyddsförordningen innehåller emellertid ytterligare två kategorier av känsliga personuppgifter; genetiska och biometriska uppgifter, som inte anges i PNR-direktivet. I 2 kap. 11 § BDL behandlas samtliga känsliga personuppgifter som avses i PNR-direktivet. Biometriska och genetiska uppgifter behandlas i 2 kap. 12 §.

18.5.3 PNR-uppgifter som kan utgöra känsliga personuppgifter

PNR-direktivet ger inte något stöd för att lufttrafikföretagen ska överföra känsliga personuppgifter till enheten för passagerarinformation. Tvärtom anges i direktivet att behandling av känsliga personuppgifter ska förbjudas. Enligt direktivet ska således inte lufttrafikföretagen skicka in känsliga personuppgifter till enheten för passagerarinformation. Dock kan sådana uppgifter komma att överföras av misstag. Känsliga personuppgifter kan t.ex. komma att ingå bland de allmänna anmärkningarna (punkten 12 i bilaga I till direktivet). Som tidigare har angetts utgör de allmänna anmärkningarna ett fritextfält för kommunikation mellan t.ex. resebokare och flygbolagspersonal. Här kan finnas uppgifter om t.ex. specialkost, behov av assistans, medicinska behov och andra hälsouppgifter. Dessa uppgifter kan avslöja en persons religion eller hälsotillstånd och får därmed inte behandlas enligt direktivet.

Även andra PNR-uppgifter kan innehålla personuppgifter som avslöjar känsliga personuppgifter. Man kan t.ex. tänka sig att en e-postadress innehåller ett partinamn eller fackföreningsnamn i en medlemsstat och adressen kan därmed avslöja en persons politiska tillhörighet eller fackföreningstillhörighet.

Uppgifter om en persons nationalitet har i lagstiftning som rör behandling av personuppgifter inte ansetts vara uppgifter som normalt avslöjar ras eller etniskt ursprung (se t.ex. SOU 2015:39 s. 328 f.). En uppgift om att en resenär är medborgare i ett visst land omfattas alltså inte av förbudet. Skulle emellertid en sådan uppgift i det enskilda fallet t.ex. avslöja etniskt ursprung faller den dock in under förbudet. Uppgifter om att en viss person närmast kommer från en viss världsdel eller ett visst land faller också som regel utanför förbudet mot behandling av känsliga personuppgifter (se prop. 2009/10:85 s. 325). Dock kan uppgifter om namn och språkkunskaper tillsammans utgöra indirekta upplysningar om en persons etniska ursprung (se t.ex. SOU 2003:40 s. 180).

18.5.4 Våra överväganden och förslag

Direktivet anger att varje medlemsstat ska förbjuda behandling av PNR-uppgifter som avslöjar känsliga personuppgifter. En bestämmelse med denna innebörd bör därmed föras in i vårt lagförslag. Med tanke på dess centrala betydelse och att den bör gälla för samtliga aktörer som omfattas av lagen bör den tas in bland lagens inledande bestämmelser. Vidare bör det i bestämmelsen hänvisas till den paragraf i brottsdatalogen vari just dessa slags känsliga personuppgifter definieras som sådana. Vårt förbud mot behandling av känsliga personuppgifter gäller i övrigt i stället för bestämmelsen i 2 kap. 11 § BDL.

Det bör vidare av lagen framgå att för det fall enheten för passagerarinformation mottar PNR-uppgifter som utgör sådana uppgifter som räknas upp i artikel 13.4, ska de omedelbart gallras genom att raderas.

Direktivet ger inte några närmare anvisningar kring hur gallringen av de PNR-uppgifter som avslöjar känsliga personuppgifter ska gå till. Det är således upp till varje medlemsstat att finna lämpliga tekniska lösningar för att uppfylla denna skyldighet. Eftersom en hel del av de känsliga personuppgifterna kan tänkas förekomma i det s.k. fritextfältet, hade en lösning varit att helt radera detta fält av PNR-uppgifter. Dock skulle en sådan lösning medföra att även sådana PNR-uppgifter som inte innehåller känsliga personuppgifter gallrades. Sådana uppgifter som enligt direktivet ska överföras av

lufttrafikföretagen och behandlas av enheterna för passagerarinformation skulle därmed helt tas bort. En sådan generell gallring av hela fritextfältet kan inte anses vara förenlig med direktivet. Vi kan därför inte förorda en sådan lösning.

Det ska vidare poängteras att förbudet mot behandling av PNR-uppgifter som utgör känsliga personuppgifter och gallringsskyldigheten inte enbart omfattar sådana PNR-uppgifter som kommer in direkt från lufttrafikföretagen. Förbudet och gallringsskyldigheten gäller även för det fall sådana PNR-uppgifter skulle komma in till enheten från motsvarande enheter i andra medlemsstater, t.ex. därför att en enhet i det andra landet inte insett att uppgiften i fråga röjer ett medlemskap i en svensk fackförening eller liknande.

De tekniska lösningar som tas fram för att genomföra PNR-systemet får utformas så att de kan tillgodose kravet på radering av PNR-uppgifter som utgör känsliga personuppgifter.

Eftersom enheten för passagerarinformation inte får behandla PNR-uppgifter som utgör känsliga personuppgifter ska sådana uppgifter inte heller föras över från enheten till de behöriga myndigheterna. Dock kan det i något fall ändå förekomma att sådana uppgifter förs vidare av misstag. T.ex. kan det först sedan PNR-uppgifter har överförts från enheten uppmärksammas att dessa innehåller en persons yrkestitel i vilken framgår att denne är t.ex. präst, rabbin eller imam i ett trossamfund. För det fall ett sådant misstag skulle inträffa och PNR-uppgifter som utgör känsliga personuppgifter skulle överföras till en behörig myndighet, bör den behöriga myndigheten omedelbart radera dessa. Vi föreslår att en bestämmelse med denna innebörd förs in i lagen. Bestämmelsen bör utformas på samma sätt som motsvarande bestämmelse för enheten för passagerarinformation. För det fall en behörig myndighet mottar PNR-uppgifter som utgör känsliga personuppgifter ska således dessa genast gallras genom att raderas.

18.6 Enhetens bevarande och gallring av resultatet av en förhandsbedömning

Våra förslag: Det förs i förordning in bestämmelser som genomför artikel 12.5 om hur resultatet av en förhandsbedömning – dvs. träffar – ska få sparas. En positiv träff ska gallras så snart resultatet inte längre behövs för att kunna informera behöriga mottagare om resultatet. En ”falsk” träff får bevaras längst till dess att de bakomliggande PNR-uppgifterna i databasen gallrats vid utgången av den femåriga lagringstiden.

Vidare införs en bestämmelse om att träffar med PNR-information som har kommit in till enheten från en motsvarande enhet i en annan medlemsstat ska gallras när den vidarebefordrats till en behörig myndighet och inte längre behövs för att en återrapportering ska kunna göras till avsändaren i den andra medlemsstaten.

18.6.1 Direktivets bestämmelser

Resultatet av en förhandsbedömning av passagerare, dvs. den träff som kan uppkomma vid de bedömningar av passagerare som ska göras före deras beräknade ankomst till eller avresa från Sverige, får endast bevaras av enheten för passagerarinformation så länge som det krävs för att informera de behöriga myndigheterna och eventuellt enheterna för passagerarinformation i andra medlemsstater om träffen. Detta framgår av första meningen i artikel 12.5.

Om resultatet av en automatisk behandling av PNR-uppgifter efter en individuell granskning enligt artikel 6.5 inte ger någon träff, dvs. inte visar sig vara intressant för vidare granskning, får resultatet dock bevaras för att undvika framtida ”falska” träffar. De falska träffarna får sparas så länge de bakomliggande PNR-uppgifterna inte har raderats. Detta anges i andra meningen i artikel 12.5.

18.6.2 Våra överväganden och förslag

Positiva träffar ska inte sparas

Bestämmelsen i artikel 12.5 första meningen skulle kunna tolkas som att en s.k. positiv match eller träff bara får sparas tills den sänts vidare till en eller flera behöriga myndigheter. Vi menar emellertid att direktivet rimligen måste förstås så att enheten ska få behålla resultatet en viss tid även efter att ha skickat en träff till en av de behöriga myndigheterna för vidare granskning. Det finns nämligen behov av viss tid för återrapportering från den behöriga myndigheten. Den behöriga myndigheten kan exempelvis återrapportera att någon ytterligare behörig myndighet eller något annat lands enhet för passagerarinformation också bör informeras om träffen.

Direktivets bestämmelse angående sparande av träffar bör genomföras så att dessa förutsättningar för hur länge resultaten av en förhandsbedömning av PNR-uppgifter får bevaras tillgodoses. Det bör således i en bestämmelse anges att ett resultat ska gallras så snart det inte längre behövs för att informera behöriga myndigheter och eventuellt andra medlemsstaters enheter för passagerarinformation om resultatet. Frågan kan regleras i förordning. Den föreslagna bestämmelsen ska utgöra en huvudregel för hur länge resultat, dvs. träffar, får bevaras. Vi ser inget behov av att fastställa en tidsgräns för hur lång tid som kan gå innan gallring ska ske. Det kan dock inte röra sig om någon längre tid, högst någon vecka enligt vår bedömning.

”Falska” träffar får sparas

En falsk träff, dvs. resultatet av en förhandsbedömning som efter den individuella granskning som skett på enheten enligt artikel 6.5 inte bedöms behöva granskas närmare och därför inte har översänts till en behörig myndighet, får alltså sparas i upp till fem år enligt artikel 12.5 andra meningen. Syftet är att undvika upprepning av samma felaktiga träff mot urvalskriterierna. Sparade uppgifter om falska träffar kan nämligen medföra att oskyldiga personer inte blir kontrollerade på nytt vid en ny resa. De falska träffarna kan även användas för att förbättra urvalskriterierna. Enligt vår tolkning av bestämmelsen måste en falsk träff kunna konstateras även efter ett översändande av träffen till en behörig myndighet, nämligen om

den myndigheten återrapporterar att den vidare granskningen visat att träffen var falsk, dvs. att det fanns inte fog för några misstankar.

En reglering i enlighet med det här sagda bör införas genom en bestämmelse som innebär ett undantag från huvudregeln om bevarande av positiva träffar. Av bestämmelsen bör framgå att om sådana träffar som fått fram vid en förhandsbedömning av PNR-uppgifter efter en initial bedömning inte anses ge anledning till behov av vidare granskning, får resultatet bevaras längst till dess de bakomliggande PNR-uppgifterna har gallrats, dvs. vid utgången av den femåriga lagringstiden. Senast då ska de gallras. Detsamma ska gälla om träffarna sänts vidare till behöriga myndigheter men dessa hinner återrapportera att träffarna inte föranlett vidare misstankar innan träffarna har hunnit gallras av enheten för passagerarinformation enligt huvudregeln om att träffar ska gallras efter det att de inte längre behövs för att kunna informera behöriga mottagare. Även denna fråga kan regleras i förordning.

Träffar som har mottagits från andra medlemsstater

PNR-direktivet innehåller inga uttryckliga bestämmelser om hur länge de träffar med PNR-uppgifter som har översänts från andra medlemsstaters enheter för passagerarinformation till vår motsvarande enhet får bevaras. Som har angetts tidigare är enheten för passagerarinformation en förmedlare av PNR-information och inte en slutlig destinationsinstans när det gäller det internationella utbytet av sådana uppgifter. Den PNR-information som överförs till enheten från andra medlemsstaters motsvarande enheter ska således sändas vidare till de behöriga myndigheterna för att användas där. Tanken är alltså inte att dessa uppgifter ska bevaras hos enheten. De PNR-uppgifter som har översänts till vår nationella enhet för passagerarinformation från andra medlemsstaters motsvarande enheter kan således, enligt vår mening, inte ens tolkningsvis anses omfattas av de lagringsbestämmelser som anges i artikel 12.

Enligt vår mening bör det föras in en bestämmelse som anger hur länge PNR-information som har översänts från andra medlemsstaters enheter för passagerarinformation till vår motsvarande enhet får bevaras där. En sådan bestämmelse bör lämpligen tas in i den nya förordningen.

Som har angetts ovan ska vår enhet för passagerarinformation vidareända den PNR-information som den mottagit från andra medlemsstaters motsvarande enheter till våra behöriga myndigheter, och inte därefter bevara den informationen. En bestämmelse liknande den i artikel 12.5 första meningen, som anger att resultatet av en behandling av PNR-uppgifter ska bevaras endast så länge som det krävs för att genomföra översändandet till behöriga myndigheter, skulle därmed kunna föreslås. Det har emellertid framförts till oss att enheten för passagerarinformation behöver kunna bevara den aktuella PNR-informationen ytterligare en tid på liknande sätt som beträffande enhetens egna träffar. Enheten för passagerarinformation ska nämligen, utan att det anges i direktivet, återrapportera till den motsvarande enhet som har översänt informationen och ange om den översända informationen har varit av intresse för våra behöriga myndigheter. För att kunna utföra denna återrapportering behöver först en liknande rapportering ske från de behöriga myndigheter som har mottagit informationen till vår enhet för passagerarinformation. Först därefter kan enheten föra dessa uppgifter vidare. För att vår enhet för passagerarinformation ska veta vilken information som återrapporteringen ska avse, vore det därför lämpligt att enheten får bevara informationen om träffen till dess den har gjort sin återrapportering. Vi föreslår därför en bestämmelse som anger att den PNR-information som har mottagits från andra medlemsstaters enheter för passagerarinformation ska gallras så snart den inte längre behövs för återrapportering till den enhet för passagerarinformation som har översänt informationen. Enligt vår bedömning talar övervägande skäl för att det är befogat med en sådan ytterligare kort tids bevarande. Vi ser inte heller här något behov av att fastställa en tidsgräns för hur lång tid som kan gå innan gallring ska ske. Liksom ovan bedömer vi dock att en veckas tid bör vara tillräcklig för att genomföra en återrapportering.

18.7 Enhetens bevarande och gallring av resultat av behandling av PNR-uppgifter på begäran

Våra förslag: Resultatet av en sådan behandling av PNR-uppgifter som görs för att besvara en begäran ska gallras så snart det inte längre behöver bevaras för återrapportering från mottagaren.

Resultat som andra medlemsstaters enheter för passagerarinformation tar fram för att besvara en svensk förfrågan och sänder över till den svenska enheten, ska gallras så snart det inte längre behövs för att kunna informera behöriga myndigheter och eventuellt återrapportera till den andra medlemsstaten.

Framtagen PNR-information efter behandling på begäran

Det finns inga bestämmelser i direktivet som reglerar vad som ska gälla för sådana resultat som fås fram när enheten behandlar och bearbetar PNR-uppgifter för att besvara en begäran från behöriga myndigheter enligt artikel 6.2 b, från enheter i andra medlemsstater enligt artikel 9.2, från Europol enligt artikel 10.2 eller vid överföringar till tredjeland, se artikel 11.1 d. Sådan information torde kunna innehålla både PNR-uppgifter och eventuell kompletterande information som fås fram genom sökningar i relevanta databaser.

Enligt vår bedömning kommer det inte att finnas någon anledning för enheten att ha tillgång till dessa resultat längre tid än vad det krävs för att kunna informera de behöriga mottagarna. Vi föreslår därför att det i förordning tas in en bestämmelse som anger att resultatet av en sådan behandling av PNR-uppgifter som görs för att besvara en särskild förfrågan ska gallras så snart återrapportering har skett eller en sådan inte längre är aktuell.

Resultat som mottagits från andra medlemsstaters enheter

Enheten för passagerarinformation kommer också att motta resultat av sådan behandling av PNR-uppgifter som har skett vid andra medlemsstaters enheter för passagerarinformation för att besvara förfrågningar från den svenska enheten enligt artikel 9.2. Direktivet innehåller inte heller några bestämmelser om bevarande eller gall-

ring av sådana uppgifter. Vår bedömning är dock i denna fråga densamma som ovan, nämligen att det inte finns något behov av att spara denna information vid den nationella enheten för passagerarinformation. Resultat som mottagits från andra medlemsstaters enheter efter en svensk begäran bör därför gallras så snart den har överförts till relevanta behöriga myndigheter och en eventuell återrapportering har skett till den andra medlemsstaten. Även denna fråga bör kunna regleras i förordning.

18.8 Bevarande och gallring av PNR-information hos behöriga myndigheter

Vårt förslag: PNR-information som de behöriga myndigheterna har mottagit från enheten för passagerarinformation efter enhetens förhandsbedömning ska gallras genom att raderas, om den visar sig sakna betydelse för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Vår bedömning: Behöriga myndigheters bevarande och gallring av PNR-information som de mottar från en enhet för passagerarinformation bör i övrigt styras av den reglering som i övrigt gäller för myndigheternas behandling av personuppgifter i aktuell verksamhet.

18.8.1 Direktivets bestämmelser

Bestämmelserna i direktivet om lagring, bevarande och radering behandlar endast hur PNR information ska och får hanteras vid enheten för passagerarinformation. I artikel 12.4 andra meningen anges dock att skyldigheten i första meningen att slutgiltigt radera PNR-uppgifter vid utgången av den femåriga lagringstiden inte gäller om specifika PNR-uppgifter har överförts till behöriga myndigheter och används i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet. Då ska de behöriga myndigheternas lagring av uppgifterna i stället regleras av nationell rätt.

18.8.2 Våra överväganden och förslag

När behöriga myndigheter mottar PNR-information från enheten för passagerarinformation sker det som en del av myndigheternas ordinarie verksamhet avseende sådan kvalificerad brottslighet som omfattas av PNR-direktivets bestämmelser. Detsamma gäller när en behörig myndighet undantagsvis får PNR-information direkt från en motsvarande enhet i en annan medlemsstat. Förutsättningen för informationshantering är i vart fall såvitt gäller personuppgifter noga reglerade hos de myndigheter som kan komma att bli behöriga sådana enligt vår lag, se t.ex. polisdatalagen och tullbrottsdatalagen. Enligt vår mening uppfyller dessa regleringar en rimlig avvägning mellan de olika intressen som står mot varandra även när det gäller PNR-uppgifter eller annan PNR-information. Det saknas därför – med ett undantag – anledning att föreslå några bestämmelser om hur länge behöriga myndigheter får bevara sådan information som de tar emot från en enhet för passagerarinformation.

Undantaget avser sådan PNR-information som enheten för passagerarinformation efter sin förhandsbedömning enligt artikel 6.2 a skickar till en eller flera behöriga myndigheter för vidare granskning. För det fall den behöriga myndigheten konstaterar att PNR-informationen med resultatet av enhetens behandling visar sig sakna betydelse för att bekämpa terroristbrottslighet eller grov brottslighet, är det vår mening att informationen ska gallras hos den behöriga myndigheten genom att raderas. Vi föreslår därför en sådan bestämmelse, som bör föras in i lagen. Bestämmelsen kan sägas utgöra en motsvarighet till de bestämmelser som finns i 26 § polislagen, 4 kap. 8 § tullagen och 16 § inregränslagen, se avsnitt 18.2.1. Bestämmelsen kommer att gälla för samtliga nuvarande och eventuellt tillkommande behöriga myndigheter. Det ska observeras att det kan ta olika lång tid i olika fall att konstatera om en uppgift saknar betydelse för den angivna brottsligheten. Det är alltså först när detta konstaterats som gallringsskyldigheten träder in.

19 Personuppgiftsansvarigas skyldigheter

19.1 Personuppgiftsansvar

19.1.1 Direktivets bestämmelser

PNR-direktivet innehåller inte några särskilda bestämmelser om personuppgiftsansvar. Däremot innehåller direktivet en rad skyldigheter som ålagts de nationella enheterna för passagerarinformation. Exempelvis anger direktivet hur enheten får behandla PNR-uppgifter och när enheten får överföra dessa uppgifter till behöriga myndigheter och andra mottagare. Vidare anges i direktivet att medlemsstaterna ska se till att enheten för passagerarinformation bevarar viss dokumentation och loggar behandlingen av uppgifter samt informerar om personuppgiftsincidenter. Enheten ska också utse ett dataskyddsombud. Alla dessa skyldigheter innebär krav på behandling av personuppgifter.

Vidare anges i artikel 13.3 att direktivet inte påverkar tillämpligheten av det nuvarande dataskyddsdirektivet¹ på lufttrafikföretags behandling av personuppgifter, i synnerhet deras skyldigheter att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifters säkerhet och konfidentialitet.

¹ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

19.1.2 Nya dataskyddsdirektivet och brottsdatalagen

En definition av begreppet personuppgiftsansvarig finns intagen i artikel 3.8 i det nya dataskyddsdirektivet. Enligt definitionen avses med personuppgiftsansvarig en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller medlemsstaternas nationella rätt. Av definitionen framgår att endast myndigheter kan vara personuppgiftsansvariga inom direktivets område. Enligt skäl 50 i direktivet bör vidare de personuppgiftsansvariga åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar.

Utredningen om 2016 års dataskyddsdirektiv föreslår att en personuppgiftsansvarig definieras som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (1 kap. 6 § BDL). Enligt 3 kap. 1 § BDL ska den personuppgiftsansvarige vara ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar. Enligt utredningens allmänna överväganden ger brottsdatalagens definition vägledning som på ett tillräckligt tydligt sätt gör att det går att fastställa vem som är personuppgiftsansvarig i verksamheter där endast brottsdatalagen kommer att gälla. Vidare pekas på att myndigheternas registerförfattningar föreskriver vem som är personuppgiftsansvarig samt att utredningen kommer att i sitt slutbetänkande behandla hur personuppgiftsansvaret ska regleras i dessa författningar (SOU 2017:29 s. 298).

19.1.3 Våra överväganden och förslag

Vårt förslag och vår bedömning: I lagen tas in en bestämmelse om att Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som utförs vid enheten för passagerarinformation. Ytterligare bestämmelser om personuppgiftsansvar behöver inte föras in i lagen.

*Personuppgiftsansvaret för behandling av personuppgifter
vid enheten för passagerarinformation*

Enheterna för passagerarinformation får enligt direktivet inrättas såsom nya, egna, myndigheter eller etableras inom en redan befintlig myndighet. Eftersom valet av organisationsform är upp till varje medlemsstat, är det förståeligt att direktivet ålägger enheterna för passagerarinformation de skyldigheter som direktivet kräver. Den svenska enheten för passagerarinformation kommer dock att inrättas inom Polismyndigheten och ingå som en organisatorisk enhet i den myndigheten. Inom svensk förvaltning är det normalt så att det yttersta ansvaret för verksamheten läggs på myndighetsnivå. Det är således myndigheten i stort som ansvarar för personuppgiftsbehandlingen.

Eftersom enheten för passagerarinformation kommer att placeras inom Polismyndigheten är det alltså den enda rimliga ordningen enligt vår mening att det är Polismyndigheten som ska vara personuppgiftsansvarig för den behandling av personuppgifter som enheten utför enligt den lag som vi föreslår. Frågan är om detta behöver regleras särskilt.

För Polismyndighetens personuppgiftsbehandling i den brottsbekämpande verksamheten kommer brottsdatalagen att bli tillämplig. I brottsdatalagen pekas inte särskilt ut vilken myndighet som är personuppgiftsansvarig för vad. Såvitt vi i skrivande stund kan förmoda kommer den befintliga regleringen av personuppgiftsansvaret att i huvudsak behållas i de särskilda registerförfattningarna för behöriga myndigheter på området, däribland polisdatalagen, även sedan de anpassats till brottsdatalagen. Polisdatalagen kommer att gälla även för arbetet vid enheten för passagerarinformation, för det fall inte annat anges i vår lag. Det torde därför inte vara helt nödvändigt att även i vår lag ange att det är Polismyndigheten som har personuppgiftsansvaret. Eftersom frågan förtjänar tydlighet föreslår dock vi att det i lagen förs in en bestämmelse om Polismyndighetens personuppgiftsansvar. Behovet av tydlighet sammanhänger bl.a. med att det annars kan uppstå missförstånd på grund av de bestämmelser som anger vad enheten för passagerarinformation ska eller får göra. Bestämmelsen är således av upplysande karaktär och förtydligar att det är Polismyndigheten som ska ansvara för att PNR-direktivets och brottsdatalagens olika skyldigheter följs vad gäller verksamheten vid enheten för passagerarinformation.

Personuppgiftsansvaret för behandling hos behöriga myndigheter

Sedan PNR-uppgifterna har överförts från enheten för passagerarinformation till olika behöriga myndigheter kommer respektive myndighet att vara ansvarig för de överförda personuppgifterna och dess fortsatta behandling. Det gäller oavsett om PNR-informationen överförs efter en förhandsbedömning eller på särskild begäran. Detta behöver inte regleras särskilt i vår lag.

Personuppgiftsansvaret för behandling hos lufttrafikföretagen

Lufttrafikföretagen åläggs en författningsreglerad skyldighet att överföra PNR-uppgifter till enheten för passagerarinformation. Så gott som samtliga lufttrafikföretag torde vara sådana i EU etablerade aktörer som kommer att omfattas av den kommande dataskyddsförordningens tillämpningsområde, se artikel 3 i förordningen. I förordningen finns en med det nya dataskyddsdirektivet likartad definition av personuppgiftsansvarig (artikel 4.7). De PNR-uppgifter som lufttrafikföretagen överför är uppgifter som företagen redan samlat in i sin kommersiella verksamhet i vilken de bestämmer ändamålen och medlen med behandlingen av uppgifterna. Det torde inte kunna råda något tvivel om att ett lufttrafikföretag har personuppgiftsansvaret för de PNR-uppgifter som företaget samlat in och behandlar. Visserligen anges i artikel 11.1 i den tidigare nämnda förordningen om en uppförandekod för datoriserade bokningssystem² att systemleverantören ska betraktas som registeransvarig, dvs. personuppgiftsansvarig för personuppgifterna i systemen. Enligt vår mening fråntar dock inte detta förhållande lufttrafikföretagens personuppgiftsansvar enligt dataskyddsförordningen för PNR-uppgifterna i samband med deras överföring till enheten för passagerarinformation. Det kan här anmärkas att artikel 13.3 respektive 21.2 i PNR-direktivet synes förutsätta att lufttrafikföretagen är personuppgiftsansvariga i detta avseende. Det förhållandet att lufttrafikföretagen åläggs en skyldighet att översända redan insamlade uppgifter till enheten för passagerarinformation medför inget behov av särskild reglering av person-

² Europaparlamentets och rådets förordning (EG) nr 80/2009 av den 14 januari 2009 om en uppförandekod för datoriserade bokningssystem och upphävande av rådets förordning (EEG) nr 2299/89.

uppgiftsansvaret menar vi. Lufttrafikföretagens personuppgiftsansvar enligt dataskyddsförordningen för PNR-uppgifterna kommer alltså att omfatta deras överföring av PNR-information till enheten för passagerarinformation. För det fall ett lufttrafikföretag anlitar en systemleverantör för överföringen till enheten för passagerarinformation uppträder denne, i fråga om överföringen, som ett personuppgiftsbiträde som behandlar personuppgifter för det personuppgiftsansvariga lufttrafikföretagets räkning.

Ansvaret för att överföringen till enheten för passagerarinformation sker på ett säkert sätt ligger således hos lufttrafikföretagen. De har dock givetvis inget ansvar för den fortsatta hantering som sker vid enheten eller behöriga myndigheter m.fl. från och med enhetens mottagande av uppgifterna.

19.2 Generella datasäkerhetsbestämmelser

19.2.1 Direktivets bestämmelser

Direktivet innehåller ett flertal bestämmelser som syftar till att säkerställa en hög nivå av datasäkerhet vid behandlingen av PNR-uppgifter. I artikel 13.7 anges att medlemsstaterna ska se till att deras enhet för passagerarinformation genomför lämpliga tekniska och organisatoriska åtgärder och förfaranden för att säkerställa en så hög säkerhetsnivå som är lämplig med tanke på de risker som är förknippade med behandlingen och arten av PNR-uppgifterna. Vidare anges i artikel 13.2 att medlemsstaterna ska föreskriva att de nationella bestämmelser om konfidentiell behandling och datasäkerhet som har antagits för genomförande av artiklarna 21 och 22 i dataskyddsrambeslutet även är tillämpliga på all behandling av personuppgifter i enlighet med detta direktiv. En ytterligare bestämmelse med anknytning till datasäkerhet är artikel 6.8 vari anges att lagring, behandling och analys av PNR-uppgifter vid enheten för passagerarinformation uteslutande ska utföras på en eller flera säkra platser på en medlemsstats territorium.

Som redan tidigare nämnts anges vidare i artikel 13.3 att direktivet inte påverkar tillämpligheten av det nuvarande dataskyddsdirektivet på lufttrafikföretags behandling av personuppgifter, i synnerhet deras skyldigheter att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifters säkerhet och

konfidentialitet. I artikel 16.1 anges vidare att all överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation ska göras med elektroniska medel som tillhandahåller tillräckliga garantier med avseende på de tekniska säkerhetsåtgärder och de organisatoriska åtgärder som styr den behandling som ska utföras. I händelse av tekniska problem får PNR-uppgifterna överföras på annat lämpligt sätt under förutsättning att samma säkerhetsnivå upprätthålls och att unionsrätten om dataskydd respekteras fullt ut (se även artikel 8.3).

19.2.2 Dataskyddsrambeslutet och dess genomförande i svensk rätt

Artikel 22 i dataskyddsrambeslutet föreskriver krav på säkerhet i samband med behandlingen av personuppgifter. Enligt bestämmelsen ska medlemsstaterna se till att behöriga myndigheter vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från att avsiktligt eller oavsiktligt utplånas eller gå förlorade samt från ändringar, otillåten spridning och otillåten tillgång till uppgifterna. I punkten 2 ställs mera konkreta krav på olika typer av åtgärder som dels ska förhindra att uppgifterna hamnar i orätta händer, dels tillförsäkra att det går att i efterhand kontrollera vem som har lagt in uppgifter och att de system som används fungerar tillfredsställande.

I artikel 21 i rambeslutet föreskrivs att personuppgifter endast får behandlas av anställda vid den behöriga myndigheten eller efter instruktioner från denna, om det inte föreligger rättsliga skyldigheter till annan behandling. Vidare ska den som anlitas för att arbeta för en behörig myndighet vara bunden av alla de bestämmelser om skydd av uppgifter som gäller för respektive myndighet.

De aktuella bestämmelserna föranledde inte några ändringar i lag eller förordning i samband med genomförandet av rambeslutet, eftersom gällande rätt för den brottsbekämpande sektorn redan ansågs tillgodose kraven enligt rambeslutet (se prop. 2008/09:16 s. 52 f.). Bland annat hänvisades till de allmänna bestämmelserna i 30–32 §§ PUL om säkerheten vid behandling av personuppgifter. Bestämmelserna avser att trygga både den tekniska säkerheten och att de personer som behandlar uppgifterna har tillräckliga instruktioner för att behandla uppgifterna på ett korrekt sätt. Den personuppgiftsansvarige har ett stort ansvar för säkerheten. Vidare hänvisades till att

bestämmelser om informationssäkerhet även finns i andra författningar, t.ex. i arkivlagen (1990:782). Vad gäller artikel 21 ansågs därutöver 14 § i lagen (1994:260) om offentlig anställning ha betydelse för att uppfylla rambeslutets krav såvitt gäller allmän verksamhet.

19.2.3 Brottsdatalagen

Som tidigare har angetts upphävs dataskyddsrambeslutet i samband med genomförandet av det nya dataskyddsdirektivet. Av PNR-direktivets skäl 27 framgår att hänvisningar till dataskyddsrambeslutet bör ses som hänvisningar till såväl nuvarande lagstiftning som de framtida bestämmelser som kommer att ersätta denna. Eftersom det nya dataskyddsdirektivet ska genomföras i nationell rätt ungefärligen samtidigt som PNR-direktivet, får hänvisningarna till dataskyddsrambeslutet läsas som hänvisningar till det nya dataskyddsdirektivet.

Som tidigare framgått föreslås det nya dataskyddsdirektivet genomföras i svensk rätt genom brottsdatalagen och den tillhörande förordningen. Så gäller även för det nya dataskyddsdirektivets bestämmelser om tekniska och organisatoriska åtgärder. Enligt 3 kap. 2 § BDL ska den personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas. I 3 kap. 3 § anges att den personuppgiftsansvarige ska, genom lämpliga tekniska och organisatoriska åtgärder, se till att dataskyddsprinciper säkerställs på ett effektivt sätt och att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd). Det gäller både vid beslut om hur behandlingen ska utföras och vid behandlingen.

Enligt 3 kap. 4 § ska den personuppgiftsansvarige se till att det i automatiserade behandlingssystem som regel endast är möjligt att behandla de personuppgifter som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

I 3 kap. 6 § anges att den personuppgiftsansvarige ska se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Kan en typ av ny behandling eller betydande förändringar avseende redan pågående behandling antas medföra särskild risk för intrång i den registrerades personliga integritet, ska den person-

uppgiftsansvarige, enligt 3 kap. 7 §, innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter. I sådana fall ska den personuppgiftsansvarige samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs.

Enligt 3 kap. 8 § ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. I 3 kap. 8 § BDF anges vidare vad som ska beaktas vid utformningen av säkerhetsåtgärder för att en lämplig säkerhetsnivå ska uppnås.

För en närmare beskrivning av de föreslagna bestämmelserna hänvisas till SOU 2017:29.

19.2.4 Våra överväganden och förslag

Vårt förslag och vår bedömning: Det ska i lagen föras in en bestämmelse som genomför artikel 6.8 i direktivet. Enligt bestämmelsen får enheten för passagerarinformations lagring och annan behandling av PNR-uppgifter inte ske utanför en medlemsstats territorium. Generella dataskyddsbestämmelser behöver i övrigt inte föras in i lagen.

Som framgått innehåller brottsdatalagen ett flertal bestämmelser som innebär att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att säkerställa en hög säkerhetsnivå till skydd av personuppgifter. De ovan angivna bestämmelserna innehåller även krav på sådan konfidentiell behandling och datasäkerhet som avses i dataskyddsrambeslutet. Brottsdatalagen kommer att gälla såväl för den personuppgiftsbehandling som sker vid enheten för passagerarinformation som vid de flesta behöriga myndigheter som senare kommer att ta del av PNR-information.

Bestämmelserna i brottsdatalagen är generellt formulerade och kommer därmed att bli direkt tillämpliga för den personuppgiftsbehandling som avses i PNR-direktivet och som utförs vid enheten för passagerarinformation eller vid de flesta behöriga myndigheter. Enligt vår uppfattning motsvarar dessa generella bestämmelser de krav som bör ställas i fråga om PNR-information. Vi förutsätter att

registerförfattningarna för de behöriga myndigheter som inte kommer att tillämpa brottsdatalagen kommer att innehålla motsvarande bestämmelser. Särskilda bestämmelser i dessa frågor behöver, med ett undantag, således inte föras in i vårt lagförslag.

Undantaget avser kravet i artikel 6.8 om att enhetens lagring, behandling och analys av PNR-uppgifter måste ske på en eller flera säkra platser på en medlemsstats territorium. Den bestämmelsen saknar motsvarighet i brottsdatalagen och bör genomföras i den nya lagstiftning vi föreslår. Enligt vår bedömning innebär bestämmelsen ett förbud mot att lagring och annan behandling sker på ett territorium utanför en medlemsstat enligt direktivet. Det innebär alltså inte nödvändigtvis ett krav på att behandlingen ska ske i Sverige även om det är så som planeras ske. För att inte låsa fast den tekniska utvecklingen av PNR-systemet och samarbetet mellan medlemsstaterna för lång tid bör det inte föreskrivas att all lagring och annan behandling måste ske i Sverige. Artikel 6.8 bör i detta avseende genomföras som ett absolut förbud mot att enheten för passagerarinformation lagrar och utför annan behandling av PNR-uppgifter utanför medlemsstaternas territorium. Med tanke på de generella säkerhetsbestämmelser som kommer att gälla ter det sig enligt vår mening inte nödvändigt att särskilt föreskriva att hanteringen ska ske på säkra platser. Att så måste ske följer enligt vår bedömning redan av de generella säkerhetskraven enligt brottsdatalagen.

Vad gäller lufttrafikföretagen kommer dessas behandling av insamlade PNR-uppgifter och överföring till enheten för passagerarinformation att omfattas av de bestämmelser om konfidentiell behandling och datasäkerhet som finns i dataskyddsförordningen (se bl.a. artiklarna 3, 5.1 f och 32 i förordningen). Vi ser inte anledning att införa ytterligare reglering om detta i den nya lagen.

19.3 Bevarande av dokumentation och loggning

19.3.1 Direktivets bestämmelser

Av direktivets skäl 37 framgår att all behandling av PNR-uppgifter bör loggas eller dokumenteras i syfte att kontrollera att den är laglig och för att möjliggöra självövervakning och säkerställande av uppgifternas integritet och en säker behandling. Artikel 13.5 i direktivet behandlar frågan om bevarande av dokumentation. I bestämmelsen

anges att enheten för passagerarinformation ska bevara dokumentation om alla system och förfaranden för uppgiftsbehandling inom dess ansvarsområde. Dokumentationen ska minst innehålla

- a) namn och kontaktuppgifter för den organisatoriska enhet och den personal vid enheten för passagerarinformation som anförtrots behandlingen av PNR-uppgifter och de olika nivåerna av åtkomstbehörighet,
- b) begäran från behöriga myndigheter och enheter för passagerarinformation i andra medlemsstater,
- c) begäran om och överföring av PNR-uppgifter till ett tredjeland.

I bestämmelsen anges vidare att enheten för passagerarinformation på begäran ska göra all dokumentation tillgänglig för den nationella tillsynsmyndigheten.

Loggning är en säkerhetsåtgärd som innebär att behandlingshistorik sparas under en viss tid. Det är en teknisk funktion i systemet som fungerar automatiskt och som inte går att ändra eller påverka på annat sätt. Loggning fyller flera olika funktioner. Den ger den personuppgiftsansvarige information både om hur behandlingssystemen används och om externa och interna angrepp mot systemen. Loggning är således mycket viktig för det interna säkerhetsarbetet. Den ger också tillsynsmyndigheten nödvändig information för granskningen i efterhand av hur personuppgifter har behandlats.

Av artikel 13.6 framgår att medlemsstaterna ska se till att enheten för passagerarinformation för loggar över behandling av PNR-uppgifter. Enligt bestämmelsen ska loggar föras över åtminstone insamling, läsning, utlämning och radering. Loggarna över läsning och utlämning ska särskilt visa ändamål, datum och tidpunkt för sådan behandling och i möjligaste mån identitetsuppgifter för den person som har läst eller lämnat ut PNR-uppgifterna samt identitetsuppgifter för de personer som har mottagit uppgifterna. Loggarna ska uteslutande användas för kontroll och självövervakning, för att säkerställa dataintegritet och datasäkerhet och för revision. Enheten för passagerarinformation ska på begäran göra loggarna tillgängliga för den nationella tillsynsmyndigheten. Av artikeln framgår vidare att loggarna ska bevaras i fem år.

19.3.2 Nuvarande reglering

Personuppgiftsansvariga har enligt det nu gällande dataskyddsdirektivet ingen skyldighet att föra register över de behandlingar som de ansvarar för. I stället är de skyldiga att anmäla behandling av personuppgifter som är helt eller delvis automatiserad till tillsynsmyndigheten, som ska föra ett sådant register över de behandlingar som har anmälts till myndigheten. Någon anmälan till tillsynsmyndigheten behöver emellertid inte göras om den personuppgiftsansvarige utser ett personuppgiftsombud, som bl.a. ska ha till uppgift att föra register över de behandlingar som utförs av den personuppgiftsansvarige. Artiklarna har genomförts dels i 36, 37 och 39 §§ PUL, dels i personuppgiftsförordningen. Enligt 3 § 3 PUF gäller undantag från anmälningsskyldigheten bl.a. för behandling av personuppgifter som regleras genom särskilda föreskrifter i lag eller förordning. Myndigheternas registerförfattningar är sådana särskilda föreskrifter. Myndigheterna i rättskedjan är därmed inte anmälningsskyldiga och Datainspektionen för således inget register över dessa behandlingar. I t.ex. polisdatalagen anges dock att ett personuppgiftsombud ska utses och, genom hänvisning till 39 § PUL, att ombudet ska föra en förteckning över de behandlingar som utförs.

Som tidigare nämnts ställs krav på säkerhetsåtgärder i 31 § PUL. De anses även omfatta loggning och liknande åtgärder. Av Datainspektionens allmänna råd om säkerhet för personuppgifter framgår att det, beroende på känsligheten hos personuppgifterna, bör finnas en behandlingshistorik (logg) som sparas viss tid så att åtkomsten till uppgifterna kan kontrolleras. Enligt Datainspektionen bör en behandlingshistorik normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Historiken bör, beroende på hur känsliga personuppgifterna är, ange t.ex. läsning, ändring, utplåning eller kopiering av personuppgifter (Säkerhet för personuppgifter, Datainspektionens allmänna råd, november 2008, s. 22). Bestämmelser om loggning kan även finnas i myndighetsföreskrifter.

19.3.3 Brottsdatalagen

Det nya dataskyddsdirektivet innehåller skyldigheter för personuppgiftsansvariga att föra såväl register över viss personuppgiftsbehandling som loggar. Skyldigheten för de personuppgiftsansvariga att föra ett register över behandlingar föreslås av Utredningen om 2016 års dataskyddsdirektiv genomförs i brottsdataförordningen. I 3 kap. 3 § BDF anges att den personuppgiftsansvarige ska förteckna kategorier av behandlingar av personuppgifter som denne ansvarar för. Registret ska, förutom namnet på och kontaktuppgifter till den personuppgiftsansvarige, gemensamt personuppgiftsansvariga och dataskyddsombud, för varje kategori av behandling innehålla följande uppgifter.

1. Den rättsliga grunden för behandlingen.
2. Ändamålen med behandlingen.
3. Kategorier av tjänstemän som har tillgång till de personuppgifter som behandlas.
4. Kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut, även i tredjeland eller internationella organisationer.
5. Kategorier av registrerade som berörs av behandlingen.
6. Kategorier av personuppgifter som kan komma att behandlas.
7. Samlingar av överföringar av personuppgifter till tredjeland eller internationella organisationer.
8. Användning av profilering.
9. Om det är möjligt, tidsfrister för hur länge kategorierna av personuppgifter får behandlas.
10. Om det är möjligt, en allmän beskrivning av vilka säkerhetsåtgärder som har vidtagits.

En bestämmelse om loggning föreslås i 3 kap. 5 § BDL. Enligt bestämmelsen ska den personuppgiftsansvarige säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet. I 3 kap. 4 § BDF anges närmare vilka behandlingar som avses. Enligt bestämmelsen ska, i automatiserade behandlingssystem, behandlingar som

innebär insamling, ändring, läsning, utlämning, överföring till tredjeland eller internationella organisationer, sammanföring och radering av personuppgifter loggas. Loggarna över läsning och utlämning ska visa datum och tidpunkt för behandlingen och, så långt möjligt, vem som har läst eller lämnat ut personuppgifterna och vem som har fått ta del av personuppgifterna.

I det nya dataskyddsdirektivet anges att loggarna över läsning och utlämning även ska göra det möjligt att fastställa motiveringen för behandlingen (i den engelska versionen *justification*, i den danska *fastlägga begrundelsen*). Enligt Utredningen om 2016 års dataskyddsdirektiv kan inte skälen till att någon i ett visst fall tar del av eller lämnar ut en viss personuppgift fastställas automatiskt genom loggning. Någon sådan skyldighet att logga motiveringen till varför personuppgifter behandlas har därför inte förts in i förordningen (se SOU 2017:29 s. 308 f.).

Bestämmelserna om loggning i 3 kap. 5 § BDL och 3 kap. 4 § BDF föreslås inte behöva tillämpas på automatiserade behandlingssystem som inrättats före den 6 maj 2018 förrän den 1 maj 2023.

Tillsynsmyndigheten ska på begäran få upplysningar om och dokumentation av behandling av personuppgifter och säkerhets- och skyddsåtgärder från den personuppgiftsansvarige (5 kap. 5 § BDL).

19.3.4 Våra överväganden och förslag

Vårt förslag: Skyldigheten för Polismyndigheten att bevara viss dokumentation och att föra logg över vissa typer av behandlingar vid enheten för passagerarinformation ska regleras i förordning.

Enligt brottsdatalagen ska den personuppgiftsansvarige, i vårt fall Polismyndigheten, föra ett register över alla kategorier av verksamheter som den ansvarar för. Den information som ska bevaras i detta register är i många fall begränsat till kategorier av uppgifter. Enligt PNR-direktivet ska mer detaljerade uppgifter bevaras än de som anges i brottsdatalagen. Dessutom ska dokumentation bevaras om vissa faktiska enskilda behandlingar. En särskild bestämmelse om bevarande av dokumentation behöver därför föras in i vår reglering.

Enligt PNR-direktivet ska dokumentation bevaras om alla system och förfaranden för uppgiftsbehandling inom enheten för passagerarinformations ansvarsområde (i den engelska versionen *documentation relating to all processing systems and procedures*). Med dokumentation om alla system avses enligt vår tolkning såväl uppgifter om det system för behandling av PNR-uppgifter som ska byggas upp inom enheten, som uppgifter om vilka olika register eller andra uppgiftssamlingar som används vid de förhandsbedömningar som görs av PNR-uppgifterna. Med förfaranden avses enligt vår mening de på förhand fastställda kriterier som också får användas vid förhandsbedömningar av passagerare. Det bör av bestämmelsen framgå att dokumentation om behandlingen av PNR-uppgifter samt uppgifter om vilka register eller andra uppgiftssamlingar och på förhand fastställda kriterier som används inom enheten ska bevaras. Detta torde vara viktig information för att det i efterhand ska kunna göras bedömningar av om faktiskt utförda sökningar, analyser och annan behandling har skett lagenligt, exempelvis med användande av databaser som varit relevanta på det sätt som krävs enligt artikel 6.3 a eller med sökkriterier som utformats i enlighet med artikel 6.4.

Bestämmelsen bör också ange att namn och kontaktuppgifter till enheten och dess personal samt personalens olika nivåer av åtkomstbehörighet ska dokumenteras. Vidare bör det av bestämmelsen framgå att varje begäran från en behörig myndighet, eller en enhet för passagerarinformation i en annan medlemsstat, samt varje begäran om och överföring av PNR-uppgifter till ett tredjeland ska dokumenteras. Med en behörig myndighet torde enligt direktivet menas även sådana myndigheter som utsetts som behöriga i andra medlemsstater. Ett förtydligande i den frågan bör föras in i författningen.

Det anges inte i PNR-direktivet hur länge informationen ska bevaras. Vi ser för vår del ingen anledning att från dataskyddssynpunkt tidsbegränsa bevarandet av dokumentationen. För det fall det i dokumentationen ingår någon PNR-uppgift som har överförts till enheten från ett lufttrafikföretag, måste den dock raderas fem år efter insamlandet.

Utredningen om 2016 års dataskyddsdirektiv föreslår generella bestämmelser om loggning av sådana personuppgifter som behandlas i automatiserade behandlingssystem. Behandlingen av PNR-upp-

gifter inom enheten för passagerarinformation kommer av naturliga skäl att ske med hjälp av sådana automatiserade behandlingssystem. Den loggning som ska ske enligt de båda direktiven har därtill samma syften. Vidare omfattar uppräknningen av de uppgifter som ska loggas enligt brottsdataförordningen, förutom i ett fall, de uppgifter som ska loggas enligt PNR-direktivet. Den bestämmelse om loggning som föreslås införas i brottsdataförordningen kan således bli tillämplig även för den loggning som ska ske över enheten för passagerarinformations personuppgiftsbehandling.

Enligt PNR-direktivet ska loggarna över läsning och utlämning även visa *ändamålet* med behandlingen (i den engelska versionen *the purpose of such operations*). I det nya dataskyddsdirektivet anges i stället att motiveringen för behandlingen (i den engelska versionen *the justification*) ska loggas. Enligt vår bedömning är den språkliga skillnaden mellan uttrycken inte avsedd att innebära någon faktisk skillnad, utan är endast ett utfall av den kontext i vilken respektive bestämmelse återfinns. Utredningen om 2016 års dataskyddsdirektiv har angett att det inte är möjligt att genom automatisk loggning fastställa de exakta skälen till att någon i ett visst fall tar del av eller lämnar ut en viss personuppgift. Vi delar den bedömningen. Eftersom loggningen är ett automatiskt förfarande kan endast viss information om behandlingen dokumenteras. Det rör sig främst om datum och tidpunkt för behandlingen. Det kommer även att gå att få fram information om vem som behandlat personuppgifterna i och med att åtkomst till PNR-databasen kommer att kräva särskild behörighet och inloggning i de it-system som behövs.

Uppgifterna i PNR-databasen kommer att behandlas för ett flertal olika ändamål. Många gånger kommer uppgifterna också att behandlas för olika ändamål samtidigt. T.ex. kommer de uppgifter som en tjänsteman vid enheten för passagerarinformation hanterar från utfallet av en förhandsbedömning (artikel 6.2 a) regelmässigt också att utgöra ett led i den kontinuerliga analys av PNR-uppgifter som kommer att göras för att skapa nya sökkriterier mot vilka PNR-uppgifterna ska kontrolleras vid framtida förhandsbedömningar (artikel 6.2 c). Skälen till att någon i ett visst fall tar del av eller lämnar ut en viss personuppgift kan således inte fastställas automatiskt genom loggning. Den tolkning som Utredningen om 2016 års dataskyddsdirektiv har gjort, att bestämmelsen måste förstås så att man indirekt av annan loggad information kan dra vissa slutsatser

om anledningen till behandlingen, är den mest rimliga. Enligt vår bedömning behöver således inte PNR-direktivets krav på att loggarna särskilt ska visa ändamålen med läsning och utlämning av uppgifter införas i våra författningsförslag. Syftet med direktivets bestämmelse uppnås i stället genom den automatiska loggning som kan ske i förening med styrdokument, arbetsbeskrivningar, systemdokumentation och behörighetsadministration.

Vi föreslår således en bestämmelse som anger att Polismyndigheten ska se till att det utförs sådan loggning som anges i 3 kap. 4 § BDF över enheten för passagerarinformations personuppgiftsbehandling. Av bestämmelsen ska vidare framgå att loggarna ska bevaras i fem år.

PNR-systemet kommer att inrättas i tiden efter den 6 maj 2018. De föreslagna övergångsbestämmelserna i brottsdatalagen och den tillhörande förordningen blir därför inte tillämpliga.

Bestämmelserna om dokumentation och loggning kan, liksom de närmare bestämmelser som genomför motsvarande artiklar i det nya dataskyddsdirektivet, föras in på förordningsnivå.

Att dokumentationen och loggarna på begäran ska göras tillgängliga för tillsynsmyndigheten framgår av brottsdatalagen och behöver inte regleras särskilt i vår lag.

19.4 Personuppgiftsincident

19.4.1 Direktivets bestämmelser

PNR-direktivet innehåller bestämmelser om personuppgiftsincidenter. Personuppgiftsincident är ett nytt begrepp när det gäller dataskydd som används även i dataskyddsförordningen och det nya dataskyddsdirektivet. På informationssäkerhetsområdet är ordet incident emellertid etablerat. En personuppgiftsincident motsvarar till viss del vad som i dagligt tal brukar kallas dataintrång. Med personuppgiftsincident avses dock inte bara ett sådant avsiktligt intrång, utan även olyckshändelser och andra oavsiktliga händelser som får oönskade effekter, t.ex. brand. En incident kan inträffa genom yttre påverkan, men kan också bero på interna brister eller otillåtet handlande av någon inom organisationen. Det som är väsentligt för definitionen av personuppgiftsincident är inte hur

händelsen uppkommit eller vem som åstadkommit den utan effekten av den. (Jfr SOU 2017:29 s. 329.)

I artikel 13.8 i PNR-direktivet anges att om en personuppgiftsincident kan antas medföra ett avsevärt hot mot skyddet av den registrerades personuppgifter eller negativt påverka dennes integritet, ska medlemsstaterna se till att enheten för passagerarinformation utan onödigt dröjsmål informerar den registrerade och den nationella tillsynsmyndigheten för dataskydd om incidenten.

19.4.2 Nuvarande reglering

Det finns inga regler om personuppgiftsincidenter i personuppgiftslagen eller myndigheternas registerförfattningar. Incidenter behandlas inte heller i Datainspektionens allmänna råd om säkerhet. Däremot ska incidenter i it-system rapporteras av andra skäl. I 20 § första stycket förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap föreskrivs att en myndighet skyndsamt ska rapportera it-incidenter som inträffat i myndighetens it-system till Myndigheten för samhällsskydd och beredskap. Det gäller om incidenten allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

Rapporteringskyldigheten omfattar inte it-incidenter som enligt 10 a § säkerhetskyddsförordningen (1996:633) ska rapporteras till Säkerhetspolisen eller Försvarsmakten. Exempel på sådana incidenter är incidenter i informationssystem där hemliga uppgifter som rör rikets säkerhet behandlas eller i it-system som särskilt behöver skyddas mot terrorism. Säkerhetskyddsförordningen gäller för myndigheter, kommuner och landsting och för vissa bolag, föreningar, stiftelser och enskilda.

19.4.3 Brottsdatalagen

Personuppgiftsincident definieras i 1 kap. 6 § BDL som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.

Enligt 3 kap. 9 § ska den personuppgiftsansvarige anmäla en personuppgiftsincident till tillsynsmyndigheten senast 72 timmar efter det att denne fått kännedom om incidenten. Det gäller dock inte om incidenten rör nationell säkerhet. Anmälan behöver inte heller göras om det kan antas att personuppgiftsincidenten inte har medfört eller kommer att medföra risk för otillbörligt intrång i den registrerades personliga integritet. Utredningen om 2016 års dataskyddsdirektiv anger att någon anmälan t.ex. inte behöver göras om incidenten påverkat få personuppgifter som inte är av känslig art eller om skyddet för personuppgifterna påverkats under en så kort tid att obehörig åtkomst inte varit möjlig (se SOU 2017:29. 331).

Det föreslagna undantaget från anmälningsplikten för det fall personuppgiftsincidenten rör nationell säkerhet har sin grund i att it-incidenter som kan antas påverka säkerheten för hemliga uppgifter som rör rikets säkerhet enligt gällande rätt enbart ska anmälas enligt säkerhetsskyddsförordningen. Behovet av att skydda sådan information anses nämligen vara så viktigt att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av den. Även om den rapporteringen har ett annat syfte än rapporteringen av personuppgiftsincidenter, anser utredningen om 2016 års dataskyddsdirektiv att behovet av skydd för uppgifter som rör rikets säkerhet väger tyngre än behovet av att skydda enskilda från eventuella intrång i den personliga integriteten. Eftersom nationell säkerhet ligger utanför dataskyddsdirektivets tillämpningsområde har utredningen funnit att sådana personuppgiftsincidenter som ska anmälas enligt säkerhetsskyddsförordningen inte bör anmälas till tillsynsmyndigheten enligt brottsdatalagen. (Jfr SOU 2017:29 s. 332.) I 3 kap. 9 § BDF förtydligas att det i 10 a och 39 §§ säkerhetsskyddsförordningen framgår vilka incidenter som enligt 3 kap. 9 § första stycket BDL inte ska anmälas till tillsynsmyndigheten på grund av att de rör nationell säkerhet.

Information till enskilda registrerade regleras i 3 kap. 10 § BDL. Om en personuppgiftsincident som ska anmälas enligt 9 § har medfört eller kan antas medföra särskild risk för otillbörligt intrång i den registrerades personliga integritet ska den personuppgiftsansvarige utan onödigt dröjsmål underrätta den registrerade om incidenten. Enligt andra stycket gäller underrättelseskyldigheten inte om den personuppgiftsansvarige

1. har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder på de personuppgifter som påverkades av incidenten,
2. har säkerställt att det inte längre finns särskild risk för otillbörligt intrång i den personliga integriteten, eller
3. skulle behöva göra oproportionerliga ansträngningar för att underätta alla berörda.

I det senare fallet ska allmänheten, enligt tredje stycket, informeras eller en liknande åtgärd vidtas genom vilken de registrerade får nödvändig information.

I 3 kap. 11 § anges att den personuppgiftsansvarige får underlåta att lämna information enligt 10 § i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att personuppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. annans fri- och rättigheter skyddas.

3 kap. 11 § innebär att bestämmelser om sekretess och tystnadsplikt har företräde framför regeln om rätt till information vid personuppgiftsincidenter.

19.4.4 Våra överväganden

Vår bedömning: Bestämmelserna om personuppgiftsincidenter i brottsdatalagen bör i sin helhet tillämpas vid enheten för passagerarinformation. Personuppgiftsincidenter behöver därför inte regleras särskilt i den av oss föreslagna lagen.

PNR-direktivets bestämmelser om personuppgiftsincidenter avser personuppgiftsbehandling vid enheten för passagerarinformation. Bestämmelserna har sin motsvarighet i 3 kap. 9 § och 10 § första stycket BDL. De senare bestämmelserna kommer att gälla för eventuella personuppgiftsincidenter vid enheten för passagerarinformation i den mån det inte införs avvikande bestämmelser i den av oss föreslagna lagen.

I 3 kap. 9 § BDL anges visserligen att den personuppgiftsansvarige inte ska anmäla personuppgiftsincidenter som rör nationell säkerhet till tillsynsmyndigheten. Ett sådant undantag finns inte angivet i PNR-direktivet. Nationell säkerhet omfattas dock inte av unionsrätten. Som tidigare har angetts har Utredningen om 2016 års dataskyddsdirektivs funnit att behovet av skydd för uppgifter som rör rikets säkerhet väger tyngre än behovet av att skydda enskilda från eventuella intrång i den personliga integriteten. Vi instämmer i den bedömningen. Således finner inte heller vi att sådana personuppgiftsincidenter som ska anmälas enligt säkerhetsskyddsförordningen även bör anmälas till tillsynsmyndigheten. 3 kap. 9 § och 10 § första stycket BDL kan därmed tillämpas även för sådana personuppgiftsincidenter som kan komma att inträffa vid enheten för passagerarinformation.

PNR-direktivet saknar motsvarigheter till de undantag från underrättelseplikten som anges i 3 kap. 10 § andra och tredje stycket samt 11 § BDL. Enligt vår mening bör dock artikel 13.8 i PNR-direktivet ses som en huvudregel som inte fråntar undantagen i artikel 31 i det nya dataskyddsdirektivet från informationsskyldigheten. Dessa undantag och deras genomförande i brottsdatalagen är resultatet av rimliga och nödvändiga avvägningar. Om inte samma undantag skulle gälla för enheten för passagerarinformation skulle enheten åläggas orimliga krav som inte står i proportion till enskildas behov av information. Enligt vår mening bör därför undantagen i brottsdatalagen vara tillämpliga även för sådana personuppgiftsincidenter som kan komma att uppstå vid enheten för passagerarinformation. Särskilda bestämmelser om personuppgiftsincidenter behöver således inte föras in i den reglering som vi föreslår.

19.5 Dataskyddsbud

19.5.1 Direktivets bestämmelser

Enheten för passagerarinformation ska, enligt artikel 5.1 i PNR-direktivet, utse ett dataskyddsbud. Någon definition av begreppet dataskyddsbud finns inte i direktivet. Termen används dock även i dataskyddsförordningen och i det nya dataskyddsdirektivet. Dagens motsvarighet till dataskyddsbud är det som i personuppgiftslagen kallas för personuppgiftsbud. Ett personuppgiftsbud definieras i 3 § PUL som den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Enligt artikel 5.1 i PNR-direktivet ska det dataskyddsbud som utses av enheten för passagerarinformation ansvara för övervakningen av behandlingen av PNR-uppgifter och för genomförandet av relevanta skyddsåtgärder. I artikel 5.2 anges att medlemsstaterna ska förse dataskyddsbuden med de resurser som de behöver för att utföra sina uppgifter på ett effektivt och oberoende sätt. Vidare ska medlemsstaterna, enligt artikel 5.3, se till att en registrerad har rätt att kontakta dataskyddsbudet, i egenskap av enda kontaktpunkt, i alla frågor som rör behandlingen av den registrerades PNR-uppgifter.

Även i andra artiklar i direktivet finns bestämmelser som rör dataskyddsbudet. I artikel 6.7 anges att medlemsstaterna ska se till att dataskyddsbudet har åtkomst till alla uppgifter som enheten för passagerarinformation behandlar. Om dataskyddsbudet anser att behandlingen av vissa uppgifter inte har varit lagenlig, ska dataskyddsbudet hänskjuta ärendet till den nationella tillsynsmyndigheten.

Enligt artikel 11.4 ska dataskyddsbudet informeras varje gång en medlemsstat överför PNR-uppgifter till ett tredjeland enligt artikel 11. Även i artikel 11.2 kan dataskyddsbudet anses involverat, eftersom där anges att överföringar utan förhandssamtycke av den medlemsstat från vilken uppgifterna hämtades ska genomgå efterhandskontroll.

Vidare ska dataskyddsbudet, enligt artikel 12.3, informeras och genomföra en efterhandsutvärdering när en annan nationell myndighet än en rättslig sådan har lämnat tillstånd till utlämnande

av fullständiga PNR-uppgifter som har bevarats vid enheten för passagerarinformation under längre tid än sex månader.

19.5.2 Nuvarande reglering

Som nyss nämnts används i dag termen personuppgiftsombud för det som motsvarar dataskyddsbud. Personuppgiftslagen föreskriver ingen skyldighet att utse personuppgiftsombud. De behöriga myndigheterna kan dock enligt sina registerförfattningar vara skyldiga att ha personuppgiftsombud. Ett sådant krav finns t.ex. i polisdatalagen.

Enligt 38–40 §§ PUL ska personuppgiftsombud självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed och påpeka eventuella brister. Har personuppgiftsombuden anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter, och viktas inte rättelse efter påpekande, ska ombuden anmäla det till tillsynsmyndigheten. Personuppgiftsombud ska även i övrigt samråda med tillsynsmyndigheten. Personuppgiftsombuden ska också föra förteckning över de behandlingar som den personuppgiftsansvarige utför och som skulle ha omfattats av anmälningsskyldighet om inte ombudet hade funnits. Personuppgiftsombud ska dessutom hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

19.5.3 Brottsdatalagen

Ett dataskyddsbud definieras i 1 kap. 6 § BDL som en fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.

Enligt 3 kap. 13 § BDL ska den personuppgiftsansvarige utse ett eller flera dataskyddsbud och anmäla till tillsynsmyndigheten när dataskyddsbud utses och entledigas.

Dataskyddsbudets uppgifter framgår av 3 kap. 14 §. Där anges att dataskyddsbudet ska

1. självständigt kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge den personuppgiftsansvarige råd vid en konsekvensbedömning och kontrollera att den genomförs på ett korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och
5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

Om den personuppgiftsansvarige bryter mot bestämmelser för behandling av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet, enligt 3 kap. 15 §, anmäla det till tillsynsmyndigheten.

Enligt 3 kap. 14 § BDF ska den personuppgiftsansvarige säkerställa att dataskyddsombud ges möjlighet att delta i de frågor som rör skyddet av personuppgifter. Den personuppgiftsansvarige ska se till att dataskyddsombud kan utföra de uppgifter som anges i 3 kap. 14 och 15 §§ BDL genom att tillhandahålla nödvändiga resurser, ge tillgång till dokumentation om behandling av personuppgifter och vid behov medge åtkomst till personuppgifter som behandlas. Den personuppgiftsansvarige ska också se till att dataskyddsombud ges möjlighet att upprätthålla sin sakkunskap.

19.5.4 Våra överväganden och förslag

Våra förslag: Polismyndigheten ska utse ett dataskyddsombud för enheten för passagerarinformation. Dataskyddsombudet ska ha tillgång till alla uppgifter som behandlas vid enheten.

Det förs i lagen in bestämmelser som anger att dataskyddsombudet vid enheten för passagerarinformation ska ansvara för genomförandet av relevanta skyddsåtgärder. Vidare ska enskilda ha rätt att kontakta dataskyddsombudet i egenskap av enda kon-

taktpunkt i alla frågor som gäller behandling av dennes PNR-uppgifter enligt lagen. Om dataskyddsombudet anser att enheten för passagerarinformation bryter mot bestämmelser för behandling av PNR-uppgifter, ska han eller hon anmäla det till tillsynsmyndigheten.

Enligt brottsdatalagen ska den personuppgiftsansvarige utse ett eller flera dataskyddsombud. I PNR-direktivet anges i stället att enheten för passagerarinformation ska utse ett eget dataskyddsombud. Som tidigare framgått ska enheten för passagerarinformation placeras vid Polismyndigheten och ingå som en organisatorisk enhet i den myndigheten. Skyldigheten att utse enhetens dataskyddsombud bör i linje med den normala strukturen inom svensk förvaltning läggas på myndighetsnivå, dvs. på den nivå inom myndigheten som har det yttersta ansvaret för verksamheten vid enheten och som är personuppgiftsansvarig för enhetens behandling av personuppgifter. Enligt vår mening kan det knappast anses strida mot PNR-direktivet att utseendet av dataskyddsombud sker i en överordnad nivå i stället för på enheten. Det väsentliga med direktivets bestämmelser, som vi tolkar dem, är att det finns ett särskilt dataskyddsombud hos enheten som kan utföra de uppgifter som ett sådant ska ha enligt direktivet.

Skyldighet för Polismyndigheten att utse ett dataskyddsombud vid enheten för passagerarinformation bör föras in i vår reglering. Skyldigheten att anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas bör också åligga den personuppgiftsansvarige, dvs. Polismyndigheten. Detta framgår av brottsdatalagen och behöver inte regleras särskilt i vår lag.

Att det ska utses ett särskilt dataskyddsombud vid enheten för passagerarinformation hindrar, som vi ser det, inte i sig att detta ombud har sin anställning utanför enheten eller har fler uppdrag som dataskyddsombud. Huruvida detta är lämpligt eller möjligt torde bero på hur mycket arbete det kommer att visa sig att ombudet behöver lägga ned på sitt uppdrag, vilket är svårt att nu bedöma. Dessutom kan säkerhetsaspekten med tanke på känsligheten i informationen och ombudets obegränsade tillgång till uppgifterna tala mot en sådan lösning.

Dataskyddsombuds uppgifter enligt brottsdatalagen omfattar i stora delar även de uppgifter som ett dataskyddsombud ska ha enligt PNR-direktivet. Men det finns vissa skillnader.

Således menar vi att skyldigheten enligt artikel 5.1 i direktivet att övervaka behandlingen av PNR-uppgifter och genomförandet av relevanta skyddsåtgärder, i huvudsak omfattas av 3 kap. 14 § 1 BDL, dock att ombudet dessutom ska ansvara för genomförandet av relevanta skyddsåtgärder. Detta innebär, enligt vår tolkning, att det ankommer på ombudet vid sidan av Polismyndigheten att ta initiativ till och lämna riktlinjer och förslag på lämpliga skyddsåtgärder samt att också se till att dessa genomförs i praktiken på enheten. Detta bör regleras särskilt i den av oss föreslagna lagen.

Vidare omfattas uppgiften att vara kontaktpunkt för enskilda enligt artikel 5.3 i stort sett av bestämmelsen i 3 kap. 14 § 4 BDL, dock att det i PNR-direktivet framhålls att registrerade ska ha rätt att kontakta dataskyddsbudet i egenskap av kontaktpunkt i *alla* frågor som rör behandlingen av den registrerades PNR-uppgifter. Detta torde vara en inte oväsentlig utvidgning av ombudets uppgifter jämfört med brottsdatalagen. Vi tolkar nämligen artikel 5.3 på så sätt att enskilda ska ha en möjlighet att vända sig till och få hjälp eller information av dataskyddsbudet vid enheten även om behandlingen i det särskilda fallet helt eller delvis utförts av ett lufttrafikföretag, en behörig myndighet eller av utländska mottagare, dock bara såtillvida det varit fråga om en tillämpning av den lag vi föreslår. Detta föreslår vi ska uttryckas genom en bestämmelse i den nya lagen som gäller utöver 3 kap. 14 § 4 BDL. Om en enskild har invändningar mot t.ex. lufttrafikföretags insamling av PNR-uppgifter får denne däremot vända sig till vederbörande lufttrafikföretag. Likaså får en enskild vända sig till vederbörande dataskyddsbud utanför enheten om det handlar om användning av PNR-uppgifter i ett förundersökningsprotokoll. Dock bör enhetens dataskyddsbud i sådana fall kunna lotsa en missnöjd eller undrande enskild vidare till rätt kontaktpunkt.

Av bestämmelsen i 3 kap. 14 § BDF framgår att den personuppgiftsansvarige ska tillhandahålla nödvändiga resurser för att dataskyddsbudet ska kunna utföra sina uppgifter (jfr artikel 5.2 i PNR-direktivet). Den bestämmelsen kommer att gälla även för dataskyddsbudet vid enheten för passagerarinformation och behöver alltså inte regleras särskilt i våra förslag.

Enligt artikel 6.7 i PNR-direktivet ska dataskyddsbudet ha åtkomst till alla uppgifter som enheten för passagerarinformation behandlar. I brottsdataförordningen anges att den personuppgifts-

ansvarige ska säkerställa att dataskyddsbudet ges möjlighet att delta i de frågor som rör skyddet av personuppgifter. Vidare ska den personuppgiftsansvarige enligt bestämmelsen ge tillgång till dokumentation om behandling av personuppgifter och *vid behov* medge åtkomst till personuppgifter som behandlas. Enligt vår mening torde ett behov av tillgång till PNR-uppgifter ständigt föreligga för att dataskyddsbudet ska kunna utföra sina uppgifter. Man skulle därför kunna resonera som så att ytterligare reglering inte är nödvändig i frågan. Vi menar dock att ombudets kontinuerliga tillgång till uppgifterna är så pass central, för att lagligheten i behandlingen ska kunna kontrolleras, att frågan bör tas in i vår reglering. Vi föreslår alltså en bestämmelse som anger att dataskyddsbudet ska ges tillgång till alla uppgifter som behandlas vid enheten.

Vidare anges i artikel 6.7, som avser behandling av PNR-uppgifter vid enheten för passagerarinformation, att dataskyddsbudet ska hänskjuta en fråga till tillsynsmyndigheten om denne anser att behandlingen av vissa uppgifter inte har varit lagenlig. Enligt brottsdatalagen ska en anmälan till tillsynsmyndigheten i liknande situationer göras först om rättelse inte vidtas (3 kap. 15 §). Bestämmelsen i PNR-direktivet är således strängare än den föreslagna bestämmelsen i brottsdatalagen. Frågan får därför regleras särskilt i vår lag.

Frågor om information till dataskyddsbudet i vissa fall och om efterhandskontroll har behandlats i tidigare avsnitt, se avsnitt 15.5.4 och 17.3.4.

20 Enskildas rättigheter

20.1 Direktivets bestämmelser

En viktig aspekt av personuppgiftsskyddet är enskildas rätt att få veta hur deras personuppgifter behandlas. Information om den personuppgiftsbehandling som pågår är en förutsättning för att någon ska kunna kontrollera om behandlingen är författningsenlig och i övrigt kunna bevaka sina intressen. Enligt PNR-direktivets skäl 37 bör medlemsstaterna se till att passagerarna klart och tydligt informeras om insamlingen av PNR-uppgifterna och om sina rättigheter. Även i skäl 29 anges att medlemsstaterna bör se till att passagerare förses med korrekt, lättåtkomlig och lättbegriplig information om insamlingen av PNR-uppgifter och överföringen av dessa uppgifter till enheten för passagerarinformation samt om sina rättigheter i egenkap av registrerade.

Direktivet anger att passagerarna ska tillerkännas vissa grundläggande rättigheter vid behandlingen av deras personuppgifter. Enligt artikel 13.1 ska medlemsstaterna föreskriva att alla passagerare vid all behandling av personuppgifter i enlighet med direktivet har samma rätt till skydd av sina personuppgifter, rätt till åtkomst, rättelse, radering och begränsning samt rätt till ersättning och tillgång till rättsmedel som fastställs i unionsrätten och nationell rätt och för genomförande av artiklarna 17, 18, 19 och 20 i dataskyddsrambeslutet. Enligt PNR-direktivet ska således de angivna artiklarna i dataskyddsrambeslutet tillämpas även vid sådan personuppgiftsbehandling som omfattas av direktivet.

20.2 Rätten till information

20.2.1 Dataskyddsrambeslutet

En enskild registrerads rätt till information om behandlingen regleras i dataskyddsrambeslutet i artiklarna 16 och 17. PNR-direktivet hänvisar dock endast till artikel 17. Enligt den bestämmelsen har den registrerade rätt att *på begäran* åtminstone få bekräftat av den registransvarige eller den nationella tillsynsmyndigheten om uppgifter rörande honom eller henne har överförts eller gjorts tillgängliga och i så fall till vilka mottagare eller mottagarkategorier (artikel 17.1.a), eller en bekräftelse från tillsynsmyndigheten att alla nödvändiga kontroller har utförts (artikel 17.1.b). Artikel 17.2 anger för vilka syften undantag får göras från reglerna om den registrerades rätt till information. Sådana undantag får göras bl.a. om begränsningen är nödvändig för att hindra obstruktion och skydda allmän eller nationell säkerhet. Artikel 17.3 föreskriver att en vägran att lämna information till den enskilde enligt huvudregeln ska vara skriftlig och innehålla skälen för vägran. Om vägran att lämna information grundas på något av undantagen i artikel 17 behöver några skäl inte anges. Den registrerade ska underrättas om möjligheten att överklaga till den nationella tillsynsmyndigheten, en rättslig myndighet eller till domstol.

Vid genomförandet av dataskyddsrambeslutet ansågs artikel 17.1 motsvaras av 26 § PUL, som ställer mer långtgående krav på vilken information som ska lämnas. Undantagsgrunderna i 8 a och 27 §§ PUL ansågs i allt väsentligt motsvara de undantagsgrunder som anges i artikel 17.2. Bestämmelserna i artikel 17.3 ansågs inte kräva några lagstiftningsåtgärder. (Se prop. 2012/13:73 s. 90 ff.) Bestämmelserna i personuppgiftslagen behandlas närmare i avsnitt 6.3.2.

20.2.2 Brottsdatalagen

Som har angetts i tidigare avsnitt får PNR-direktivets hänvisningar till dataskyddsrambeslutet läsas som hänvisningar till det nya dataskyddsdirektivet, som föreslås genomföras i brottsdatalagen. Enskildas rätt till information behandlas i 4 kap. brottsdatalagen. Enligt 4 kap. 1 § ska den personuppgiftsansvarige göra viss allmän information tillgänglig för registrerade. Informationen omfattar den personuppgiftsansvariges identitet och kontaktuppgifter, dataskydds-

ombudet kontaktuppgifter, ändamålen med behandlingen, rätten att begära att få information om behandling av personuppgifter och att få del av dem, rätten att begära rättelse, radering eller begränsning av behandlingen samt möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifter till den.

Om den personuppgiftsansvarige anser att en registrerad behöver ytterligare information för att kunna ta tillvara sina rättigheter ska, enligt 4 kap. 2 §, den personuppgiftsansvarige på eget initiativ även lämna viss personrelaterad information. Denna information omfattar den rättsliga grunden för behandlingen, kategorier av mottagare av personuppgifterna, hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det samt övrig nödvändig information. Vid bedömningen av om övrig nödvändig information ska lämnas ut ska det särskilt beaktas om personuppgifterna samlats in utan den registrerades vetskap.

I 4 kap. 3 § anges vilken information som ska lämnas till en registrerad *på begäran*. Enligt bestämmelsen ska den personuppgiftsansvarige till den som begär det utan dröjsmål lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och även få viss skriftlig information om behandlingen. Den skriftliga informationen ska omfatta

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån uppgifterna kommer,
3. den rättsliga grunden för behandlingen,
4. ändamålen med behandlingen,
5. mottagare eller kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
6. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det,
7. rätten att begära rättelse, radering eller begränsning av behandlingen, och
8. möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Sökanden behöver inte få del av personuppgifter som han eller hon har tagit del av, om det inte begärs. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

I 4 kap. 5 § anges att rätten till information får begränsas i lag, annan författning eller i beslut som har meddelats med stöd av författning. En sådan begränsning får endast göras av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. annans fri- och rättigheter skyddas.

Om dessa förutsättningar är uppfyllda är den personuppgiftsansvariga inte heller skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandling.

Informationsskyldigheten enligt 4 kap. 3 § gäller som huvudregel inte heller för personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller i minnesanteckningar eller liknande (4 kap. 6 §).

Om en begäran om information om att personuppgifter behandlas eller att få del av dem är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den (4 kap. 7 §).

Information ska som huvudregel lämnas utan avgift. Om någon begär information eller uppgifter enligt 3 § oftare än en gång per år får den personuppgiftsansvarige dock ta ut en rimlig avgift eller avslå begäran (4 kap. 7 och 12 §§).

I brottsdataförordningen anges krav på utformningen av bl.a. den information som lämnas till enskilda. Informationen ska vara lättillgänglig och lättbegriplig och lämnas i lämplig form (4 kap. 1 §). En enskilds begäran om att ta del av information ska göras skriftligen hos den personuppgiftsansvarige (4 kap. 2 §).

20.2.3 Dataskyddsförordningen

Lufttrafikföretagen hör inte till den brottsbekämpande sektorn. För dem kommer således inte bestämmelserna om personuppgiftsbehandling enligt dataskyddsrambeslutet eller det nya dataskyddsdirektivet att vara tillämpliga. Lufttrafikföretagens personuppgiftsbehandling omfattas i stället i dag av tillämpningsområdet för det nu gällande dataskyddsdirektivet¹, som genomförts i svensk rätt genom personuppgiftslagen. Som tidigare angetts ska det nu gällande dataskyddsdirektivet ersättas av dataskyddsförordningen, som ska börja tillämpas den 25 maj 2018.

Enligt artikel 13.2 i PNR-direktivet ska detta inte påverka tillämpligheten av det nu gällande dataskyddsdirektivet när det gäller lufttrafikföretagens behandling av personuppgifter. PNR-direktivets hänvisning till dataskyddsdirektivet får, med hänsyn till ovanstående, läsas som en hänvisning till dataskyddsförordningen.

Enskildas rätt till information regleras i artiklarna 12–14 i dataskyddsförordningen. Av artikel 12 framgår att den information som den personuppgiftsansvarige lämnar ska vara koncis, klar och tydlig, begriplig och lätt tillgänglig. Informationen ska tillhandahållas skriftligt eller i någon annan lämplig form. Om den registrerade begär det kan informationen lämnas muntligt. Informationen ska normalt tillhandahållas kostnadsfritt.

I artikel 13 anges vilken information som ska tillhandahållas om personuppgifter har samlats in från den registrerade. Den information som lufttrafikföretagen i sådant fall ska tillhandahålla omfattar bl.a. identitet och kontaktuppgifter för den personuppgiftsansvarige och eventuellt dataskyddsombud, ändamålen med behandlingen, den period under vilken personuppgifterna kommer att lagras, rätten att begära tillgång till uppgifterna, rätten till rättelse, radering eller begränsning av behandlingen av uppgifterna och rätten att inge klagomål till en tillsynsmyndighet. Den information som ska lämnas ska även omfatta vilka mottagare eller kategorier av mottagare som i förekommande fall ska ta del av personuppgifterna.

Om personuppgifterna i stället har lämnats till lufttrafikföretagen från någon annan, exempelvis en resebyrå eller researrangör,

¹ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

anges vilken information som ska lämnas i artikel 14. Bestämmelsen innehåller ungefärligen samma uppgifter som föregående artikel. Dock ska informationen i dessa fall även omfatta uppgifter om bl.a. varifrån personuppgifterna kommer samt information om de kategorier av personuppgifter som behandlingen gäller. Även i dessa fall ska den personuppgiftsansvarige lämna uppgift om mottagare eller de kategorier av mottagare som ska ta del av personuppgifterna. Informationen ska lämnas inom en rimlig tid efter det att personuppgifterna erhållits, dock senast inom en månad. Om ett utlämnande till en annan mottagare förutses, ska informationen lämnas senast när personuppgifterna lämnas ut för första gången. Information som den registrerade redan förfogar över behöver inte lämnas. Informationen behöver inte heller lämnas om erhållande eller utlämnande av uppgifterna följer av unionsrätten eller nationell rätt som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen.

20.2.4 Våra överväganden och förslag

Vårt förslag: Lufttrafikföretagen ska informera passagerarna om överföringen av PNR-uppgifter till enheten för passagerarinformation och om syftet med överföringen.

Vår bedömning: Ytterligare bestämmelser om enskildas rätt till information behöver inte föras in i lagen.

Rätten till information om insamlingen av PNR-uppgifter och överföringen av dessa uppgifter till enheten för passagerarinformation

Enligt skälen till PNR-direktivet ska medlemsstaterna se till att passagerarna förses med korrekt, lättåtkomlig och lättbegriplig information om insamlingen av PNR-uppgifter och om överföringen av dessa uppgifter till enheten för passagerarinformation. Vem som ska lämna denna information till passagerarna anges inte. Informationen skulle således kunna lämnas såväl av lufttrafikföretagen som av enheten för passagerarinformation. Kommissionen har angett att den

mest praktiska lösningen vore om informationen lämnades av lufttrafikföretagen och att det därför är den mest önskvärda lösningen.²

Lufttrafikföretagen ska enligt dataskyddsförordningen tillhandahålla information om sin egen insamling av PNR-uppgifter. Informationsskyldigheten omfattar även vilka mottagare eller kategorier av mottagare som ska ta del av personuppgifterna. Således följer det redan av dataskyddsförordningen att lufttrafikföretagen ska informera sina passagerare om att de insamlade PNR-uppgifterna kommer att överföras till enheten för passagerarinformation. Den skyldigheten gäller dock inte för det fall lufttrafikföretagen erhållit PNR-uppgifterna från en researrangör eller resebyrå, dvs. i fall då lufttrafikföretagen inte samlat in uppgifterna från den registrerade själv, eftersom lufttrafikföretagen kommer att överföra uppgifterna till följd av en författningsreglerad skyldighet att göra det (jfr artikel 14.5 c i förordningen). Förordningen ställer vidare inga krav på att informationen i denna fråga även ska innehålla skälen till överföringen, i detta fall att den följer av ett författningsreglerat åläggande som genomför ett EU-direktiv om användning av PNR-uppgifter för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

Vi anser att lufttrafikföretagen bör åläggas en skyldighet att informera sina passagerare om överföringen till enheten för passagerarinformation alldeles oavsett om PNR-uppgifterna samlats in direkt från passagerare eller via en resebyrå eller researrangör. Vi föreslår därför detta.

Endast en upplysning om att PNR-uppgifterna kommer att överföras till enheten för passagerarinformation torde dock för den enskilde resenären framstå som svårförståelig. För att det tydligt ska framgå för passagerarna varför deras personuppgifter överförs bör de, enligt vår mening, även informeras om lufttrafikföretagens skyldigheter enligt PNR-direktivet och om direktivets syfte. Det bör därför i vår lag föras in en bestämmelse som anger att passagerarna ska informeras om överföringen av PNR-uppgifter till enheten för passagerarinformation och om skälen till överföringen.

Lufttrafikföretagen lämnar redan i dag liknande information till sina resenärer inför resor till länder som kräver tillgång till PNR-

² COM, Report of the third meeting on the implementation of the PNR Directive, 12 December 2016.

uppgifter. Vi delar kommissionens uppfattning att den mest praktiska lösningen vore om lufttrafikföretagen ålades att lämna även den här aktuella informationen till sina passagerare. Således föreslår vi att informationsskyldigheten ska åläggas lufttrafikföretagen.

Informationen kan lämpligen lämnas tillsammans med den övriga information som lufttrafikföretagen ska tillhandahålla enligt dataskyddsförordningen. Informationen kan framgå av flygbiljetten eller av lufttrafikföretagens hemsidor, eller, allra helst, på båda sätten.

Ett åläggande för lufttrafikföretagen att lämna denna information påverkar inte tillämpligheten av dataskyddsförordningen. Åläggandet medför inte heller någon inskränkning i Polismyndighetens skyldigheter enligt brottsdatalagen att såsom personuppgiftsansvarig lämna information om den personuppgiftsbehandling som kommer att ske vid enheten för passagerarinformation.

Rätten till information om personuppgiftsbehandlingen vid enheten för passagerarinformation och behöriga myndigheter

Efter det att PNR-uppgifterna har överförs till enheten för passagerarinformation kommer enskildas rätt till information om personuppgiftsbehandlingen i stort att styras av bestämmelserna i det nya dataskyddsdirektivet så som detta genomförts i Sverige.

Som tidigare har framgått hänvisar PNR-direktivet till vissa bestämmelser i det nu gällande dataskyddsrambeslutet. Enligt direktivets skäl 27 bör dock hänvisningarna läsas som hänvisningar även till de framtida bestämmelser som kommer att ersätta dessa. Det nya dataskyddsdirektivet går i vissa avseenden längre än dataskyddsrambeslutet i bemärkelsen att det ålägger personuppgiftsansvariga fler skyldigheter och enskilda förstärkta rättigheter. Det vore i och för sig möjligt att vid genomförandet av PNR-direktivet lägga sig på den något lägre nivå av rättigheter för enskilda som rambeslutet anger. PNR-direktivet innebär dock en så pass känslig personuppgiftshantering att det vore helt oproportionerligt om enskilda skulle ges ett sämre skydd än vad som annars gäller på det brottsbekämpande området till följd av det nya dataskyddsdirektivet. Enligt vår tolkning bör således dataskyddsdirektivets mer långtgående krav gälla och inte rambeslutets. Vi menar att skäl 27 i PNR-direktivet ligger i linje med vår uppfattning i denna fråga.

Det nya dataskyddsdirektivets bestämmelser om enskildas rätt till information föreslås genomföras i 4 kap. 1–7 §§ BDL och i den tillhörande förordningen. I 4 kap. 12 § BDL finns en bestämmelse om avgifter för informationen. Samtliga angivna bestämmelser är allmänt formulerade och kan tillämpas även för behandlingen av PNR-uppgifter.

Brottsdatalagen kommer att gälla utöver den av oss föreslagna lagen beträffande behandling som utförs vid enheten för passagerarinformation eller vid sådana behöriga myndigheter som i sin verksamhet har att tillämpa brottsdatalagen, dvs. Polismyndigheten, Ekobrottsmyndigheten och Tullverket som det ser ut i nuläget.

Som tidigare nämnts föreslås Säkerhetspolisen i allt väsentligt inte omfattas av brottsdatalagens tillämpningsområde. Däremot kommer det inom kort föreslås särreglering för Säkerhetspolisen. Det är rimligt att tro att det i det sammanhanget kommer att föreslås en generell lösning för frågan om enskildas rätt till information gällande Säkerhetspolisens verksamhet. Vi ser ingen anledning att nu föregripa det arbetet med någon särskild lösning för Säkerhetspolisens del. Vi gör samma bedömning vad gäller Försvarmakten vars författningsreglering av personuppgiftsbehandlingen inom försvarsunderrättelseverksamheten och den militära säkerhetstjänsten för närvarande utreds. Det är alltså vår sammantagna bedömning att särskilda bestämmelser om enskildas rätt till information från berörda myndigheter inte bör föras in i vårt lagförslag.

Det bör påpekas att skyldigheten att lämna ut uppgifter i många fall kommer att begränsas av bl.a. bestämmelserna i offentlighets- och sekretesslagen.

20.3 Rätt till rättelse, radering eller begränsning av behandlingen av uppgifter

20.3.1 Dataskyddsrambeslutet

I artikel 18 i dataskyddsrambeslutet anges att en registrerad ska ha rätt att förvänta sig att en registeransvarig fullgör sina skyldigheter enligt rambeslutet att rätta, radera eller blockera personuppgifter. Medlemsstaterna ska fastställa hur den registrerade ska kunna göra anspråk på rätten till rättelse, radering och blockering. Om den registeransvariga vägrar att rätta, radera eller blockera uppgifter måste

vägran meddelas skriftligen och den registrerade informeras om möjligheterna att anföra klagomål eller begära prövning. När ett klagomål eller en begäran prövats ska den registrerade informeras om huruvida den registeransvarige handlat korrekt eller inte.

Vid genomförandet av rambeslutet ansågs bestämmelsen inte kräva några ändringar eller tillägg i personuppgiftslagen (se prop. 2012/13:73 s. 95 f.), där frågan behandlas i 28 §. Se om den bestämmelsen i avsnitt 6.3.2.

20.3.2 Brottsdatalagen

Artikel 16 i det nya dataskyddsdirektivet innehåller bestämmelser om registrerades rätt till rättelse eller radering av personuppgifter och begränsning av behandling. Artikeln föreslås genomföras genom 4 kap. 9 och 10 §§ BDL.

I 4 kap. 9 § BDL anges att den personuppgiftsansvarige på begäran av den registrerade utan onödigt dröjsmål ska *rätta* eller *komplettera* personuppgifter som rör honom eller henne om de är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Om den personuppgiftsansvarige inte kan fastställa att personuppgifterna är korrekta ska behandlingen i stället utan onödigt dröjsmål *begränsas*.

I 4 kap. 10 § första stycket BDL anges att den personuppgiftsansvarige, på begäran av den registrerade, utan onödigt dröjsmål ska *radera* personuppgifter som rör honom eller henne om de behandlas i strid med vissa särskilt angivna bestämmelser i lagen som innehåller grundläggande krav på behandling av personuppgifter eller lagens bestämmelser om behandling av känsliga personuppgifter, rättslig grund eller ändamål med behandlingen. Detsamma gäller om radering krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse. Uttrycket rättslig förpliktelse syftar på en skyldighet som åligger den personuppgiftsansvarige enligt brottsdatalagen, den behöriga myndighetens registerförfattning eller andra författningar med bestämmelser om personuppgiftsbehandling. Med radering avses detsamma som utplåning. För att radera personuppgifter i allmänna handlingar krävs författningsstöd för gallring. Utrymmet för att radera personuppgifter i allmänna handlingar på grund av att person-

uppgifterna inte har behandlats författningsenligt torde därför vara begränsat (jfr bl.a. SOU 2015:39 s. 529 och 573 f.).

Om förutsättningarna för att radera personuppgifter är uppfyllda, men uppgifterna behöver finnas kvar som bevisning, ska den personuppgiftsansvarige på begäran av den registrerade i stället utan onödigt dröjsmål *begränsa behandlingen* av dem (4 kap. 10 § andra stycket). Med begränsning av behandling avses enligt direktivet en markering av lagrade personuppgifter i syfte att begränsa behandlingen av dem i framtiden. Dagens motsvarighet till begränsning av behandling är blockering.

Det är den personuppgiftsansvarige som avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandling (4 kap. 11 §).

Som tidigare framgått innehåller brottsdataförordningen flera bestämmelser om enskildas rättigheter. Här framgår att beslut gällande enskildas rättigheter ska vara skriftliga och att beslut som går den registrerade emot ska motiveras, om inte annat angetts i lagen (4 kap. 3 §). Vidare anges en rad situationer då den registrerade eller andra ska underrättas om beslut och om möjligheten att lämna in klagomål till tillsynsmyndigheten m.m. Bl.a. ska en underrättelse alltid skickas på den personuppgiftsansvariges eget initiativ till den myndighet som har mottagit en personuppgift, för det fall denna uppgift senare har rättats eller raderats eller behandlingen av den har begränsats (4 kap. 8 § andra stycket).

20.3.3 Våra överväganden och förslag

Vårt förslag: Det förs i lagen in en bestämmelse som anger att rätten till radering eller begränsning av behandling av personuppgifter enligt 4 kap. 10 § BDL ska gälla vid behandling i strid mot bestämmelserna i vår lag om otillåten behandling av PNR-information, förbud mot behandling av känsliga personuppgifter samt skyldigheten att gallra PNR-uppgifter i PNR-databasen efter fem år. Sådana beslut kan överklagas till allmän förvaltningsdomstol enligt 7 kap. 2 § BDL.

Vår bedömning: Ytterligare bestämmelser om enskildas rätt till rättelse, radering eller begränsning av behandling av uppgifter behöver inte föras in i lagen.

Som konstaterats i avsnitt 20.2.4 bör de nationella bestämmelser om enskildas rättigheter som genomför det nya dataskyddsdirektivet fullt ut vara tillämpliga vid sådan personuppgiftsbehandling som regleras i den av oss föreslagna lagen.

Brottsdatalagen innehåller bestämmelser om den registrerades rätt till rättelse, radering och begränsning av behandling av personuppgifter i 4 kap. 9–11 §. Bestämmelserna i 4 kap. 9 och 11 §§ är formulerade på ett sådant allmängiltigt sätt att de blir direkt tillämpliga vid personuppgiftsbehandling även enligt vår lag, för det fall inget annat anges. Någon hänvisning till dessa bestämmelser behöver därför inte föras in i vårt lagförslag.

4 kap. 10 § anger att den registrerade har rätt till radering eller begränsning av personuppgifter om uppgifterna har behandlats i strid mot vissa angivna bestämmelser i brottsdatalagen. De angivna bestämmelserna är av så generell natur att överträdelser av dem bör medföra en rätt för registrerade till radering eller begränsning även vid personuppgiftsbehandling enligt vår lag. Enligt vår mening bör en registrerad dock också ha rätt till radering eller begränsning av behandling av personuppgifter vid överträdelser av vissa centrala bestämmelser enligt vårt lagförslag. En sådan rättighet bör förekomma när personuppgifter har behandlats i strid mot vår lags förbud mot behandling av känsliga personuppgifter, lagens begränsning i fråga om vad för slags brottslighet som uppgifterna får användas för samt förpliktelsen att gallra PNR-uppgifterna slutligt efter fem år. Vi föreslår därför att det i lagen förs in en bestämmelse som anger att 4 kap. 10 § BDL ska tillämpas vid behandling i strid mot de angivna bestämmelserna i vår lag. Vidare föreslår vi att det förs in en upplysning om att det i 7 kap. 2 § BDL föreskrivs att sådana beslut kan överklagas till allmän förvaltningsdomstol (se nedan i avsnitt 20.5.2).

Så som vi formulerar bestämmelsen, kommer den att vara tillämplig alldeles oavsett vem som i ett enskilt fall har utfört den felaktiga behandlingen; ett lufttrafikföretag, enheten för passagerarinformation eller en behörig myndighet. I praktiken torde den dock bara bli aktuell att tillämpa för de myndigheter som annars omfattas av

brottsdatalagens tillämpningsområde. Alldeles oavsett detta förutser vi dock inte att det kommer att uppstå några tillämpningsproblem med anledning av brottsdatalagbestämmelsens i viss mån vidgade tillämpningsområde. När det gäller Säkerhetspolisen och Försvarsmakten gör vi vidare motsvarande bedömningar som ovan i avsnitt 20.2.4 och ser således inte skäl till att i detta lagstiftningsarbete föreslå någon särreglering vad avser motsvarigheter till 4 kap. 9 och 11 §§ BDL.

20.4 Rätt till ersättning

20.4.1 Dataskyddsrambeslutet

Enligt artikel 19 i dataskyddsrambeslutet har var och en som lidit skada till följd av otillåten behandling av personuppgifter eller någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av rambeslutet, rätt till ersättning av den registeransvarige, eller av en annan myndighet, för den skada han eller hon lidit. Det är inte möjligt att undgå skadeståndsansvar genom att åberopa att behandlingen avser uppgifter som har överförts från annat land och som var felaktiga redan vid överföringen.

Vid genomförandet av dataskyddsrambeslutet ansågs kraven i rambeslutet vara uppfyllda genom skadeståndsbestämmelsen i 48 § första stycket PUL. Dock ansågs inte den jämkningsmöjlighet som finns i den bestämmelsens andra stycke förenlig med rambeslutet. Därför infördes en bestämmelse i 10 § lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen som anger att 48 § andra stycket PUL inte gäller för uppgifter som har överförts vid sådant polisiärt eller straffrättsligt samarbete som rambeslutet omfattar.

20.4.2 Brottsdatalagen

Enligt 7 kap. 1 § BDL ska den personuppgiftsansvarige ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med brottsdatalagen, eller föreskrifter som har meddelats i anslutning till den, har orsakat. Bestämmelsen har utformats med motsvarande bestämmelse

i personuppgiftslagen som mönster. Någon möjlighet till jämkning förekommer dock inte.

20.4.3 Våra överväganden och förslag

Vårt förslag: Det förs i lagen in en bestämmelse som innebär att 7 kap. 1 § BDL om skadestånd ska gälla också i fråga om behandling av personuppgifter i strid med bestämmelser enligt den nya lagen eller föreskrifter som meddelats med stöd av lagen.

Bestämmelsen om skadestånd enligt brottsdatalagen kommer att gälla om personuppgifter behandlas i strid med den lagen eller föreskrifter som har meddelats i anslutning till den. För att bestämmelsen i brottsdatalagen även ska vara tillämplig vid behandling av personuppgifter i strid med den av oss föreslagna lagen eller med föreskrifter som meddelats med stöd av den lagen behöver en hänvisning till bestämmelsen föras in i vårt lagförslag.

Vi föreslår därför att en hänvisning till 7 kap. 1 § BDL förs in i den av oss föreslagna lagen. Den ska dock bara avse sådana överträdelser av bestämmelser som avser att ge skydd för personuppgifter. Om ett lufttrafikföretag bryter mot bestämmelserna i 2 kap. genom att inte skicka PNR-uppgifter till enheten för passagerarinformation eller när enheten för passagerarinformation bryter mot sin skyldighet att besvara förfrågningar från behöriga myndigheter eller fullgöra sina förpliktelser om informationsutbyte med andra medlemsstater ska givetvis inte skadeståndsbestämmelsen i 7 kap. 1 § BDL tillämpas. Detta ska framgå i lagen genom att hänvisningen till 7 kap. 1 § BDL endast ska avse behandling i strid med bestämmelser i lagen eller förordningen till skydd för personuppgifter.

20.5 Rätt till rättsmedel

20.5.1 Dataskyddsrambeslutet

Enligt artikel 20 i dataskyddsrambeslutet ska den registrerade ha rätt att inför domstol föra talan mot kränkningar av sådana rättigheter som skyddas av den tillämpliga lagstiftningen. En liknande skrivning i det nu gällande dataskyddsdirektivet medförde inte några särskilda

lagstiftningsåtgärder vid personuppgiftslagens införande. Rambeslutets bestämmelser om överklagande ansågs inte heller kräva några lagstiftningsåtgärder (se prop. 2012/13:73 s. 97 f.).

20.5.2 Brottsdatalagen

Rätten att vid allmän domstol föra talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde om den registrerades rättigheter har kränkts genom personuppgiftsbehandlingen kräver, enligt Utredningen om 2016 års dataskyddsdirektiv, inga lagstiftningsåtgärder. Den möjlighet enskilda har att väcka talan vid allmän domstol i den ordning som gäller för tvistemål anses vara tillräcklig (se SOU 2017:29 s. 529 f.).

Enligt brottsdatalagen ska dock beslut i fråga om rättelse, komplettering, radering eller begränsning av behandlingen av personuppgifter, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, få överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad, att ta ut avgift för att lämna sådan information eller att inte medge omprövning av ett automatiserat beslut. Vid överklagande till kamrarrätten ska, på samma sätt som i dag, krävas prövningstillstånd. Beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän ska inte kunna överklagas (7 kap. 2 §).

En registrerads rätt att lämna in klagomål till en tillsynsmyndighet om han eller hon anser att hans eller hennes personuppgifter har behandlats felaktigt har inte ansetts kräva några lagstiftningsåtgärder. Däremot föreslås det införas en ny möjlighet för en registrerad att föra en s.k. dröjsmålstalan mot tillsynsmyndigheten. Enligt förslaget ska tillsynsmyndigheten inom tre månader från den dag ett klagomål kom in till myndigheten lämna skriftligt besked om den avser att utöva tillsyn eller i ett särskilt beslut avslå begäran (5 kap. 9 §). Om tillsynsmyndigheten avslår den registrerades begäran om besked om huruvida tillsyn kommer att utövas, får han eller hon överklaga beslutet till allmän förvaltningsdomstol. Om domstolen bifaller ett överklagande av ett avslagsbeslut, ska den förelägga tillsynsmyndigheten att, inom den tid som domstolen bestämmer, lämna den registrerade besked om tillsyn kommer att utövas. Annars ska dom-

stolen avslå överklagandet. Domstolens beslut får inte överklagas. (Se 7 kap. 3 §.)

I 7 kap. 4 § föreskrivs att tillsynsmyndighetens beslut i andra frågor än de som regleras i 3 § får överklagas. Det är framför allt fråga om beslut som tillsynsmyndigheten har fattat med stöd av sina korrigerande befogenheter. Det kan t.ex. vara beslut om rättelse och radering. Det kan även vara beslut om sanktionsavgift.

Några andra beslut än de som uttryckligen anges i brottsdatalagen ska inte få överklagas (7 kap. 5 §).

20.5.3 Våra överväganden och förslag

Vår bedömning: Ytterligare bestämmelser om enskildas rätt till rättsmedel behöver inte föras in i lagen.

Bestämmelser om överklagande har tagits in i 7 kap. 2–5 §§ BDL. Att bestämmelsen i 7 kap. 2 §, som behandlar möjligheten att överklaga vissa myndighetsbeslut, bör vara tillämplig även vid överklagande av sådana beslut om radering eller begränsning av uppgifter som fattas med stöd av vår lag har vi redan angett ovan.

Någon hänvisning till bestämmelsen om dröjsmålstalan i 7 kap. 3 § är inte nödvändig för att bestämmelsen ska bli tillämplig för sådan behandling som avses i vår lag. Vidare kommer tillsynsmyndigheten inte att fatta några beslut enligt vår lag utan endast enligt bestämmelserna i brottsdatalagen. Någon hänvisning till 7 kap. 4 § BDL är därför inte nödvändig i vår lag. Inte heller ser vi det som befogat att hänvisa till 7 kap. 5 § BDL i vår lag.

När det gäller Säkerhetspolisen och Försvarsmakten gör vi vidare motsvarande bedömningar som ovan i avsnitt 20.2.4 och ser således inte skäl till att i detta lagstiftningsarbete föreslå någon särreglering vad avser motsvarigheter till 7 kap. 3 och 5 §§ BDL.

21 Tillsyn

21.1 Direktivets bestämmelser

PNR-direktivet innehåller särskilda bestämmelser om tillsyn. I artikel 15.1 anges att varje medlemsstat ska föreskriva att den nationella tillsynsmyndighet som avses i artikel 25 i dataskyddsrambeslutet ska ansvara för att ge riktlinjer för och övervaka tillämpningen av de nationella bestämmelser som genomför direktivet. Vid tillsynen ska artikel 25 i dataskyddsrambeslutet tillämpas.

Tillsynsmyndigheten ska, enligt artikel 15.2, utföra sina uppgifter i syfte att skydda grundläggande rättigheter i samband med behandling av personuppgifter. I artikel 15.3 anges att varje nationell tillsynsmyndighet också ska

- a) hantera klagomål från en registrerad, undersöka ärendet och inom rimlig tid informera de registrerade om förloppet för och resultatet av dennes klagomål,
- b) kontrollera att uppgiftsbehandlingen är laglig, genomföra utredningar, inspektioner och revision i enlighet med nationell rätt, antingen på eget initiativ eller på grundval av ett klagomål som avses i led a.

Vidare ska, enligt artikel 15.4, varje nationell tillsynsmyndighet på begäran ge registrerade råd om hur de kan utöva de rättigheter som fastställs vid genomförandet av direktivet.

Som vi berört i tidigare avsnitt framgår av artikel 6.7 att ärenden kan initieras hos tillsynsmyndigheten av dataskyddsombudet vid enheten för passagerarinformation, nämligen om ombudet anser att enhetens behandling av uppgifter inte varit lagenlig. I artikel 13.5 och 13.6 anges vidare att enheten för passagerarinformation på be-

gäran ska göra dokumentation och loggar tillgängliga för tillsynsmyndigheten.

21.2 Bakgrund

21.2.1 Dagens tillsyn över behandling av personuppgifter

Datainspektionen

Datainspektionen utövar i dag tillsyn över all behandling av personuppgifter, om inte ansvaret uttryckligen har anförtrotts någon annan myndighet. Tillsynen omfattar såväl sådan personuppgiftsbehandling som regleras i personuppgiftslagen som i särskilda registerförfattningar eller andra författningar som innehåller bestämmelser om behandling av personuppgifter. Datainspektionens uppdrag regleras i förordningen (2007:975) med instruktion för Datainspektionen (nedan kallad Datainspektionens instruktion).

Inspektionen har utsetts till nationell tillsynsmyndighet enligt flera EU-rättsakter, b.la. enligt dataskyddsrambeslutet. Tillsynsuppgifterna framgår av 2 a och 4 §§ Datainspektionens instruktion. Datainspektionen är enligt 2 § PUF även tillsynsmyndighet enligt personuppgiftslagen.

Datainspektionen har till uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Inspektionen ska särskilt inrikta sin verksamhet på att informera om gällande regler och att ge råd och hjälp åt personuppgiftsombud. Vidare ska myndigheten följa och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik (1 § Datainspektionens instruktion).

Inspektionen har rätt att för sin tillsyn få tillgång till personuppgifter, upplysningar och dokument och tillträde till lokaler som används för behandling av personuppgifter (43 § PUL). Genom påpekanden och liknande förfaranden ska Datainspektionen i första hand försöka åstadkomma rättelse och i andra hand besluta om förbud mot annan behandling än lagring (45 §) eller vid domstol ansöka om utplåning av personuppgifter som behandlats på olagligt sätt (47 §). I vissa fall kan inspektionen förena sina förelägganden med

vite (44 och 45 §§). Datainspektionens beslut i tillsynsfrågor får överklagas (52 §).

Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden (SIN) utövar också tillsyn över de brottsbekämpande myndigheterna. Nämndens uppdrag regleras i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

SIN utövar tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet. De myndigheter vars verksamhet med hemliga tvångsmedel berörs av tillsynen är Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten och Tullverket. Nämnden utövar även tillsyn över Säkerhetspolisens och Polismyndighetens behandling av personuppgifter enligt polisdatalagen och lagen (2010:362) om polisens allmänna spaningsregister. Tillsynen ska särskilt ta sikte på behandlingen av känsliga personuppgifter.

SIN utövar sin tillsyn genom inspektioner och andra undersökningar. Nämnden är också skyldig att på begäran av en enskild kontrollera om denne har varit föremål för hemliga tvångsmedel eller sådan behandling av personuppgifter inom nämndens tillsynsområde som strider mot lag eller annan författning. Den enskilde ska underättas om att kontrollen genomförts. För sin tillsyn har nämnden rätt att få tillgång till de uppgifter och den hjälp som den begär av den myndighet som tillsynen avser. Om nämnden finner något att anmärka på får den lämna synpunkter på hur bristerna bör avhjälpas. Nämndens rekommendationer är inte bindande och kan inte överklagas.

Om SIN i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det till Åklagarmyndigheten och om nämnden finner något som kan leda till skadeståndsansvar för staten ska det anmälas till JK. Vidare ska nämnden, om den finner omständigheter som Datainspektionen bör uppmärksammas på, anmäla det till inspektionen.

JO och JK

JO och JK utövar tillsyn över hur lagar och andra föreskrifter tillämpas i offentlig verksamhet. Deras tillsyn omfattar därmed även behandlingen av personuppgifter och skyddet av enskildas integritet vid sådan behandling. JO:s verksamhet regleras framför allt i regeringsformen, riksdagsordningen och lagen (1986:765) med instruktion för Riksdagens ombudsmän. JK:s verksamhet regleras huvudsakligen i lagen (1975:1339) om Justitiekanslerns tillsyn och i förordningen (1975:1345) med instruktion för Justitiekanslern.

Ett granskningsärende kan inledas både efter klagomål från enskilda och på JO:s eller JK:s eget initiativ. De som står under JO:s och JK:s tillsyn ska på begäran lämna upplysningar och yttranden och ge tillgång till handlingar och protokoll. Såväl JO som JK kan genomföra inspektioner som ett led i granskningen. Tillsynsärendena kan resultera i beslut som kan innehålla kritik eller vägledande uttalanden. JO och JK kan även väcka åtal mot någon som står under deras tillsyn för brott som begåtts i tjänsten. JO och JK har också rätt att väcka frågor om disciplinär bestraffning.

21.2.2 Förslag om förändrat tillsynsansvar

Utredningen om tillsyn över den personliga integriteten (Ju 2015:02) har haft till uppdrag att kartlägga vilken tillsyn över behandling av personuppgifter som bedrivs i dag och överväga om tillsynen i större utsträckning kan samlas hos en myndighet. Utredningen har också haft i uppdrag att bl.a. peka ut vilken eller vilka svenska myndigheter som bör vara tillsynsmyndighet enligt dataskyddsförordningen respektive det nya dataskyddsdirektivet. Även frågor om hur tillsynsverksamheten ska organiseras har ingått i den utredningens uppdrag. Utredningen har avgett betänkandet Ett samlat ansvar för tillsyn över den personliga integriteten (SOU 2016:65).

Utredningen föreslår att tillsynen enligt både dataskyddsförordningen och det nya dataskyddsdirektivet ska samlas hos Datainspektionen och att det i myndighetens instruktion ska föreskrivas att Datainspektionen ska vara tillsynsmyndighet enligt de båda rättsakterna. Enligt förslaget ska SIN – vid sidan av Datainspektionen – även fortsättningsvis utöva tillsyn över Säkerhetspolisens behandling av personuppgifter men däremot inte över Polismyndighetens

personuppgiftsbehandling i allmänhet. SIN föreslås också behålla uppgiften att utöva tillsyn över bl.a. användningen av hemliga tvångsmedel.

Statsmakterna har ännu inte tagit ställning till förslagen.

21.2.3 Dataskyddsrambeslutet

I artikel 25 i dataskyddsrambeslutet förutsätts att det ska finnas minst en oberoende tillsynsmyndighet i varje medlemsstat. Enligt artikeln ska tillsynsmyndigheten bl.a. ha utredningsbefogenheter och tillgång till alla de uppgifter som behövs för tillsynen. Tillsynsmyndigheten ska också ha faktiska befogenheter att ingripa och att inleda rättsliga förfaranden eller uppmärksamma de rättsliga myndigheterna på överträdelser. Vidare ska enskilda kunna vända sig till tillsynsmyndigheten med klagomål över personuppgiftsbehandlingen.

Vid genomförandet av dataskyddsrambeslutet bedömdes inte rambeslutets regler om tillsyn kräva några lagstiftningsåtgärder, eftersom bestämmelserna i 43–47 §§ PUL ansågs uppfylla de aktuella reglerna (se prop. 2012/13:73 s. 113 f.).

Regeringen har, som tidigare angetts, utsett Datainspektionen till nationell tillsynsmyndighet enligt rambeslutet.

21.2.4 Brottsdatalagen

Som framgått i tidigare avsnitt får PNR-direktivets hänvisningar till dataskyddsrambeslutet läsas som hänvisningar till det nya dataskyddsdirektivet, som ska ersätta rambeslutet. I Utredningen om 2016 års dataskyddsdirektivs uppdrag har ingått att föreslå hur det nya direktivets förpliktelser ska genomföras även när det gäller tillsyn. Dock undantogs från uppdraget sådana frågor som omhändertagits av Utredningen om tillsynen över den personliga integriteten.

I 1 kap. 6 § BDL definieras tillsynsmyndigheten som den myndighet som regeringen utser att enligt dataskyddsdirektivet utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Enligt utredningen om 2016 års dataskyddsdirektiv värnas tillsynsmyndighetens oberoende bäst om det inte införs några regler om när och hur tillsyn ska inledas respektive avslutas eller hur tillsynen närmare ska bedrivas. Det som har funnits nödvändigt att reglera är tillsynsområdet, vem som ska utföra tillsyn, tillsynsmyndighetens uppgifter samt myndighetens befogenheter. Enligt utredningen behövs det även vissa regler om handläggningen av ärenden. (Se SOU 2017:29 s. 442 f.)

Tillsynsmyndigheten ska enligt 5 kap. 1 § BDL ha dubbla perspektiv. Således anges i bestämmelsen att tillsynsmyndigheten ska verka både för att fysiska personers grundläggande fri- och rättigheter och friheter skyddas i samband med personuppgiftsbehandling och för att underlätta det fria flödet av personuppgifter inom lagens tillämpningsområde. Samtidigt som det är viktigt att tillsynsmyndigheten verkar för en hög skyddsnivå för personuppgifter och bedriver ett kraftfullt tillsynsarbete, måste de behöriga myndigheternas perspektiv beaktas. I den mån det finns utrymme att välja olika lösningar som är likvärdiga ur integritetssynpunkt, bör tillsynsmyndigheten välja den som bäst tillgodoser det fria flödet av personuppgifter. (Se SOU 2017:29 s. 445.)

I det nya dataskyddsdirektivet behandlas tillsynsmyndighetens uppgifter i artikel 46. Denna artikel är i brottsdatalagen genomförd genom 5 kap. 2–4 §§ BDL. Tillsynsmyndighetens huvuduppgifter definieras i 2 §. Där anges att tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling,
2. handlägga klagomål från registrerade,
3. utföra kontroll enligt 3 §, och
4. på begäran bistå en tillståndsmyndighet i en annan stat.

I allmän tillsyn ingår, enligt utredningen, de uppgifter som nämns i artikel 46.1 punkterna a och i. Direktivets bestämmelser om hur klagomål ska hanteras av tillsynsmyndigheten motsvarar enligt utredningen vidare vad som redan tillämpas enligt allmänna principer för tillsyn och reglerna i förvaltningslagen (1986:223). Utöver bestämmelsen om att det ska framgå att handläggning av klagomål ingår i tillsynsuppgifterna, behövs därför inga lagstiftningsåtgärder för att genomföra bestämmelserna i artikel 46.1 f (se SOU 2017:29 s. 449).

Personuppgiftsansvariga får under vissa förutsättningar begränsa enskildas rätt till information (se avsnitt 20.2). Av 5 kap. 3 § BDL framgår att tillsynsmyndigheten på begäran ska kontrollera om uppgifter om en fysisk person behandlas författningsenligt. Den som begär sådan kontroll ska visa att han eller hon först har begärt information från eller en korrigeringsåtgärd av den personuppgiftsansvarige. Tillsynsmyndigheten får vägra att utföra en kontroll om begäran är orimlig eller uppenbart ogrundad.

I 5 kap. 4 § anges att tillsynsmyndigheten ska ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden. Enligt utredningens mening följer det dock redan av den allmänna service-skyldigheten enligt 4 § förvaltningslagen att myndigheterna har en skyldighet att på begäran ge *enskilda* information och råd om hur de kan ta tillvara sina rättigheter. När det behövs och är lämpligt ska en myndighet vägleda den enskilde genom att, beroende på omständigheterna, ta initiativ till ytterligare utredning, verka för att utredningen begränsas till vad som är nödvändigt och fästa den enskildes uppmärksamhet på att det finns något annat, bättre sätt att nå det han eller hon eftersträvar. Någon lagstiftningsåtgärd för att genomföra artikel 46.1 e föreslås därför inte. (Se SOU 2017:29 s. 460.)

I 5 kap. 5–7 §§ BDL regleras tillsynsmyndighetens befogenheter (motsvarar bl.a. artikel 47 i det nya dataskyddsdirektivet). I 5 kap. 5 § anges tillsynsmyndighetens undersökande befogenheter. Enligt bestämmelsen ska tillsynsmyndigheten ha rätt att från personuppgiftsansvariga och personuppgiftsbiträden på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandling av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Tillsynsmyndigheten föreslås, på liknande sätt som i dag, ha möjlighet att tillgripa olika befogenheter för det fall personuppgifter behandlas i strid med lag eller annan författning. Enligt utredningens

förslag ska dessa befogenheter ses som en trappa som ger tillsynsmyndigheten möjlighet att successivt använda kraftfullare medel och därigenom stegra påtryckningarna på den som inte självmant rättar sig efter myndighetens anvisningar (se SOU 2017:29 s. 468). I 5 kap. 6 § behandlas tillsynsmyndighetens förebyggande befogenheter. För det fall tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning ska, enligt bestämmelsen, tillsynsmyndigheten genom råd, rekommendationer och påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken. Tillsynsmyndigheten får utfärda en skriftlig varning för att det finns risk för att planerad behandling av personuppgifter kan komma att stå i strid med lag eller annan författning. Detsamma gäller om det finns risk för att pågående behandling kan komma att stå i strid med lag eller annan författning. I 5 kap. 7 § anges tillsynsmyndighetens korrigerande befogenheter. Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet annars inte fullgör sina skyldigheter får tillsynsmyndigheten

1. genom förebyggande åtgärder förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningensenlig eller att uppfylla andra skyldigheter,
2. förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningensenlig eller att uppfylla andra skyldigheter,
3. förbjuda fortsatt behandling om bristen är allvarlig, eller
4. besluta om sanktionsavgift.

Innan tillsynsmyndigheten fattar ett bindande beslut mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövt (5 kap. 8 §).

I brottsdataförordningen anges att tillsynsmyndigheten ska anmäla personuppgiftsbehandling som kan utgöra brott eller medföra

skadeståndsskyldighet för staten till den myndighet i vars arbetsuppgifter det ingår att utreda frågan (5 kap. 3 §). Enligt 5 kap. 10 § BDF ska tillsynsmyndigheten utföra sina tillsynsuppgifter avgiftsfritt, om inte annat bestäms.

21.2.5 Dataskyddsförordningen

Bestämmelser om tillsyn finns i artiklarna 51–76 i dataskyddsförordningen. Av artikel 51.1 framgår att tillsyn enligt förordningen, på samma sätt som enligt det nya dataskyddsdirektivet, ska ske i syfte att skydda fysiska personers grundläggande fri- och rättigheter i samband med personuppgiftsbehandling samt att underlätta det fria flödet av sådana uppgifter inom unionen. De närmare tillsynsuppgifterna framgår av artikel 57. Bland uppgifterna ingår att övervaka och verkställa tillämpningen av förordningen, att på begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt förordningen, att behandla klagomål från bl.a. registrerade och att utföra undersökningar om tillämpningen av förordningen.

Som tidigare har angetts har Utredningen om tillsyn över den personliga integriteten föreslagit att Datainspektionen ska vara tillsynsmyndighet även enligt dataskyddsförordningen.

21.3 Våra överväganden och förslag

Vårt förslag: Det ska i lagen föras in en bestämmelse som anger att tillsyn över personuppgiftsbehandling enligt lagen ska utföras av tillsynsmyndigheten enligt brottsdatalagen och i enlighet med bestämmelserna om tillsyn i den lagen.

Enligt PNR-direktivet ska den tillsynsmyndighet som avses i dataskyddsrambeslutet ha tillsyn över de bestämmelser som genomförs enligt direktivet. Eftersom direktivets hänvisningar till rambeslutet ska läsas som hänvisningar till det nya dataskyddsdirektivet, ska således samma myndighet som ska utöva tillsyn enligt det nya dataskyddsdirektivet vara tillsynsmyndighet även enligt PNR-direktivet. Utredningen om tillsyn över den personliga integriteten har föreslagit att Datainspektionen ska vara tillsynsmyndighet för det nya data-

skyddsdirektivet och att detta ska regleras i Datainspektionens myndighetsinstruktion. Det kommer inte att finnas något ställningsstagande till förslaget när vårt uppdrag ska redovisas. Om Datainspektionen utses till tillsynsmyndighet enligt dataskyddsdirektivet bör det i myndighetens instruktion föras in att inspektionen ska vara tillsynsmyndighet även enligt PNR-direktivet. Så kan ske förslagsvis i instruktionens 4 §. I lagförslaget benämner vi tillsynsmyndigheten som den tillsynsmyndighet som avses i brottsdatalagen.

Vid tillsynen ska, enligt PNR-direktivet, bestämmelserna om tillsyn i rambeslutet tillämpas, vilket alltså får tolkas som det nya dataskyddsdirektivets bestämmelser. Bestämmelserna om tillsyn i det nya dataskyddsdirektivet föreslås samtliga genomföras i brottsdatalagen och den tillhörande förordningen. De aktuella bestämmelserna i brottsdatalagen är generellt formulerade och kan bli direkt tillämpliga även vid tillsyn över sådan personuppgiftsbehandling som avses i vår lag i den mån de personuppgiftsansvariga annars omfattas av brottsdatalagens tillämpningsområde. Så är emellertid inte fallet med lufttrafikföretagen, för vilka tillsyn i övrigt kommer att regleras i dataskyddsförordningen och den föreslagna kompletterande lagen, respektive Försvarsmakten beträffande vilka det i nu aktuell del finns bestämmelser om tillsyn i 5 kap. lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Enligt den anslutande förordningen till den sistnämnda lagen är Datainspektionen tillsynsmyndighet enligt lagen. Det är vidare ännu oklart vad som kommer att gälla för tillsyn och annan dataskyddsreglering beträffande Säkerhetspolisen.

I PNR-direktivet pekas vissa särskilda uppgifter ut, som tillsynsmyndigheten ska utföra. Myndigheten ska, enligt artikel 15.3, hantera klagomål från enskilda och kontrollera att uppgiftsbehandlingen är laglig. Vidare ska tillsynsmyndigheten genomföra utredningar, inspektioner och revision i enlighet med nationell rätt. Dessa grundläggande tillsynsuppgifter omfattas enligt vår mening av 5 kap. 2 § BDL. I det nya dataskyddsdirektivet anges inte särskilt att revision ska utföras och det föreslås således inga bestämmelser om detta i brottsdatalagen. Med hänsyn till att det i PNR-direktivet anges att revision ska utföras i enlighet med nationell rätt tolkar vi det inte som någon skyldighet för medlemsstaterna att införa någon ny sorts tillsynsuppgift i nationell rätt. De tillsynsuppgifter som

anges i brottsdatalagen är således enligt vår mening tillräckliga för att uppfylla PNR-direktivets krav i denna del.

Vidare ska tillsynsmyndigheten, enligt artikel 15.4 i direktivet, på begäran ge registrerade råd om hur de kan utöva sina rättigheter. Denna uppgift har Utredningen om 2016 års dataskyddsdirektiv ansett omfattas av den allmänna serviceskyldigheten i förvaltningslagen och därmed inte kräva några lagstiftningsåtgärder. Vi delar den bedömningen. De tillsynsuppgifter som anges i brottsdatalagen kan således tillämpas för all personuppgiftsbehandling enligt PNR-direktivet.

I direktivet anges att tillsynsmyndigheten ska utföra sina uppgifter i syfte att skydda grundläggande rättigheter i samband med behandling av personuppgifter. Även enligt brottsdatalagen ska tillsynen ske i detta syfte (5 kap. 1 § BDL). Enligt den bestämmelsen ska tillsynen också ske i syfte att underlätta det fria flödet av personuppgifter. Enligt vår mening kommer inte tillsynens dubbla syften att medföra en lägre skyddsnivå för personuppgifterna. Bestämmelsen i brottsdatalagen uppfyller därmed direktivets krav. Det kan i sammanhanget påpekas att tillsyn även enligt dataskyddsförordningen ska ske både i syfte att skydda fysiska personers grundläggande fri- och rättigheter i samband med personuppgiftsbehandling och i syfte att underlätta det fria flödet av sådana uppgifter inom unionen. Tillsynen inom såväl direktivets som förordningens tillämpningsområden kommer således framöver att ske enligt båda dessa syften.

Som nyss angetts kommer den av oss föreslagna lagen att tillämpas även av aktörer som inte omfattas av brottsdatalagens tillämpningsområde, t.ex. lufttrafikföretag och Försvarsmakten. Enligt vår mening bör det därför i lagen föras in en allmän bestämmelse som anger att tillsyn över personuppgiftsbehandling enligt lagen ska utföras av tillsynsmyndigheten enligt brottsdatalagen och i enlighet med den lagens bestämmelser om tillsyn. Därmed regleras att tillsynsmyndigheten enligt brottsdatalagen ska ha tillsyn även över lufttrafikföretags behandling av personuppgifter enligt lagen. Bestämmelsen blir även tillämplig såväl för den behandling av personuppgifter enligt lagen som sker vid enheten för passagerarinformation som vid de behöriga myndigheterna, oavsett vilken tillsynsmyndighet som i övrigt har tillsynsansvaret för den myndigheten. Enligt vår mening är det nämligen en rimlig ordning att samma tillsynsmyndighet har tillsyn över

hela lagens tillämpning, vilket vi menar också är den ordning som föreskrivs i artikel 15.1 i PNR-direktivet.

22 Sanktioner

22.1 Direktivets bestämmelser och vårt uppdrag

PNR-direktivet innehåller krav på att medlemsstaterna ska införa bestämmelser om sanktioner. I artikel 14 anges att medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt direktivet och vidta alla nödvändiga åtgärder för att se till att de genomförs. I bestämmelsen anges vidare att medlemsstaterna särskilt ska fastställa bestämmelser om sanktioner, inklusive ekonomiska sådana, mot lufttrafikföretag som inte översänder uppgifter i enlighet med artikel 8 eller som inte översänder uppgifterna i det fastställda formatet. Sanktionerna ska vara effektiva, proportionella och avskräckande.

I vårt uppdrag ingår således att föreslå sanktioner mot de lufttrafikföretag som inte uppfyller skyldigheten att överföra PNR-uppgifter eller som inte överför uppgifterna i det fastställda formatet. I kommittédirektiven anges att ett sådant sanktionssystem riktat mot lufttrafikföretagen bör vara uppbyggt enligt den struktur som redan gäller i dag, som innebär att en myndighets beslut om sanktioner kan överklagas till allmän förvaltningsdomstol.

Vidare ingår i uppdraget att föreslå bestämmelser om sanktioner för sådana eventuella överträdelser som kan komma att ske vid enheten för passagerarinformation och vid behöriga myndigheter av de nationella bestämmelser som genomför direktivet. Dessa sanktioner ska tillse att direktivets bestämmelser om behandling och skydd av PNR-uppgifter efterlevs av myndigheterna och syftar främst till att förhindra att enskildas integritet kränks.

Lufttrafikföretagens behandling av personuppgifter kommer framöver att regleras av dataskyddsförordningen. Förordningen kommer att vara direkt tillämplig i medlemsstaterna. För det fall lufttrafikföretagen i samband med sin överföring av PNR-uppgifter skulle

bryta mot någon dataskyddsbestämmelse i förordningen, t.ex. genom att inte skydda PNR-uppgifterna med erforderlig informationssäkerhet eller inte ha rättsenliga avtal med eventuella personuppgiftsbiträden, kommer de sanktioner som anges i dataskyddsförordningen att bli tillämpliga.

22.2 Olika typer av sanktioner

Det finns inte någon rättslig definition av begreppet sanktion. En sanktion är dock i princip alltid handlingsdirigerande eller har ett bestraffande syfte. Med en vid definition skulle sanktion kunna sägas vara alla former av påföljder som kan följa på ett rättsstridigt handlande.

En sanktion kan vara repressiv eller icke repressiv. Med att en sanktion är repressiv avses att det är staten som kan ta initiativ till sanktionen. En icke repressiv sanktion är t.ex. möjligheten att begära skadestånd i en civilprocess.

Det finns flera olika sorter av repressiva sanktioner. Den mest ingripande formen utgörs av straff. Straffsanktioner bör dock användas i sista hand och endast om det inte finns någon annan sanktion som är tillräckligt effektiv (jfr Europeiska unionens råd, dokument 16542/3/09).

I många fall utgörs sanktioner av ekonomiska sådana. Böter, företagsbot, sanktionsavgifter och vite är alla olika former av ekonomiska sanktioner.

Böter är en straffrättslig påföljd, som kan åläggas genom dom, strafföreläggande eller föreläggande av ordningsbot. *Företagsbot* är en särskild rättsverkan av brott som är avsedd att tillämpas vid allvarliga brott i näringsverksamhet. Företagsboten har en bestraffande funktion riktad mot näringsidkare i vars verksamhet brott har begåtts.

Med *sanktionsavgifter* avses sådana administrativa avgifter som utgör en ekonomisk sanktion vid sidan av eller i stället för vissa skadestånd, vite, böter och förverkande. Avgifterna är knutna till vissa bestämmelser på ett sådant sätt att en överträdelse av bestämmelsen medför skyldighet att betala avgift till det allmänna. Sanktionsavgifter drabbar den som bedriver den verksamhet inom vars ram överträdelsen har inträffat. Skyldigheten att betala avgifterna

åläggs vanligen med strikt ansvar. Bestämmelsen i 19 kap. 5 a § utlänningslagen (2005:716), som anger att transportörer som inte fullgör sin skyldighet att överföra API-uppgifter ska betala en särskild avgift, utgör ett exempel på en sanktionsavgift.

Vite är ett ekonomiskt påtryckningsmedel för att få någon att vidta en åtgärd eller underlåta något. Det kan, liksom sanktionsavgifter, användas mot såväl fysiska som juridiska personer. Ett vite har alltid anknytning till ett visst föreläggande eller förbud och riktas mot den i beslutet angivna adressaten. Möjligheten att införa vite går ofta tillbaka på generella regler av något slag, ofta av förbuds-karaktär, men måste inte ha den konstruktionen. Föreläggande och utdömmande av vite regleras i lagen (1985:206) om viten (viteslagen).

Därutöver finns det en rad icke-ekonomiska sanktionsmöjligheter. I API-direktivet (artikel 4.2) anges som exempel på andra sanktioner som kan användas gentemot transportörer körförbud, beslag och förverkande av transportmedel och tillfälligt upphävande eller återkallande av den operativa licensen.

22.3 Sanktioner mot lufttrafikföretag

22.3.1 Chicagokonventionens bestämmelser

Chicagokonventionen, även kallad Icao-konventionen, innehåller bestämmelser om internationell civil luftfart. Så gott som alla länder har anslutit sig till konventionen, som behandlas närmare i avsnitt 4.2.1.

I annex 9 till konventionen finns bl.a. bestämmelser om behandlingen av API- och PNR-uppgifter. I artikel 3.48 behandlas överföringen av API-uppgifter. Här anges att de fördragsslutande staterna så långt det är möjligt bör försöka minimera de operativa och administrativa bördorna för lufttrafikföretagen (artikel 3.48.5). Enligt artikel 3.48.6 rekommenderas de fördragsslutande staterna att avhålla sig från användningen av sanktioner mot lufttrafikföretag på grund av tekniska överföringsfel.

I artikel 3.49 behandlas överföringen av PNR-uppgifter. Enligt bestämmelsen bör fördragsslutande stater som kräver tillgång till PNR-uppgifter anpassa sin behandling av uppgifterna och sina tekniska krav till bl.a. de riktlinjer som anges i Icao:s dokument 9944, Guidelines on Passenger Name Record (PNR) Data. Sanktioner och straff behandlas i artikel 2.16 i dokument 9944. I artikel 2.16.1 anges

att stater bör erkänna att de PNR-uppgifter som inhämtas av lufttrafikföretagen inte kan verifieras i fråga om riktighet eller fullkomlighet. Därför bör, enligt bestämmelsen, åtgärder inte vidtas mot en operatör eller denne hållas ansvarig för att uppgifter överförda i god tro senare visar sig vara inkorrekta. I artikel 2.16.2 finns en bestämmelse om omdirigerade flygningar, dvs. flygningar som inte sker enligt den förutbestämda rutten. Om en operatör inte har överfört PNR-uppgifter för en sådan flygning bör stater ta hänsyn till omständigheterna rörande omdirigeringen. Enligt artikel 2.16.3 ska de sanktioner som stater kan använda sig av mot operatörer som inte överför PNR-uppgifter, endast rikta sig mot de företag som direkt utför de aktuella flygningarna.

22.3.2 Jämförbara nationella sanktionsbestämmelser

Flera olika sanktioner kan, som tidigare angetts, tänkas vara möjliga att använda gentemot de lufttrafikföretag som inte överför PNR-uppgifter i enlighet med de nationella bestämmelser som genomför PNR-direktivet. I detta avsnitt redogörs för vissa jämförbara nationella sanktionssystem.

Sanktionsavgifter kopplade till transportörsansvaret i utlänningslagen

Sedan den 1 juli 2004 finns i utlänningslagen regler om en transportörs ansvar för att kontrollera att en utlänning, som denne transporterar till Sverige direkt från en stat som inte omfattas av Schengenkonventionen, innehar pass och de tillstånd som krävs för att resa in i landet (se avsnitt 4.4.2). I 19 kap. 5 § utlänningslagen finns bestämmelser om ekonomiska sanktioner mot de transportörer som inte uppfyller denna kontrollskyldighet. Bestämmelsen innebär att de transportörer som inte uppfyller sina skyldigheter ska betala en särskild avgift (sanktionsavgift) om beslut om avvisning har meddelats på grund av att utlänningen saknar pass eller de tillstånd som krävs för inresa och beslutet har vunnit laga kraft eller har verkställts trots att det inte har vunnit laga kraft. Om transportören visar sig ha haft skäligen anledning att anta att utlänningen hade rätt att resa in i Sverige ska emellertid någon särskild avgift inte betalas. Detsam-

ma gäller om det framstår som uppenbart oskäligt att ta ut avgiften. Den särskilda avgiften ska enligt 19 kap. 6 § bestämmas till högst 46 000 kronor för varje utlänning. Frågan om transportören ska betala en avgift prövas enligt 19 kap. 7 § av den myndighet som ska verkställa avvisningen. I bestämmelsen anges att avgiften ska betalas till Migrationsverket och tillfaller staten. Vidare anges att mål om uttagande av avgift handläggs som allmänt mål samt att bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Beslut om särskild avgift får enligt 14 kap. 14 § utlänningslagen överklagas hos allmän förvaltningsdomstol. Prövnings-tillstånd krävs vid överklagande till Kammarrätten.

Sanktionsavgifter enligt genomförandet av API-direktivet

Enligt API-direktivets artikel 4.1 ska medlemsstaterna vidta de åtgärder som är nödvändiga för att införa påföljder för transportörer som genom fel eller försummelse har underlåtit att lämna uppgifter eller som lämnar ofullständiga eller felaktiga uppgifter. Liksom i PNR-direktivet ska påföljderna vara avskräckande, effektiva och proportionella. Maximibeloppet för en påföljd får inte understiga 5 000 euro, eller motsvarande belopp i nationell valuta, för varje resa som gjorts utan att uppgifterna om passagerarna har lämnats eller om de har lämnats inkorrekt. Påföljden får inte heller understiga ett minimibelopp om 3 000 euro. I artikel 4.2 anges vidare att direktivet inte ska hindra medlemsstaterna från att gentemot de transportörer som mycket allvarligt åsidosätter de skyldigheter som följer av bestämmelserna i direktivet, införa eller bibehålla andra påföljder. Som förslag på sådana andra påföljder anges i bestämmelsen, som tidigare framgått, körförbud, beslag och förverkande av transportmedel eller tillfälligt upphävande eller återkallande av den operativa licensen.

Genomförandet av API-direktivet i svensk rätt har behandlats bl.a. i avsnitt 4.5. För att uppnå enhetlighet med transportörsansvaret i utlänningslagen valdes samma sanktionssystem, dvs. sanktionsavgifter (se prop. 2005/06:129 s. 41 ff.). Således anges i 19 kap. 5 a § utlänningslagen att en transportör som inte har fullgjort sin uppgiftsskyldighet ska betala en särskild avgift. För det fall transportören visar att underlåtenheten inte beror på fel eller försummelse, eller om det framstår som uppenbart oskäligt att ta ut avgiften, ska dock

transportören undgå detta ansvar. Enligt 19 kap. 6 § ska den särskilda avgiften för varje flygning som har gjorts utan att transportören har fullgjort sin uppgiftsskyldighet bestämmas till högst 46 000 kronor. Frågan om transportören ska betala en särskild avgift ska enligt 19 kap. 7 § prövas av Polismyndigheten. Avgiften ska också betalas dit, men tillfaller staten. Även mål om uttagande av denna avgift handläggs som allmänt mål och får överklagas hos allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten (14 kap. 14 § utlänningslagen).

API-direktivet förhindrar alltså inte medlemsstaterna från att införa andra än ekonomiska sanktioner mot de transportörer som allvarligt åsidosätter sina skyldigheter enligt direktivets bestämmelser. Möjligheten att införa sådana andra än ekonomiska sanktioner diskuterades inte i förarbetena till genomförandet av direktivet i svensk rätt.

Vite enligt tullagstiftningen

I såväl polislagen (1984:387) som i tullagstiftningen finns bestämmelser om transportörers skyldighet att på begäran av myndigheterna lämna vissa uppgifter om transporten (se avsnitt 5.2). Om transportföretag inte lämnar dessa uppgifter på Tullverkets begäran, har Tullverket möjlighet att förelägga transportföretaget att vid vite lämna uppgifterna. Bestämmelser härom finns i 4 kap. 24 § och 7 kap. 5 § tullagen (2016:253) samt i 21 § lagen (1996:701) om Tullverkets befogenhet vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränslagen). Ett sådant föreläggande innebär en skyldighet för transportföretaget att lämna tidigare begärda bokningsuppgifter till Tullverket. Till föreläggandet kopplas ett vite som kan dömas ut om transportföretaget inte lämnar de begärda uppgifterna. Föreläggandet gäller först när delgivning har skett. Vitesbeloppet fastställs av Tullverket och ska enligt 3 § viteslagen uppgå till ett belopp som med hänsyn till vad som är känt om adressatens ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som förenats med vitet. Om transportföretaget inte följer föreläggandet om att lämna bokningsuppgifter till Tullverket ska verket ansöka hos Förvaltningsrätten i Stockholm om att få vitet utdömt.

Tullverket har endast vid två tillfällen använt sig av möjligheten att förelägga lufttrafikföretag att vid vite lämna ut bokningsuppgifter. Inte något av fallen har gått vidare till domstol.

Sanktionsavgifter vid överträdelser av regelverket om identitetskontroller vid transporter med buss, tåg eller passagerarfartyg

Lagen (2015:1073) om särskilda åtgärder vid allvarlig fara för den allmänna ordningen eller den inre säkerheten i landet trädde i kraft den 21 december 2015. Lagen är tillfällig och gäller under tre år. I lagen ges regeringen eller den myndighet som regeringen bestämmer rätt att vid allvarlig fara för den allmänna ordningen eller den inre säkerheten i landet meddela föreskrifter om identitetskontroller vid transporter som utförs med buss, tåg eller passagerarfartyg till Sverige från en annan stat. Regeringen får också meddela föreskrifter om sanktionsavgifter. Föreskrifterna får gälla i högst sex månader i taget. I lagens förarbeten anges att ett system med sanktionsavgift har den fördelen att man uppnår en snabb, enkel och kostnadseffektiv hantering av överträdelser av regelverket. Det ansågs därför vara lämpligt att en sanktionsavgift ska kunna tas ut av den som låter bli att utföra identitetskontroller enligt sådana föreskrifter som får meddelas med stöd av lagen (se prop. 2015/16:67 s. 17).

Regeringen har vid fyra tillfällen beslutat om en förordning med närmare föreskrifter om transportörers skyldighet att utföra identitetskontroller vid resor till Sverige från Danmark. Den senaste förordningen gällde till den 4 maj 2017. Förordningen gäller dock fortfarande för ärenden eller mål om sanktionsavgift som har inletts innan förordningen upphörde att gälla.

Sanktioner på luftfartens område

I luftfartslagen (2010:500) finns grundläggande bestämmelser om rätt att utöva luftfart inom svenskt område. Numera finns även en rad EU-förordningar på luftfartens område som gäller vid sidan av lagen och som har företräde framför nationell rätt.

I 11 kap. luftfartslagen finns sanktionsbestämmelser bestående i avgångsförbud. Enligt 11 kap. 1 § får Transportstyrelsen eller den

som styrelsen utser förbjuda en flygning och hindra ett luftfartyg från att avgå om det, när flygningen ska påbörjas, kan antas att luftfartyget inte uppfyller de villkor som anges i luftfartslagen eller som har fastställts med stöd av lagen. Detsamma gäller när andra villkor som fastställts för flygningen inte är uppfyllda. Den som bryter mot ett beslutat avgångsförbud kan dömas enligt 17 kap. 13 § brottsbalken för överträdelse av myndighets bud.

Vidare finns i 11 kap. 2 § luftfartslagen en bestämmelse som anger att den som driver en flygplats får hindra ett luftfartygs avgång om avgifter för användningen av flygplatsen och tjänsterna för luftfarten, som avser luftfartygets senaste ankomst, uppehåll och avgång, inte har betalats och säkerhet inte har ställts.

Luftfartslagen innehåller flera straffbestämmelser i dess 13 kap. Dessutom finns en bestämmelse om förverkande. Om ägaren eller någon som är i ägarens ställe uppsåtligen begår eller medverkar till vissa brottsliga gärningar kan ett luftfartyg enligt 13 kap. 12 § förklaras förverkat, om det behövs för att förebygga brott eller om det i övrigt finns särskilda skäl. Detta gäller dock inte, om förverkande är uppenbart oskäligt.

I 13 kap. 13 § finns vidare en generell bestämmelse som anger att ett föreläggande eller ett förbud som en myndighet meddelar enligt lagen eller enligt föreskrifter som har meddelats med stöd av lagen får förenas med vite.

För det fall ett luftrafikföretag inte uppfyller aktuella regler kan vidare ett meddelat tillstånd återkallas. Exempelvis anges i 7 kap. 6 § att ett *drifttillstånd* ska återkallas om tillståndshavaren i väsentlig grad åsidosätter föreskrifterna eller villkoren för verksamheten. Tillståndet kan också återkallas, om det måste antas att innehavaren inte kan upprätthålla verksamheten. I 7 kap. 11 § anges att ett *trafiktillstånd* får återkallas helt eller för viss tid eller begränsas, om tillståndshavaren inte iakttar de föreskrifter eller villkor som gäller för verksamheten, eller det i övrigt finns särskilda skäl.

En *operativ licens* kan enligt artikel 9 i EU:s luftrafikförordning¹ återkallas tillfälligt eller permanent om förordningens krav på ekonomiska förutsättningar inte längre är uppfyllda. Detsamma gäller om luftrafikföretaget uppsåtligen eller genom försumlighet förser

¹ Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av luftrafik i gemenskapen.

tillståndsmyndigheten med information som är felaktig i sak eller om företaget inte längre lever upp till förordningens krav på gott anseende.

22.3.3 Sanktioner som tillämpas i andra länder

Krav på överföring av PNR-uppgifter från lufttrafikföretag till ett lands myndigheter infördes för första gången i USA i början av 2000-talet. Om lufttrafikföretagen inte överförde de angivna uppgifterna kunde detta leda till ekonomiska sanktioner eller indraget landningstillstånd. Många länder har därefter infört egna PNR-system. De sanktioner som kan användas mot de lufttrafikföretag som inte överför sina PNR-uppgifter utgörs i de flesta fall av ekonomiska sådana. T.ex. använder sig Mexiko, Argentina och Sydkorea av ekonomiska sanktioner.

I de gällande avtalen mellan EU och USA respektive Australien som reglerar överföringen av PNR-uppgifter till dessa länder finns inga bestämmelser om sanktioner mot de lufttrafikföretag som inte överför PNR-uppgifter. Inte heller det nya förslaget till avtal med Kanada innehåller bestämmelser om sanktioner mot de lufttrafikföretag som inte överför sina PNR-uppgifter.

Storbritannien har i sitt nuvarande PNR-system såväl ekonomiska som straffrättsliga sanktionsmöjligheter. Inte vid något tillfälle har man dock använt sig av någon av dessa former av sanktioner. I Danmark finns en sanktionsbestämmelse som innebär att ett flyg kan nekas att avgå om PNR-uppgifter inte lämnas. Det finns även en möjlighet att neka åtkomst till eller utgång från flygplanet samt att neka tillförsel eller frånförsel av varor till dess uppgifterna har lämnats.

Det pågår för närvarande arbete inom samtliga medlemsstater med att genomföra PNR-direktivet i nationell rätt. Det råder därför varierande osäkerhet kring vilka sanktionsmöjligheter de övriga medlemsstaterna kommer att använda sig av.

22.3.4 Valet av sanktionsform

Vårt förslag: Administrativ sanktionsavgift bör användas som enda sanktionsform mot lufttrafikföretagen.

Våra överväganden och förslag

Allmänna utgångspunkter

Som framgått finns sedan tidigare bestämmelser i svensk rätt som innebär skyldigheter för lufttrafikföretag att lämna uppgifter om sina transporter till de svenska myndigheterna. I vissa fall kan sanktioner bli tillämpliga när dessa bestämmelser inte efterlevs. I svensk rätt är det således ingen ny företeelse att lufttrafikföretag, såväl inhemska som utländska, är skyldiga att vidta vissa åtgärder, ibland före ankomst till landet, liksom att underlåtenhet att genomföra dessa åtgärder i vissa fall kan resultera i ekonomiska sanktioner.

Straffbestämmelser bör inte väljas

PNR-direktivet pekar inte ut vilka sanktioner som ska införas mot lufttrafikföretagen. Det som anges är att ekonomiska sådana i vart fall ska införas. Vidare anges att sanktionerna ska vara effektiva, proportionella och avskräckande (artikel 14). Den sanktion som åtminstone teoretiskt anses som mest avskräckande är straff. Generellt kan konstateras att kriminalisering inte är det enda och inte heller alltid det mest effektiva medlet för att motverka oönskade beteenden. Det allmännas resurser för brottsbekämpning bör rimligen koncentreras på sådana förfaranden som kan leda till påtaglig skada eller fara och som inte kan hanteras på annat sätt (jfr prop. 1994/95:23 s. 54 ff.). Straffsanktioner ska således användas i sista hand och endast om det inte finns någon annan sanktion som inte är tillräckligt effektiv. Någon straffbestämmelse bör således enligt vår mening inte införas i lagen. Andra sanktionsformer bör övervägas i stället.

Ekonomiska sanktioner

Såväl böter som företagsbot förutsätter en kriminalisering. Av de ekonomiska sanktionerna faller därmed både böter och företagsbot bort som tänkbara sanktionsformer. De möjliga ekonomiska sanktionsformer som återstår utgörs därmed av sanktionsavgifter och vite.

Administrativa sanktionsavgifter används numera allt oftare. Övergången från straffbestämmelser till bestämmelser om sanktionsavgifter syftade ursprungligen till att bättre utnyttja rättsväsendets resurser och att kunna beivra en del mindre allvarliga och ofta förekommande överträdelseer effektivare. Ett annat syfte var att skapa en kännbar ekonomisk sanktion mot juridiska personer, som inte kan bli föremål för straffrättsliga åtgärder. Sanktionsavgift kan därmed riktas mot det subjekt som tjänar på överträdelsen eller bär det största ansvaret för att överträdelsen begicks. (Jfr SOU 2017:29 s. 498.)

Sanktionsavgifter finns inom en rad områden. De har olika syften och utformning. Tillämpningsområdet varierar också. I vissa fall är sanktionsavgift den enda sanktionen för en överträdelse, men i andra fall kan avgift påföras vid sidan av eller i stället för straff. Både fysiska och juridiska personer kan påföras sanktionsavgift. Ofta kan avgiften påföras oavsett om reglerna överträtts uppsåtligen eller av oaktsamhet.

Sanktionsavgifter har bl.a. den fördelen att de medför ett enklare och snabbare beivrande av överträdelseer. Att det är en myndighet och inte domstol som beslutar om avgiften anses ha betydelse för effektiviteten. Det förhållande att myndigheten fattar beslut utifrån sin egen utredning medför också en resurseffektivitet. Andra myndigheter behöver därmed inte kopplas in i processen, utom vid överklagande. (Jfr SOU 2014:83, s. 104 f.)

Särskilt i förhållande till viten anses sanktionsavgifter vara mer effektiva. Användning av vite innebär ett mer omständligt förfarande, eftersom det först måste föreläggas och sedan överträdelse för att kunna dömas ut.

Det finns givetvis även nackdelar med sanktionsavgifter. Om avgiften är satt för lågt kan verksamhetsutövaren se avgiften enbart som en kostnad som det går att kalkylera med. I dessa fall bidrar avgiften inte till ökad regelefterlevnad. Att införa system med sanktionsavgifter kan vidare kräva mer resurser hos myndigheten. Avsaknaden av domstols bedömning av händelseförlopp kan också inverka menligt på rättssäkerheten (se prop. 2007/08:107 s. 17 och

SOU 2014:83 s. 104 f.). Domstolsväsendet kan, i vart fall inledningsvis, få fler ärenden att hantera om sanktionsavgifter införs. Det kan t.ex. råda osäkerhet om när sanktionsavgift ska påföras och med vilket belopp innan det finns vägledande praxis. Det behöver alltså inte bli en ekonomisk besparing för staten att införa sanktionsavgifter (SOU 2014:83 s. 106).

I dataskyddsförordningen föreskrivs sanktionsavgifter vid överträdelse av bestämmelserna om personuppgiftsbehandling. Utredningen om 2016 års dataskyddsdirektiv föreslår också att sanktionsavgifter ska användas vid överträdelser av brottsdatalagens bestämmelser om personuppgiftsbehandling.

Det är viktigt att regelverk på snarlika områden är enhetligt utformade. Reglerna blir då lättare att tillämpa och mer förutsägbara. Bestämmelserna i PNR-direktivet uppvisar stora likheter med API-direktivet. Båda direktiven innebär en skyldighet för lufttrafikföretag att överföra uppgifter om sina passagerare till nationella myndigheter. Oavsett vilket direktiv som är tillämpligt kommer överföringen enligt svensk rätt att ske till Polismyndigheten. API-direktivet är, som tidigare angetts, genomfört i bl.a. utlänningslagen. Underlåtenhet att överföra API-uppgifter kan medföra en skyldighet för lufttrafikföretagen att betala att en sanktionsavgift.

Av regeringens skrivelse Förebygga, förhindra, försvåra – den svenska strategin mot terrorism (skr. 2014/15:146) framgår att PNR-systemet bör samordnas med systemet för API-uppgifter, eftersom de tillsammans kan vara ett användbart verktyg i kampen mot terrorism. Enligt Polismyndighetens planering kommer också de båda systemen att hanteras parallellt inom enheten för passagerarinformation. Med hänsyn till den samordnade hanteringen vore det lämpligt om samma sorts sanktioner användes i båda systemen. För att tillgodose kravet på en enhetlig utformning bör således bestämmelserna om sanktioner mot lufttrafikföretagen enligt PNR-systemet så långt som möjligt utformas i enlighet med de gällande bestämmelserna om sanktioner vid underlåtenhet att överföra API-uppgifter.

Sanktionsavgifter är därtill en snabb och tydlig sanktion – som även kan vara kännbar ekonomiskt. Risken att påföras sanktionsavgifter skulle enligt utredningens bedömning verka avskräckande. Sanktionsavgifter synes också vara mer ändamålsenliga än viten. Sanktionsavgifter bör därför enligt vår mening kunna åläggas de luft-

trafikföretag som inte har fullgjort sin överföringsskyldighet enligt PNR-direktivet.

Andra än ekonomiska sanktioner bör inte införas

Förutom de ekonomiska sanktionerna finns det andra sanktionsformer som skulle kunna användas mot de lufttrafikföretag som inte överför PNR-uppgifter i enlighet med direktivet. Några sådana sanktionsformer tillämpas dock inte för närvarande vid liknande situationer enligt svensk rätt. Frågan om användande av andra än ekonomiska sanktioner berördes inte ens i samband med det svenska genomförandet av API-direktivet.

Som har angetts ovan bör en enhetlig utformning av bestämmelserna om sanktioner mot lufttrafikföretag eftersträvas. Vidare bör sanktionerna, enligt vår bedömning, inte riskera att gå ut över tredje man, främst flygresenärer. Införandet av ett avgångsförbud skulle kunna få konsekvenser för bilaterala luftfartsavtal, varför användningen av en sådan sanktion nogga bör övervägas innan den införs. Indragande av ett lufttrafikföretags operativa licens synes därtill inte vara möjligt i en situation som den förevarande enligt bestämmelserna i lufttrafikförordningen.

Enligt vår mening är ekonomiska sanktioner tillräckliga för att förmå lufttrafikföretagen att fullgöra sin överföringsskyldighet. Först om det i ett senare skede skulle visa sig att de införda sanktionerna inte är tillräckligt effektiva, bör det övervägas om ytterligare sanktionsformer behöver föras in i svensk rätt.

22.3.5 När ska sanktionsavgift få användas?

Vårt förslag: Sanktionsavgift ska tas ut av de lufttrafikföretag som inte överför PNR-uppgifter i enlighet med bestämmelserna i lagen eller den tillhörande förordningen.

Sanktioner mot lufttrafikföretag som inte överför PNR-uppgifter

Enligt direktivet ska sanktioner träffa de lufttrafikföretag som inte översänder uppgifter i enlighet med artikel 8 eller som inte överför uppgifterna i det fastställda formatet. I artikel 8.3 anges att lufttrafikföretagen som huvudregel ska överföra PNR-uppgifterna elektroniskt med användning av de gemensamma protokoll och understödda dataformat som har antagits av kommissionen. Således anges redan i artikel 8 att överföringarna ska överföras i det fastställda formatet. Bestämmelserna i artikel 8 ska enligt vårt förslag genomföras såväl i den av oss föreslagna lagen som i den tillhörande förordningen. Sanktionsavgifterna bör därmed träffa de lufttrafikföretag som inte överför PNR-uppgifter i enlighet med dessa bestämmelser.

En bestämmelse som innebär att sanktionsavgift ska tas ut av lufttrafikföretag som inte fullgör sina skyldigheter motsvarar liknande bestämmelser om sanktionsavgifter för transportörer i utlänningslagen och i det tidigare gällande regelverket om identitetskontroller vid transporter med buss, tåg eller passagerarfartyg. Liksom i dessa författningar bör det finnas en möjlighet att i det enskilda fallet inte ta ut en sådan avgift, se nedan i avsnitt 22.3.6.

Enligt vårt förslag ska PNR-uppgifterna överföras av det lufttrafikföretag som utför själva flygningen. Sanktioner kommer således inte att drabba de lufttrafikföretag som endast delar linjebeteckning med det företag som utför flygningen.

Inga sanktioner vid utebliven information

Den av oss föreslagna regleringen innehåller en bestämmelse om att lufttrafikföretag ska informera sina passagerare om överföringen av PNR-uppgifter till enheten för passagerarinformation och om skälen till överföringen. Denna informationsskyldighet följer inte av någon artikel i direktivet utan framgår endast av skälen till direktivet. Det kan redan av denna omständighet ifrågasättas om det är lämpligt att införa sanktioner mot den som inte följer bestämmelsen. Den föreslagna bestämmelsen utgör därtill främst en utökad informationsskyldighet i förhållande till de krav som följer av dataskyddsförordningen. Enligt förordningen ska nämligen information om överföringen lämnas till passagerarna för det fall uppgifterna har kommit in direkt från dem till ett lufttrafikföretag. I sådana fall är det således bara information om

skälen till överföringen som följer endast av vårt lagförslag. För det fall PNR-uppgifterna kommer in till ett lufttrafikföretag från en resebyrå eller researrangör har lufttrafikföretaget dock inte motsvarande skyldighet att informera enligt förordningen. Eftersom informationsskyldigheten till viss del redan följer av dataskyddsförordningen skulle införandet av sanktioner i detta avseende kunna påverka tillämpligheten av dataskyddsförordningen när det gäller lufttrafikföretagens behandling av personuppgifter, vilket inte får ske enligt PNR-direktivet (jfr artikel 13.2).

Visserligen kan det ses som grundläggande att passagerarna informeras fullt ut om överföringen om PNR-uppgifter, för att de ska ha möjlighet att utöva sina rättigheter enligt direktivet. Sanktionsavgifter bör dock enligt vår mening endast användas vid överträdelser av de bestämmelser om behandling av personuppgifter som anses viktigast för att värna enskildas integritet, som innehåller de grundläggande reglerna om hur personuppgifter får behandlas och som – om de inte efterlevs – riskerar att leda till allvarliga kränkningar av registrerades integritet. Eftersom informationsskyldigheten till viss del redan följer av dataskyddsförordningen kan det inte anses leda till någon allvarlig kränkning av enskildas personliga integritet att de inte också informeras om skälen till överföringen. Det finns därtill andra möjligheter att ingripa mot ett lufttrafikföretag som inte lämnar angiven information, eftersom tillsynsmyndigheten kommer att ha tillsyn över efterlevandet av bestämmelsen. Enligt vår mening saknas därmed tillräckliga skäl att i lagen införa sanktioner mot lufttrafikföretag för utebliven information till passagerarna.

22.3.6 Utformningen av sanktionsavgiftssystemet

Enligt direktivet ska medlemsstaterna vidta de åtgärder som krävs för att säkerställa att de sanktioner som införs också genomförs. Det finns i dag inga generella förfaranderegler för handläggningen av sanktionsavgifter. Regeringen har dock meddelat riktlinjer för hur sanktionsavgifter ska utformas och användas (se prop. 1981/82:142 s. 24 f.). Sådana riktlinjer följer även av internationella åtaganden.² Vid utformningen av sanktionsavgiftssystemet bör bestämmelserna utformas i

² Se t.ex. Europarådets rekommendation nr R (91) om administrativa sanktionsavgifter.

linje med hur sådana avgifter utformats inom andra rättsområden och de rättssäkerhetskrav som ställs på sanktionsavgift bör få genomslag. Det innebär att sanktionsavgiftssystemet bör regleras i lag och att det av den bör framgå när, hur och av vem sanktionsavgift får tas ut. Systemet ska också vara förutsägbart. Det ska även möta kravet på rimlig handläggningstid, domstolsprövning och en rättssäker process. (Jfr SOU 2017:29 s. 504.)

Ska sanktionsavgift alltid tas ut?

Vårt förslag: Regleringen av sanktionsavgifter ska bygga på strikt ansvar.

Syftet med att införa administrativa sanktionsavgifter är att erhålla ett förenklat och effektivt sanktionsavgiftssystem. Som tidigare framgått är det en förutsättning att sanktionsavgiftssystemet omfattar överträdelse av bestämmelser som typiskt sett är klara och tydliga och att överträdelserna i normalfallet inte kräver någon mer ingående utredning. På så sätt kan en överträdelse leda till en snabb reaktion från samhället i form av en avgift. En avgiftsskyldighet som bygger på strikt ansvar bidrar till en förenkling och effektivisering av sanktionssystemet. Bedömningsinslaget blir betydligt mindre än om det för ansvar skulle krävas oaktsamhet eller uppsåt.

Sanktionsavgiftssystem utformas som huvudregel med strikt ansvar. I API-direktivet anges dock att medlemsstaterna ska införa sanktioner för transportörer som genom fel eller försummelse underlåtit att lämna uppgifter. En annan utformning av sanktionssystemet fick därför användas vid genomförandet av det direktivet. Något krav på att underlåtenheten att överföra PNR-uppgifter ska bero på fel eller försummelse anges inte i PNR-direktivet. Enligt vår mening finns det därför inte skäl att i vårt fall avvika från den grundprincip som gäller för sanktionsavgifter, nämligen att ansvaret ska vara strikt.

Att ansvaret är strikt utesluter inte att myndigheten får avgöra om en överträdelse är så allvarlig att sanktionsavgift bör tas ut. Strikt ansvar innebär endast att uppsåt eller oaktsamhet inte krävs för att sanktionsavgift över huvud taget ska tas ut.

Lagrådet har uttalat att skrivningar om att avgiftsskyldigheten bygger på strikt ansvar inte bör tas med i författningstext. I mot-

sats till vad som gäller för straffbestämmelser finns det nämligen inte något formellt krav på uppsåt eller oaktsamhet för att besluta om sanktionsavgift (se prop. 2012/13:55 s. 142). Vi ser därför inget skäl att införa en sådan bestämmelse.

Avgiftens storlek

Vårt förslag: Avgiften ska uppgå till minst 20 000 kronor och högst 100 000 kronor för varje flygning som har utförts utan att lufttrafikföretaget har fullgjort sin överföringskyldighet.

Ett effektivt sanktionsavgiftssystem innebär att sanktionsavgift ska kunna påföras frekvent och kort tid efter det att överträdelsen ägt rum. För att uppfylla grundläggande rättssäkerhetskrav krävs det också att systemet är förutsebart. Ett sådant system kan åstadkommas endast om det är enkelt att avgöra med vilket belopp som avgiften ska påföras vid varje enskilt tillfälle. Detta innebär att avgiften i viss mån får fastställas schablonmässigt.

Underlåtenhet att överföra API-uppgifter kan, enligt det svenska genomförandet av API-direktivet, medföra en sanktionsavgift om högst 46 000 kronor. Avgiften är bestämd med ledning av den sanktionsavgift på samma belopp som enligt utlänningslagen ska betalas av de transportörer som inte uppfyller sin kontrollskyldighet enligt transportörsansvaret. Avgifterna har sin grund i de EU-direktiv som bestämmelserna genomför.

Den transportör som inte har fullgjort sin kontrollskyldighet enligt det tidigare gällande regelverket om identitetskontroller vid transporter med buss, tåg eller passagerarfartyg, ska betala en sanktionsavgift om 50 000 kronor per transporttillfälle. Sanktionsavgiften är således på förhand bestämd till ett visst belopp. Dock finns det möjlighet för myndigheten att sätta ned avgiften eller avstå från att ta ut den om det finns särskilda skäl för det.

Det är vår bedömning att de möjliga sanktionsavgifterna vid underlåtenhet att överföra PNR-uppgifter, på samma sätt som vid jämförbara sanktionsavgifter riktade mot transportörer, bör bestämmas med ledning av vissa i lagen angivna belopp, och inte knyts till omsättningen av verksamheten, vinsten eller liknande kriterium. Vidare bör avgiftsnivåerna inte i alltför stor grad avvika från de nivåer som

gäller i dag vid underlåten överföring av API-uppgifter. Eftersom inte vi, på det sätt som gällde vid genomförandet av API-direktivet, är bundna av några särskilda nivåer, anser vi att det finns skäl att sätta nivån för den högsta avgift som kan utgå vid underlåten eller felaktig överföring av PNR-uppgifter något högre. Därmed skapas ett visst utrymme för en differentierad avgiftsanvändning. Vi föreslår därför att den högsta avgiften som kan användas bör uppgå till 100 000 kronor. Enligt vår bedömning bör även ett minsta belopp för avgiften införas i lagen, för att ett spann ska kunna föreligga. Eftersom sanktionsavgifterna ska vara avskräckande bör minimibeloppet inte sättas alltför lågt. Enligt vår mening bör den lägsta avgiften som kan åläggas lufttrafikföretagen därför bestämmas till 20 000 kronor. Således bör sanktionsavgiften för varje flygning som har utförts utan att lufttrafikföretaget har fullgjort sin överföringsskyldighet bestämmas till minst 20 000 kronor och högst 100 000 kronor.

Avgifter som motsvarar eller ligger i närheten av maximibeloppet är avsedda för de allvarligare fallen. Det kan röra sig om upprepade överträdelser eller fall som rör ett stort antal passagerare och där ingen rimlig förklaring finns till att de aktuella uppgifterna inte har lämnats. I övriga fall bör en lägre avgift kunna fastställas. Direktivets föreskrift om att sanktionerna ska vara effektiva, proportionella och avskräckande ska dock alltid beaktas.

Sanktionsavgiften bör kunna sättas ned helt eller delvis

Vårt förslag: Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Lufttrafikföretagen kommer normalt sett ha möjlighet att lämna uppgifter i enlighet med direktivets bestämmelser. Det kan emellertid finnas olika orsaker till att ett lufttrafikföretag inte har fullgjort sin överföringsskyldighet. Det kan t.ex. vara så att det har skett ett tekniskt fel vid överföringen av uppgifterna. Vidare kan ett flyg som inte var tänkt att anlända till Sverige oväntat ha omdirigerats hit. Det kan således finnas situationer där det bedöms oskäligt att ta ut en särskild avgift för att lufttrafikföretaget inte har överfört sina PNR-uppgifter. Det behöver därför i lagen finnas en möjlighet att i sådana

situationer sätta ned avgiften helt. Detta följer av våra åtaganden enligt Chicagokonventionen. Vidare bör det i vissa situationer finnas möjlighet att jämka en avgift. Så kan t.ex. vara fallet när en överträdelse av någon orsak bedöms vara ursäktlig.

Således bör det i lagen införas en bestämmelse om att sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

22.3.7 Förfarandet vid beslut om sanktionsavgift

Som tidigare har angetts finns det inte några generella förfaranderegler för handläggningen av sanktionsavgifter. Detta regleras i stället vanligtvis i de författningar som föreskriver att sådana avgifter ska kunna påföras.

Vi har tidigare angett att bestämmelserna om sanktioner mot lufttrafikföretag enligt PNR-systemet så långt som möjligt bör utformas i enlighet med de gällande bestämmelserna om sanktioner vid underlåtenhet att överföra API-uppgifter. API-direktivet är i denna del dock genomfört i utlänningslagen endast genom ett fåtal bestämmelser och någon förordning på området finns ännu inte i bruk. Det är således inte möjligt för oss att på detaljnivå använda samma handläggningsregler som enligt det systemet.

Utredningen om 2016 års dataskyddsdirektiv föreslår, som tidigare framgått, också ett system med sanktionsavgifter, som ska användas vid överträdelser av brottsdatalagens bestämmelser om personuppgiftsbehandling. I brottsdatalagen och i den tillhörande förordningen finns således bestämmelser som hanterar förfarandet vid beslut om sanktionsavgifter. De föreslagna förfarandereglerna i brottsdatalagen och den tillhörande förordningen motsvarar enligt vår mening de rättssäkerhetskrav som kan ställas. Regleringen synes väl avvägd och får anses vara förutsägbar.

Vårt förslag till lag om flygpassageraruppgifter i brottsbekämpningen kommer att utgöra en sektorspecifik särreglering i förhållande till brottsdatalagen i den mån vår lag också utgör en dataskyddsreglering. Dock utgör vår lag även en verksamhetsreglering som i den aktuella frågan ålägger lufttrafikföretagen vissa skyldigheter att överföra PNR-uppgifter. Dessa skyldigheter har inte med dataskydd att

göra, snarare tvärtom. Lufttrafikföretagen utgör inte heller sådana behöriga myndigheter med brottsbekämpande uppgifter som brottsdatalogen uteslutande är tillämplig för. För lufttrafikföretagens personuppgiftsbehandling blir i stället dataskyddsförordningen med anslutande reglering tillämplig.

Av systematiska skäl vore det därför olämpligt att, när det gäller frågan om sanktioner mot lufttrafikföretag, hänvisa till de förfaranderegler som anges i brottsdatalogen och den tillhörande förordningen. Inte heller vore det lämpligt att hänvisa till bestämmelserna i dataskyddsförordningen eller den lagstiftning som kommer att innehålla till dataskyddsförordningen kompletterande bestämmelser. Nödvändiga förfaranderegler får i stället föras in i den av oss föreslagna regleringen.

Ansvarig myndighet

Vårt förslag: Polismyndigheten ska besluta om sanktionsavgift.

Beslut om sanktionsavgift fattas normalt av en tillsynsmyndighet eller en domstol. Som tidigare har angetts är dock ett av syftena med användandet av sanktionsavgifter just att man inte ska behöva gå vägen via en domstol för att kunna använda sanktionen.

Transportstyrelsen utövar tillsyn över lufttrafikföretagen. Det är också den myndigheten som beslutar om sanktionsavgifter vid överträdelser av regelverket om identitetskontroller vid transporter med buss, tåg eller passagerarfartyg. Transportstyrelsens tillsyn över lufttrafikföretagen innebär dock främst att myndigheten övervakar och kontrollerar att krav och regelverk följs av dem som fått ett visst tillstånd. Det kan inte sägas ingå i Transportstyrelsens normala uppdrag att kontrollera att lufttrafikföretagen överför PNR-uppgifter till brottsbekämpande verksamhet.

Om ett lufttrafikföretag inte uppfyller sin överföringsskyldighet enligt vår lag kommer det att vara Polismyndigheten genom enheten för passagerarinformation som upptäcker detta. Polismyndigheten är också den myndighet som enligt dagens system prövar om sanktionsavgift ska betalas av ett lufttrafikföretag som inte har överfört sina API-uppgifter.

Krav på effektivitet och rättssäkerhet måste balanseras mot varandra vid utformningen av ett system om sanktionsavgifter. Om uppgiften att besluta om sanktionsavgift läggs på Polismyndigheten även enligt PNR-systemet kommer frågan att hanteras av den myndighet som har den största sakkunskapen. Handläggningen skulle troligtvis också gå snabbare, eftersom myndigheten redan har tillgång till det material som ett sanktionsbeslut kommer att grundas på.

Enligt vår mening talar övervägande skäl för att Polismyndigheten även bör pröva frågor om åläggande av sanktionsavgift enligt PNR-systemet. En bestämmelse med denna innebörd bör därför föras in i vår lag.

Polismyndighetens beslut om sanktionsavgifter bör få överklagas till allmän förvaltningsdomstol (se nedan). På så sätt tillgodoses rättssäkerhetsaspekterna för den som åläggs sanktionsavgift.

En särskild fråga är vem hos Polismyndigheten som bör pröva frågor om sanktionsavgift. Det har i annat sammanhang ansetts finnas starka skäl – inte minst ur rättsäkerhetssynpunkt – som talar mot att samma person som har utrett en eventuell överträdelse får besluta om sanktionsavgift. Det har ansetts viktigt att verksamheten organiseras så att förtroendet för myndigheten inte riskerar att rubbas. Det har vidare ansetts böra ställas höga krav på den som får besluta sanktionsavgift och det har funnits lämpligt att sådana beslut bara får fattas av ett fåtal personer (se SOU 2017:29 s. 521). Vi delar denna uppfattning. Det kommer därmed fordras att enheten för passagerarinformation gör en utredning och rapportering till Polismyndighetens ledning för beslutsfattande av den som getts behörighet att företräda myndigheten i fråga om sanktionsavgifter. Detta är dock inget som vi ser anledning att föreslå regler kring utan det får vara en intern angelägenhet för Polismyndigheten.

Närmare om handläggningen vid Polismyndigheten

Våra förslag: Innan sanktionsavgift beslutas ska den som anspråket riktas mot ges tillfälle att yttra sig. Sanktionsavgift får inte beslutas om den som ska påföras avgiften inte har getts tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum.

Att beslutet ska delges den som sanktionsavgiften ska tas ut av kan regleras i förordning.

Innan Polismyndigheten beslutar om sanktionsavgift bör lufttrafikföretaget ges tillfälle att yttra sig. Det ger lufttrafikföretaget möjlighet att anföra omständigheter som kan påverka både frågan om sanktionsavgift ska tas ut och frågan om sanktionsavgiftens storlek. Möjligheten att komma till tals innan beslut fattas i frågan är en förutsättning för materiellt riktiga avgöranden och är en viktig rättssäkerhetsfråga.

Det bör finnas en borte gräns för när en sanktionsavgift får beslutas. En regel som anger när avgift senast får beslutas, som blir en form av preskriptionsregel, bör därför tas in i vår lag. Förfarandet är avsett att leda till snabbt beivrande av överträdelser och dessa kan inte anses vara svåra att upptäcka. Preskriptionstiden bör därför sättas kort. Enligt vår bedömning bör preskriptionstiden uppgå till två år, vilket motsvarar den åtalpreskriptionstid som gäller för brott som kan medföra böter eller fängelse i högst ett år. Motsvarande preskriptionstid tillämpas t.ex. vid uttagande av sanktionsavgift från transportörer enligt regelverket om identitetskontroller vid transporter med buss, tåg eller passagerarfartyg.

Utgångspunkten är att avgiften ska betalas kort tid efter beslutet. Polismyndighetens beslut bör därför av rättssäkerhetsskäl delges lufttrafikföretaget. Denna fråga bör kunna regleras i förordning.

Rätt att överklaga

Våra förslag: Polismyndighetens beslut om sanktionsavgift får överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

Ett beslut om att påföra sanktionsavgift bör kunna prövas av domstol. Den som har ålagts sanktionsavgift bör ha rätt att överklaga beslutet. Enligt kommittédirektiven bör ett sanktionssystem vara uppbyggt enligt den struktur som redan gäller i dag, som innebär att en myndighets beslut om sanktioner kan överklagas till allmän förvaltningsdomstol.

Det bör i vår lag införas en bestämmelse som anger att Polismyndighetens beslut om sanktionsavgift får överklagas till allmän förvaltningsdomstol. Av regeln bör framgå att det vid överklagande till kam-

marrätten krävs att domstolen fattar ett beslut om att bevilja prövningstillstånd för att klaganden ska få sitt överklagande prövat i sak.

Betalning och verkställighet

Våra förslag: Sanktionsavgifter ska tillfalla staten. I förordning ska det bl.a. regleras att en sanktionsavgift ska betalas till Polismyndigheten, när en sanktionsavgift ska betalas och vad som gäller vid indrivning.

Polismyndighetens beslut om sanktionsavgift bör gälla som en dom och vara verkställbar. Genom en sådan lösning skapas förutsättningar för en effektiv och snabb handläggning.

Sanktionsavgiften bör som brukligt tillfalla staten. Denna fråga bör regleras i lagen.

Betalningen bör göras inom 30 dagar från det att beslutet fick laga kraft. Betalningen sker lämpligen till Polismyndigheten.

Ett beslut om sanktionsavgift bör få lämnas till indrivning efter sista betalningsdagen. Bestämmelser om indrivning finns i lagen om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

På samma sätt som det bör anges en tidpunkt för när sanktionsavgift inte längre får påföras, bör det också finnas en bortre gräns för när ett beslut om sanktionsavgift får verkställas. När beslutet om sanktionsavgift fått laga kraft bör beslutet verkställas inom fem år. Om så inte blir fallet bör avgiften falla bort till den del den inte har betalats. Dessa frågor kan regleras i förordning.

22.4 Sanktioner vid felaktig behandling av PNR-uppgifter

22.4.1 Dagens sanktionssystem vid felaktig behandling av personuppgifter

I personuppgiftslagen finns flera bestämmelser som innehåller sanktioner mot den som behandlar personuppgifter i strid med lagen. Genom dessa bestämmelser genomförs artikel 24 i det nu gällande

dataskyddsdirektivet. Artikeln i direktivet överlåter till medlemsstaterna att välja sanktioner.

Personuppgiftslagen innehåller dels regler om straffansvar (49 §), dels regler som ger tillsynsmyndigheten rätt att vid vite förbjuda behandling på annat sätt än genom lagring (44 och 45 §§). Det finns även en möjlighet för tillsynsmyndigheten att hos domstol ansöka om att personuppgifter som behandlats på ett olagligt sätt ska utplånas (47 §). Även möjligheten att begära skadestånd brukar ses som en del av sanktionssystemet. I förarbetena till personuppgiftslagen framhöll regeringen att de huvudsakliga sanktionerna mot personuppgiftsansvariga som inte följer lagen är skadestånd och vite. Dessa sanktioner ansågs effektiva och i stort sett tillräckliga (jfr prop. 1997/98:44 s. 104 f.).

22.4.2 Administrativa sanktionsavgifter enligt brottsdatalagen

Även det nya dataskyddsdirektivet överlåter till medlemsstaterna att välja sanktioner. Enligt brottsdatalagen ska tillsynsmyndigheten, på liknande sätt som i dag, ha befogenheter att tillgripa olika medel för det fall personuppgifter behandlas i strid med lag eller annan författning. Befogenheterna ska ses som en trappa som ger tillsynsmyndigheten möjlighet att successivt använda olika medel och därigenom stegra påtryckningarna mot den som inte självmant rättar sig efter myndighetens anvisningar. Befogenheterna sträcker sig från rådgivning och omfattar även möjligheten att meddela förelägganden och besluta om förbud mot fortsatt behandling. Dessa lindrigare befogenheter behandlas i vårt avsnitt 21 om tillsyn. I sista hand har tillsynsmyndigheten en möjlighet att besluta om sanktionsavgift.

Enligt brottsdatalagen ska sanktionsavgifter få tas ut av personuppgiftsansvariga och i vissa fall av personuppgiftsbiträden. Denna reglering är införd i 6 kap. BDL. Sanktionsavgifter ska få tas ut vid överträdelse av de bestämmelser om behandling av personuppgifter i brottsdatalagen som anses viktigast för att värna enskildas integritet, som innehåller de grundläggande reglerna om hur personuppgifter får behandlas och som – om de inte efterlevs – riskerar att leda till allvarliga kränkningar av registrerades integritet. Sanktionsavgift föreslås även få tas ut vid underlåtenhet att bistå tillsyns-

myndigheten eller att rätta sig efter förelägganden eller beslut som myndigheten meddelat. (1 och 2 §§.)

För allvarliga överträdelser ska, enligt 3 §, sanktionsavgiften uppgå till minst 50 000 kronor och högst 20 000 000 kronor. För mindre allvarliga överträdelser ska avgiften uppgå till minst 25 000 kronor och högst 10 000 000 kronor. Om flera bestämmelser har överträtts genom samma personuppgiftsbehandling, eller om en eller flera bestämmelser har överträtts genom sammankopplade personuppgiftsbehandlings, ska sanktionsavgiften kunna bestämmas efter överträdelsernas allvar. Sanktionsavgiften får dock aldrig överstiga maximibeloppet för den allvarligaste överträdelser.

Till mindre allvarliga överträdelser räknas att tillgången till personuppgifter inte har begränsats internt. Enligt Utredningen om 2016 års dataskyddsdirektiv är risken för kränkning av den enskildes integritet då mindre än om uppgifterna sprids utanför verksamheten eller behandlas otillåtet på annat sätt. Till mindre allvarliga överträdelser bör enligt utredningen också räknas underlåtenhet att anmäla eller dokumentera personuppgiftsincidenter. Även en underlåtenhet att göra en konsekvensbedömning eller att inleda ett förhandssamråd med tillsynsmyndigheten anses som mindre allvarlig. Övriga överträdelser, som utgör den övervägande majoriteten av de överträdelser som enligt förslaget kan leda till sanktionsavgift, ska räknas som allvarliga överträdelser. (Se SOU 2017:29 s. 515.)

Strikt ansvar ska gälla för överträdelserna. Avsikten med överträdelserna ska dock vägas in när tillsynsmyndigheten överväger frågan om sanktionsavgift ska påföras och bestämmer dess storlek. Vid bedömningen av om sanktionsavgift ska tas ut och till vilket belopp sanktionsavgiften ska bestämmas, ska, enligt 4 §, särskild hänsyn även tas till vilken skada, fara eller kränkning som överträdelserna inneburit, dess karaktär, svårhetsgrad och varaktighet och vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa skadan. Om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts sanktionsavgift ska det vägas in.

Sanktionsavgiften får sättas ned helt eller delvis om överträdelserna är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften (5 §).

Det är tillsynsmyndigheten som ska besluta om sanktionsavgift (6 §). Sanktionsavgiften ska som brukligt tillfalla staten. Den som ska påföras sanktionsavgift ska ges tillfälle att yttra sig innan till-

synsmyndigheten fattar sitt beslut (7 §). Beslutet får överklagas till allmän förvaltningsdomstol (7 kap. 4 §).

I brottsdataförordningen finns ytterligare förfaranderegler om delgivning, betalning, verkställighet, preskription och återbetalning.

Enligt utredningens förslag ska överträdelse av reglerna om personuppgiftsbehandling i brottsdatalagen inte medföra straffrättsliga påföljder, utöver vad som gäller enligt brottsbalken. Vite föreslås inte heller användas i brottsdatalagen.

22.4.3 Sanktionsavgiftssystemet i brottsdatalagen bör användas

Våra förslag: Administrativ sanktionsavgift får tas ut av personuppgiftsansvariga myndigheter vid överträdelse av de bestämmelser i lagen som har till syfte att skydda enskildas integritet.

Vid bestämmande av sanktionsavgiftens storlek och i handläggningsfrågor ska sanktionsavgiftssystemet i brottsdatalagen och den tillhörande förordningen tillämpas. Beslut om sanktionsavgift kan överklagas till allmän förvaltningsdomstol enligt 7 kap. 4 § BDL.

Våra överväganden och förslag

Allmänna utgångspunkter

Som tidigare har framgått innehåller PNR-direktivet såväl en verksamhetsreglering med bestämmelser om hur PNR-uppgifterna ska användas i brottsbekämpningen, som en dataskyddsreglering med bestämmelser som har till avsikt att skydda resenärernas personliga integritet vid myndigheternas behandling av uppgifter om dem. Som vi ser det innebär direktivets krav på sanktioner i denna del att det ska finnas bestämmelser i nationell rätt som tillser att direktivets dataskyddsreglering efterlevs av de myndigheter som behandlar PNR-uppgifter. Sådana sanktioner bör kunna träffa såväl den behandling av PNR-uppgifter som utförs vid enheten för passagerarinformation som vid de behöriga myndigheter som därefter får tillgång till PNR-information. Om enheten för passagerarinforma-

mation exempelvis inte gallrar PNR-uppgifter i rätt tid eller om de behöriga myndigheterna, utan stöd i den särskilda bestämmelsen om det, skulle komma att använda PNR-uppgifterna för bekämpande av annan brottslighet än den som avses i direktivet, ska det således finnas sanktioner att tillgripa.

Utredningen om 2016 års dataskyddsdirektiv har föreslagit att administrativa sanktionsavgifter ska användas mot den som behandlar personuppgifter i strid med vissa närmare bestämmelser i brottsdatalagen. Det finns stora effektivitetsvinster med att använda sig av samma sanktionssystem i vår lag som i den föreslagna brottsdatalagen. På så sätt undviks införandet av en onödigt dubbelreglering. För de tillämpande myndigheterna vore det också av värde om samma sanktioner kan följa på all otillåten behandling av personuppgifter inom det brottsbekämpande området. Det sanktionssystem som föreslås av Utredningen om 2016 års dataskyddsdirektiv synes därtill vara lämpligt och väl avvägt. Någon annan sanktionsmöjlighet än sanktionsavgifter föreslås inte heller vid överträdelser av bestämmelserna om personuppgiftsbehandling på det brottsbekämpande området. Enligt vår mening bör således sanktionsavgifter användas även vid överträdelser av de bestämmelser om personuppgiftsbehandling som genomför PNR-direktivet. Vidare bör det sanktionssystem som föreslås i brottsdatalagen vara tillämpligt även vid överträdelser av bestämmelserna i vår lag. Med hänsyn till legalitetsprincipen och sanktionsavgifternas straffrättsliga karaktär bör det dock direkt av vår lag framgå vilka förfaranden enligt lagen som kan leda till sanktionsavgift. Det bör vidare framgå vem som ska kunna åläggas sanktionsavgift samt med vilket belopp.

För vilka överträdelser ska sanktionsavgift tas ut?

De bestämmelser i vår lag som bör föranleda sanktionsavgift är som utgångspunkt de som innehåller grundläggande regler om hur PNR-uppgifterna får behandlas och som därför får anses viktigast för att värna enskildas integritet. Med det som utgångspunkt bör enligt utredningens mening överträdelser av följande skyldigheter föranleda sanktionsavgift.

Bestämmelsen om att PNR-uppgifter inte får behandlas för andra syften än att förebygga, förhindra, upptäcka, utreda eller lagföra

terroristbrottslighet eller grov brottslighet är av så grundläggande natur att överträdelser av den bör föranleda sanktionsavgift. Det samma gäller för överträdelser av förbudet mot behandling av känsliga personuppgifter.

Vidare bör överträdelser av bestämmelserna om hur enheten för passagerarinformation får behandla PNR-uppgifter kunna leda till sanktionsavgift. Här inräknas lagens ändamålsbestämmelser och bestämmelser som begränsar tillgången till PNR-information och förbjuder direktåtkomst. Även överträdelser av lagens bestämmelser om bevarande och gallring bör kunna föranleda sanktionsavgift samt överträdelser av bestämmelserna om maskering av PNR-uppgifter och överföring av avmaskerade PNR-uppgifter. Även överträdelser av bestämmelser om hur PNR-uppgifter får användas vid de behöriga myndigheterna bör kunna bli föremål för sanktionsavgift. Slutligen bör, på samma sätt som i brottsdatalagen, de bestämmelser som begränsar möjligheten att överföra uppgifter till tredjeland kunna bli föremål för sanktionsavgift.

De bestämmelser som innebär att PNR-uppgifter ska överföras till behöriga myndigheter, andra medlemsstater och Europol utgör en ren verksamhetsreglering som enligt vår mening inte bör föranleda sanktionsavgifter. Inte heller bör underlåtenhet att utse dataskyddsombud föranleda sanktionsavgift. Liksom Utredningen om 2016 års dataskyddsdirektiv anser vi att det är tillräckligt att det i brottsdatalagen finns en skyldighet att anmäla att ombud har utsetts och entledigats till tillsynsmyndigheten. Om en personuppgiftsansvarig inte skulle fullgöra den skyldigheten, kan tillsynsmyndigheten reagera och t.ex. utfärda ett föreläggande.

För det fall det inom enheten för passagerarinformation skulle ske överträdelser av andra tillämpliga dataskyddsbestämmelser än de som anges i vår lag, t.ex. bestämmelserna i brottsdatalagen, blir de sanktionsbestämmelser som anges i de lagarna tillämpliga.

Vem ska träffas av sanktionsavgift?

En personuppgiftsansvarig bär ansvaret inte bara för sin egen personuppgiftsbehandling utan även för den behandling ett personuppgiftsbiträde eller någon annan som behandlar personuppgifter på den personuppgiftsansvariges vägnar utför, dvs. anställda, personer

som är att jämställa med anställda (inhyrd personal) eller uppdragstagare. För den behandling av PNR-uppgifter som enheten för passagerarinformation utför, är det Polismyndigheten som är personuppgiftsansvarig. De behöriga myndigheterna har personuppgiftsansvaret för den behandling som de utför. För Polismyndighetens del kommer personuppgiftsansvaret för behandling av personuppgifter enligt den nya lagen således att omfatta både enhetens behandling och den behandling enligt lagen som myndigheten utför med den PNR-information som mottagits från enheten.

Enligt brottsdatalagen får sanktionsavgift tas ut av en personuppgiftsansvarig. Även personuppgiftsbiträden ska enligt förslaget kunna påföras sanktionsavgift i vissa fall, dock endast när de har uttryckliga skyldigheter som framgår direkt av författning.

Eventuella personuppgiftsbiträden som kan komma att anlitas av enheten för passagerarinformation eller av behöriga myndigheter kommer inte att ha några uttryckliga skyldigheter enligt vår reglering. Det är därför tillräckligt att i vår lag ange att sanktionsavgifter kan åläggas den personuppgiftsansvariga myndigheten. Dock kommer bestämmelserna i brottsdatalagen om personuppgiftsbiträdens skyldigheter att vara tillämpliga även vid enheten för passagerarinformation i förekommande fall.

Storleken på sanktionsavgifterna

Sanktionsavgift kan enligt brottsdatalagen tas ut enligt två nivåer; en lägre nivå vid överträdelser som betraktas som mindre allvarliga och en högre nivå vid allvarligare överträdelser. Den högre nivån föreslås gälla för de flesta överträdelser.

Enligt vår mening bör överträdelser av samtliga aktuella bestämmelser i den av oss föreslagna lagen anses vara så allvarliga att den högre nivån enligt brottsdatalagen bör tillämpas. Detta gäller även för skyldigheten att internt inom Polismyndigheten begränsa tillgången till PNR-information som behandlas vid enheten för passagerarinformation. Vilken sanktionsnivå som kan bli aktuell bör uttryckligen framgå av lagen.

Utgångspunkten vid bestämmandet av sanktionsavgift är den behandling som skett av personuppgifterna. Det är möjligt att ett agerande i strid med vår lag skulle kunna föranleda sanktionsavgift

enligt såväl vår lag som enligt den mer generella regleringen i brottsdatalagen. Tanken är inte att ett sådant agerande ska leda till dubbla sanktionsavgifter. Dock bör ett sådant agerande kunna föranleda en högre sanktionsavgift. Frågan får avgöras från fall till fall av tillsynsmyndigheten.

I övrigt bör brottsdatalagens bestämmelser vara tillämpliga

Bestämmelserna om handläggningen av sanktionsavgifter i brottsdatalagen och den tillhörande förordningen bör i övrigt vara tillämpliga även vid överträdelser av de angivna bestämmelserna i vår lag. Särskilda bestämmelser om handläggningen behöver därför inte föras in i våra författningsförslag. En hänvisning till aktuella bestämmelser i brottsdatalagen och den tillhörande förordningen är tillräcklig. Dessutom föreslår vi att det förs in en upplysning om att det i 7 kap. 4 § BDL föreskrivs att beslut om sanktionsavgifter kan överklagas till allmän förvaltningsdomstol.

23 Bestämmelser i direktivet som inte kräver lagstiftningsåtgärder

Vår bedömning: Artiklarna 17 och 19–22 i direktivet kräver inga lagstiftningsåtgärder.

Det har i tidigare avsnitt framkommit i vilken mån de behandlade artiklarna i direktivet bör bli föremål för lagstiftningsåtgärder. Vi har där i några fall gjort bedömningen att vissa bestämmelser inte behöver föranleda författningsreglering. Därutöver innehåller direktivet artiklar som inte överhuvudtaget behöver omsättas i lagstiftning. Således kräver inte artikel 17 om kommittéförfarande, artikel 19 om översyn, artikel 20 om statistik, artikel 21 om förhållandet till andra instrument samt artikel 22 om direktivets ikraftträdande några lagstiftningsåtgärder.

24 Sekretess

24.1 Vårt uppdrag i denna del

PNR-direktivet innehåller inga bestämmelser om sekretess. Däremot innebär direktivet begränsningar i för vilka ändamål PNR-information får användas. Vidare hänvisas i artikel 13.2 till att de nationella bestämmelser om konfidentiell behandling som har antagits för genomförande av artikel 21 i dataskyddsrambeslutet ska vara tillämpliga på all behandling av personuppgifter enligt PNR-direktivet. I skäl 30 anges att direktivet inte påverkar tillämpningen av principen om allmänhetens tillgång till officiella handlingar.

Enligt kommittédirektiven ska vi ta ställning till om reglerna i offentlighets- och sekretesslagen innebär ett tillräckligt skydd för de uppgifter som ska utbytas enligt PNR-direktivet eller om nuvarande lagstiftning behöver ändras för att Sverige ska leva upp till bestämmelserna i direktivet. I uppdraget ingår också att föreslå en reglering för sekretess som passar in i den befintliga svenska strukturen och ger en rättssäker och mer effektiv brottsbekämpning, samtidigt som skyddet för den personliga integriteten säkerställs.

Vi har tolkat vårt uppdrag i denna del på så sätt att vi bör behandla frågor om sekretesskydd för

- PNR-uppgifter som enheten för passagerarinformation mottar från lufttrafikföretag och resultaten av enhetens behandling av sådana uppgifter, samt
- PNR-information som enheten för passagerarinformation mottar från enheter eller behöriga myndigheter i andra medlemsstater.

Vi har dessutom sett det som en uppgift för oss att behandla frågan om det finns behov av sekretessbrytande bestämmelser för att möjliggöra det utbyte av PNR-information som direktivet syftar till.

Som vi tidigare redogjort för behandlar vi inte frågor om enheten för passagerarinformations tillgång till register, databaser eller andra informationskällor, se avsnitt 10.5. Följaktligen behandlar vi inte heller eventuella behov av sekretessgenombrott för sådan informationsinhämtning som enheten för passagerarinformation kan komma att vilja göra sedan den börjat arbeta med PNR-information efter ikraftträdandet.

24.2 Sekretess i brottsbekämpande verksamhet m.m.

Uppgifter inom Polismyndighetens, Säkerhetspolisens, Tullverkets, Ekobrottsmyndighetens och Försvarmaktens verksamheter omfattas av bestämmelserna i offentlighets- och sekretesslagen. Detsamma gäller för andra myndigheter som i framtiden kan komma att utses som behöriga myndigheter enligt den nya lagen.

Sekretess gäller i förhållande till såväl enskilda (fysiska eller juridiska personer) som andra myndigheter (8 kap. 1 § OSL). Uppgifter som skyddas av sekretess får inte lämnas ut till en enskild eller annan myndighet utan stöd i offentlighets- och sekretesslagen. Detsamma gäller visavi utländska myndigheter. Enligt 8 kap. 3 § OSL får en uppgift för vilken sekretess gäller bara röjas för en utländsk myndighet eller en mellanfolklig organisation, om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning (punkten 1), eller uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen (punkten 2). I bestämmelsen görs det ingen skillnad mellan myndigheter i EU:s medlemsstater eller i tredjeländer.

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligt, genom utlämnande av allmän handling eller på något annat sätt (3 kap. 1 § OSL). Sekretess innebär således både handlingssekretess och tystnadsplikt.

De viktigare materiella sekretessbestämmelserna

Offentlighets- och sekretesslagen innehåller en stor mängd sekretessbestämmelser som kan bli tillämpliga för aktuella myndigheter. Vissa gäller generellt för alla myndigheter, t.ex. bestämmelserna om utrikes- eller försvarssekretess i 15 kap. 1 och 2 §§ OSL, vilka i detta sammanhang torde vara av särskild relevans för Försvarsmakten. Andra generella bestämmelser skyddar känsligare uppgifter om enskilda och finns i 21 kap. OSL. Flertalet sekretessbestämmelser har emellertid en avgränsad räckvidd som innebär att de bara gäller inom exempelvis viss verksamhet eller vid viss myndighet. I det följande redovisar vi enbart ett urval bestämmelser som vi bedömt särskilt relevanta att beröra för de frågeställningar som behandlas i detta kapitel. Det ska alltså observeras att redovisningen nedan är långt ifrån fullständig.

Sekretess till skydd för allmänna intressen

Sekretessbestämmelser till skydd för intresset av att förebygga eller beivra brott finns i 18 kap. OSL. Enligt 18 kap. 1 § gäller sekretess för uppgift som hänför sig till en förundersökning i brottmål eller angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott. Enligt andra stycket 2 gäller sekretess även för uppgifter som hänför sig till annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av bl.a. Polismyndigheten, Säkerhetspolisen och Tullverket. Även åklagarmyndighet omfattas av bestämmelsen vilket i sammanhanget innebär att också Ekobrottsmyndigheten omfattas av bestämmelsens räckvidd. Det som åsyftas med andra stycket 2 är brottsförebyggande och brottsbeivrande verksamhet i allmänhet utan anknytning till något konkret fall. Sekretessen gäller exempelvis för uppgifter hänförliga till spaningsmetoder och för sådana uppgifter som finns i de register som används i polisär verksamhet. För uppgifter i t.ex. Polismyndighetens verksamhet för att förebygga brott etc. som hänför sig till underrättelseverksamhet ska dock 18 kap. 2 § tillämpas.¹ Bestämmelserna i 18 kap. 1 § har ett rakt skaderekvisit, som har konstruerats så att sekretessen gäller endast om följden av

¹ Lenberg m.fl., Zeteo juli 2016, kommentaren till 18 kap. 1 § OSL.

att uppgifterna lämnas ut kan antas bli att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Vidare gäller enligt 18 kap. 2 § sekretess för uppgift som hänför sig till bl.a. sådan verksamhet som avses i 2 kap. 7 § 1 (förebygga, förhindra eller upptäcka brottslig verksamhet) eller 6 kap. 1 § 1 PDL (förebygga, förhindra eller upptäcka viss slags brottslig verksamhet som innefattar t.ex. terrorbrott). Det polisarbete som åsyftas är i första hand underrättelseverksamhet, dvs. arbete med insamling, bearbetning och analys av information för att förhindra eller upptäcka brottslig verksamhet när det inte finns konkreta misstankar om att ett visst brott har begåtts. Polisarbete som är inriktat på en redan begången individualiserad gärning faller inte in under punkten (se prop. 2009/10:85 s. 318). Sekretessen för uppgifterna enligt bestämmelsen i polisdatalagen gäller enligt 18 kap. 2 § OSL med ett omvänt skaderekvisit, vilket innebär att uppgifterna inte får lämnas ut om det inte står klart att de kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Enligt andra stycket 2 gäller motsvarande sekretess för uppgifter som hänför sig till Tullverkets underrättelseverksamhet.

Det kan påpekas att sekretessen enligt 18 kap. 1 och 2 §§ OSL även gäller hos myndigheter som inte bedriver brottsbekämpande verksamhet. Det beror på att sekretessen, enligt paragraferna, avser uppgifter *som hänför sig till* förundersökning och underrättelseverksamhet m.m. som bedrivs av de i paragraferna angivna brottsbekämpande myndigheterna. Sekretessen enligt 18 kap. 1 eller 2 § kan därmed sägas, i bildlig mening, följa med när den lämnas vidare till en helt annan slags myndighet.

Sekretessen till skydd för brottsbekämpande verksamhet gäller enbart svensk sådan verksamhet. Därför har en särskild bestämmelse, som skyddar utländsk brottsbekämpande verksamhet, införts i 18 kap. 17 § OSL. Sekretess gäller i verksamhet som avser visst rättsligt samarbete samt utbyte inom ramen för Schengens informationssystem. Regeringen har i en lagrådsremiss som beslutades den 4 maj 2017 föreslagit en ny sekretessbestämmelse, 18 kap. 17 a §, enligt vilken sekretess ska gälla hos brottsbekämpande myndigheter för uppgift som lämnats av ett utländskt organ vid internationellt polisiärt samarbete i syfte att förebygga, uppdaga, utreda eller beivra brott, om det kan antas att en förutsättning för att uppgiften lämnades var att den inte

skulle röjas. Syftet med bestämmelsen är att göra sekretesskyddet för uppgifter som mottas i samarbetet tydligare och mer heltäckande. Lagändringen föreslås träda i kraft den 1 december 2017.

Sekretess till skydd för enskildas intressen

Sekretess till skydd för enskildas personliga och ekonomiska förhållanden i sådan verksamhet som syftar till att förebygga eller beivra brott regleras huvudsakligen i 35 kap. OSL. Med begreppet ”enskilda” avses såväl fysiska som juridiska personer.

Sekretessen enligt 35 kap. 1 § OSL skyddar enskilds personliga och ekonomiska förhållanden i bl.a. förundersökningar, brottsförebyggande verksamhet och vissa polisiära register m.m. Enligt första stycket 4 gäller sekretess för uppgift i annan verksamhet (annan än bl.a. förundersökning som regleras i punkten 1) som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs bl.a. av åklagarmyndighet (t.ex. Ekobrottsmyndigheten, se ovan), Polismyndigheten, Säkerhetspolisen och Tullverket. Genom bestämmelsen blir det möjligt att hemlighålla uppgifter som mera allmänt hänför sig till de i bestämmelsen uppräknade myndigheternas brottsbekämpande verksamhet. Bestämmelsen är bl.a. tillämplig på sådana personregister som förs inom myndigheterna och som inte omfattas av särskilda bestämmelser (bl.a. punkterna 6, 7 och 10 i denna bestämmelse och 3 §). Även behandling av personuppgifter som inte sker i register omfattas av bestämmelsen. Enligt punkten 6 gäller sekretess för uppgifter i register som förs av Polismyndigheten enligt 4 kap. PDL eller som annars behandlas med stöd av de bestämmelserna. De register som avses är register över DNA-profiler, fingeravtrycks- och signalementsregister, penningtvättsregister och det internationella registret. Enligt punkten 7 gäller sekretess för uppgifter i register som förs enligt lagen om misstankeregister. Register som förs av Tullverket omfattas av punkten 10. Sekretessen enligt bestämmelsen i 35 kap. 1 § första stycket gäller om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående lider skada eller men. Presumtionen är alltså att sekretess gäller.

Bestämmelser om sekretess för Polismyndighetens register finns vidare i 35 kap. 3 och 4 §§. I 3 § regleras sekretessen för uppgifter i belastningsregistret. I 4 § regleras sekretessen för ytterligare några

register, bl.a. register över strafföreläggande och föreläggande av ordningsbot. Sekretessen enligt såväl 3 och 4 §§ är absolut, dvs. något skaderekvisit ställs inte upp som villkor för sekretessen.

Minimiskyddsregler till skydd för enskildas personliga integritet finns i 21 kap. OSL. I 21 kap. 5 § regleras sekretess för särskilt känsliga uppgifter om utlänningar. Bestämmelsen tar sikte på varje slag av uppgifter som rör utlänningar, oavsett i vilket sammanhang uppgifterna förekommer. För sekretess krävs att det kan antas att röjande av uppgiften skulle medföra att någon utsätts för övergrepp eller annat allvarligt men. Dessutom fordras att risken för skada ska vara föranledd av förhållandet mellan utlänningen och utländsk stat eller myndighet eller organisation av utlänningar.

Särskilt om gällande sekretessbestämmelser för API-uppgifter

Vid genomförandet av API-direktivet ansågs det saknas sekretessbestämmelser till skydd för svenska medborgares personliga förhållanden liksom en bestämmelse till skydd för enskildas – och då särskilt juridiska personers – ekonomiska förhållanden (se prop. 2005/06:129 s. 51).

I förarbetena till lagstiftningen om s.k. trängselskatt gjordes vissa uttalanden avseende möjligheten att kartlägga en persons förflyttningar in och ut ur ett område (prop. 2003/04:145 s. 103). Det anfördes bl.a. att det är angeläget att den enskildes integritet värnas så långt det är möjligt inom ramen för systemet med trängselskatt och att möjligheten att kartlägga en persons förflyttningar in och ut ur ett område som omfattas av trängselskatt därför ska förhindras. Mot denna bakgrund gjorde regeringen den bedömningen att det var nödvändigt att undanta vissa uppgifter i de aktuella beskattningsbesluten från offentlighet. Dessa var uppgift om vilken betalstation bilen har passerat och om tidpunkten för denna passage. För dessa uppgifter råder absolut sekretess.

Vid genomförandet av API-direktivet hänvisades till ovan nämnda uttalanden i förarbetena till lagstiftningen om trängselskatt. Med hänsyn till den enskildes integritet och för att förhindra möjligheten att kartlägga personers förflyttningar, infördes en absolut sekretessbestämmelse till skydd för uppgifter om personers namn och födelsedatum i passagerarregistret. Med hänsyn till att passnummer

eller nummer på identitetskort kan användas för att utröna en passagerares namn och födelsedatum, omfattar sekretessskyddet även nummer på resehandlingen. (Se prop. 2005/06:129 s. 50 ff.).

Uppgifterna i passagerarregistret betraktades i övrigt typiskt sett som harmlösa. Till detta kom att uppgifterna i det registret ska gallras relativt snabbt om det inte finns särskilda omständigheter. Det ansågs dock kunna finnas uppgifter eller sammanställningar som kan missbrukas eller som i ett särskilt fall kan användas till skada för den uppgiften rör. Detta ansågs särskilt gälla uppgifter om enskildas, främst transportörernas, ekonomiska förhållanden. Som exempel angavs flygplanens beläggning, vilken kan utläsas om uppgifter om det totala antalet passagerare jämförs med antalet platser i det aktuella flygplanet. Eftersom det ansågs kunna finnas risk för att enskilda lider skada om uppgifter om deras ekonomiska förhållanden röjs, infördes en möjlighet att sekretessbelägga uppgifter i passagerarregistret till skydd för enskilds förhållanden av ekonomisk natur. För dessa uppgifter ansågs det tillräckligt med en presumtion för offentlighet där sekretess endast gäller om det kan antas att den enskilde lider skada om uppgiften röjs. (Se prop. 2005/06:129 s. 50 ff.).

I anlutning till lagen (2006:444) om passagerarregister infördes således en bestämmelse om sekretess för vissa uppgifter i det register som förs enligt lagen. Bestämmelsen, som numera återfinns i 32 kap. 7 § OSL, stadgar att sekretess gäller i verksamhet som avser förande av eller uttag ur register enligt lagen om passagerarregister för uppgift om enskilds namn och födelsedatum samt nummer på resehandling. Sekretessen är i denna del absolut. Sekretess gäller också för uppgift om en enskilds ekonomiska förhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs. I denna del gäller sekretessen således med ett s.k. rakt skaderekvisit.

Sekretessbrytande bestämmelser

I offentlighets- och sekretesslagen finns ett flertal bestämmelser som möjliggör utbyte av uppgifter mellan myndigheter trots den sekretess som annars gäller för uppgifterna. Många av generell räckvidd finns i 10 kap.

Av 10 kap. 2 § OSL framgår att sekretessbelagda uppgifter får lämnas från en myndighet till en annan om det är nödvändigt för att

den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen, som är avsedd att tillämpas restriktivt, medger inte sekretessgenombrott på den grunden att den mottagande myndigheten behöver uppgifterna i sin verksamhet.

Enligt 10 kap. 28 § första stycket hindrar sekretess inte att uppgifter lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Med lag avses även en EU-förordning. Det är mycket vanligt förekommande med sekretessbrytande bestämmelser om uppgiftsskyldighet, exempelvis i registerförfattningar som syftar till att möjliggöra direktåtkomst mellan myndigheter. Ett exempel på en sådan är 2 kap. 16 § PDL som föreskriver att vissa myndigheter med brottsbekämpande uppgifter trots sekretess enligt 21 kap. 3 § första stycket (enskilds adress, kontaktuppgifter m.m.) och 35 kap. 1 § OSL har rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga, om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet. Uppgifter kan vidare, med vissa undantag, lämnas ut med stöd av 10 kap. 18 a–26 §§, när uppgifterna behövs för olika i paragraferna angivna ändamål inom brottsbekämpningen, bl.a. förundersökning.

Enligt 10 kap. 27 §, den s.k. generalklausulen, gäller som huvudregel att en uppgift får lämnas ut till en annan myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Undantag görs dock för vissa sekretessregler som är av begränsat intresse här. Har det i en lag eller förordning föreskrivits att uppgifter ”bör” eller ”får” lämnas från en myndighet till en annan, finns det normalt särskild anledning att anse att generalklausulen är tillämplig.² En annan bestämmelse av generell innebörd är 12 kap. 1 § OSL enligt vilken sekretess till skydd för enskild inte annat än i undantagsfall gäller i förhållande till den enskilde själv. Samma uppgift om den enskilde kan emellertid skyddas också av sekretess för ett annat intresse, t.ex. brottsbekämpningens enligt 18 kap., vilket då kan medföra att den enskilde inte har någon rätt att få ut uppgiften om sig själv.

I anslutning till offentlighets- och sekretesslagens materiella sekretessbestämmelser finns inte sällan ytterligare sekretessbrytande bestämmelser som gäller just den aktuella sekretessen i fråga. En sådan är 35 kap. 10 § OSL. Av den bestämmelsen följer att sekretessen

² Lenberg m.fl., Zetec juli 2016, kommentaren till 10 kap. 27 § OSL.

enligt 1 § i samma kapitel inte hindrar att en uppgift lämnas ut bl.a. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister och polisdatalagen eller förordningar som har stöd i dessa lagar. Denna sekretessbrytande bestämmelse har bl.a. införts för att myndigheterna inte ska behöva förlita sig på en sekretessprövning enligt generalklausulen i 10 kap. 27 § OSL. Bestämmelsen medför också en möjlighet att lämna ut uppgifter till enskilda eller till andra stater enligt vad som föreskrivs i de i bestämmelsen angivna författningarna (jfr 8 kap. 3 § OSL). En ytterligare i förhållande till 35 kap. 1 § sekretessbrytande bestämmelse är 35 kap. 10 a § enligt vilken sekretessen i 1 § inte hindrar att uppgift om en enskild lämnas mellan Polismyndigheten och Säkerhetspolisen, om den mottagande myndigheten behöver uppgiften i sin brottsbekämpande verksamhet.

Även här kan påpekas att redogörelsen ovan är ofullständig.

24.3 Våra överväganden

24.3.1 Skyddet för PNR-information hos enheten för passagerarinformation

Vår bedömning: Sekretessregleringen i 18 kap. 1 och 2 §§ samt 35 kap. 1 § första stycket 4 OSL ger ett tillfredsställande skydd för PNR-uppgifter som kommer in från lufttrafikföretagen för att lagras i PNR-databasen och även vid senare användning inom enheten. PNR-uppgifter som överförts från andra medlemsstater omfattas också av denna sekretessreglering liksom sådana träffar, analyser och andra resultat som tas fram inom enheten eller kommer in till enheten genom det internationella utbytet för vidare granskning av svenska behöriga myndigheter. Någon ny eller ändrad sekretessreglering, t.ex. avseende sekretessens styrka, är därför inte motiverad.

I PNR-databasen hos enheten för passagerarinformation kommer det att lagras PNR-uppgifter från miljontals flygpasagerare. Som vi tidigare berört innebär PNR-systemet en massregistrering som potentiellt sett möjliggör en kartläggning av enskildas flygresande till och från Sverige. Även om uppgifterna sedda var för sig ofta kan te sig harmlösa finns det därför ett behov av sekretesskydd för

att skydda passagerarnas personliga integritet. Bland uppgifterna kan också finnas en del skyddsvärda ekonomiska uppgifter såsom bank- eller kontokortsinformation. Likaså kan lufttrafikföretagen, researrangörer och resebyråer ha kommersiella intressen av att PNR-uppgifter som emanerar från dem inte blir offentligt tillgängliga och sammanförda med konkurrenters motsvarande uppgifter.

För det allmännas intresse av sekretesskydd för den brottsbekämpande verksamheten torde det stora flertalet PNR-uppgifter i och för sig kunna röjas för vem som helst utan skada för verksamheten. De allra flesta uppgifter som enheten för passagerarinformation mottar från lufttrafikföretagen avser ju passagerare av intet intresse för bekämpningen av terroristbrottslighet eller grov brottslighet. Däremot säger det sig själv att ett röjande av träffar som fås fram vid enhetens förhandsbedömningar liksom annat resultat av enhetens bearbetning och analys av PNR-uppgifterna kan antas skada kommande insatser som grundas på denna information. Detsamma gäller för PNR-information som mottagits från andra medlemsstater som bedömt att det finns anledning för Sverige att undersöka denna vidare. Även framtagna riskkriterier torde behöva skyddas från offentlighet för att det långsiktiga brottsbekämpande arbetet vid enheten och hos behöriga myndigheter inte ska störas.

Arbetet vid enheten för passagerarinformation går med ett sammanfattande ord ut på att informationsförsörja den brottsbekämpande verksamheten och är därmed en del av Polismyndighetens verksamhet med att förebygga, förhindra, upptäcka och utreda brott. Som sådan är det vår bedömning att uppgifter som behandlas i PNR-databasen vid enheten kommer att omfattas av de sekretessbestämmelser i 18 kap. 1 och 2 §§ samt 35 kap. 1 § första stycket 4 OSL som vi redogjort för ovan. Vad gäller den sistnämnda bestämmelsen kommer den att reglera inte bara uppgifter i PNR-databasen utan även andra uppgifter om enskilda som enheten behandlar enligt den nya lagen. Sekretessen enligt 35 kap. 1 § gäller, om det inte står klart att en uppgift kan röjas utan att den enskilde eller någon närstående lider skada eller men. Det kan för övrigt nämnas att de bokningsuppgifter som inhämtas i dag med stöd av bestämmelserna i 25 och 26 §§ polislagen (1984:387) också anses omfattas av sekretesskyddet i bestämmelserna i 18 och 35 kap. OSL under den tid de förvaras hos Polismyndigheten (jfr prop. 1996/97:175 s. 68). Såvitt vi nu kan bedöma torde det inte bli aktuellt att PNR-information skulle omfattas av

sekretess enligt 21 kap. 5 § OSL till skydd för utlänningars säkerhet, men vi kan inte helt utesluta det i särskilda fall.

När det gäller sekretessen enligt 18 kap. 1 eller 2 § OSL kan det inte på ett enkelt sätt anges om den ena eller andra paragrafen är tillämplig i olika fall och mycket talar för att båda bestämmelserna ibland är parallellt tillämpliga. Enligt vår uppfattning kan det bero på den aktuella situationen. Själva lagringen av PNR-uppgifter (vilket kan komma att avse minst 28 miljoner flygpassagerarresor per år) torde kunna ses som en sådan annan verksamhet som *syftar till* att förebygga, uppdaga, utreda eller beivra brott som avses i 18 kap. 1 § andra stycket 2. Enligt vår mening talar emellertid det mesta för att förhandsbedömningar, träffar och resultat från behandlingar för att t.ex. besvara en särskild begäran från underrättelseenheter vid behöriga myndigheter omfattas av den starkare sekretessregleringen i 18 kap. 2 § första stycket. Däremot torde resultat av behandlingar som gjorts för att besvara en förfrågan om att hämta in PNR-information i en förundersökning inte höra hemma i 18 kap. 2 §. Det är dock under alla förhållanden vår slutsats att det allmännas intresse och behov av sekretesskydd för enhetens PNR-information är väl tillgodosett genom 18 kap. 1 och 2 §§ även om det i det enskilda fallet inte är alldeles enkelt att bedöma om det är den ena eller andra paragrafen eller båda som ska tillämpas parallellt.

Sekretessregleringen inom det brottsbekämpande området, inte minst när det får internationella inslag, är redan i dag relativt komplex. Det talar för att inte i onödan föreslå ytterligare bestämmelser om de som redan gäller ger ett tillfredsställande sekretesskydd. Det är vår uppfattning att så är fallet när det gäller såväl det allmännas intresse av att skydda den brottsbekämpande verksamheten som intresset av att skydda passagerares integritet och berörda företags kommersiella verksamhet.

Vad gäller integritetsintresset ser vi således inte tillräckliga skäl att, såsom gjorts beträffande vissa andra register, införa någon absolut sekretess för uppgifter i PNR-databasen. Absolut sekretess bör användas återhållsamt och när det verkligen finns ett oundgängligt behov av det. Det omvända skaderekvisitet i 35 kap. 1 § med presumption för sekretess ger enligt vår mening ett tillräckligt starkt skydd. Vi ser heller inte anledning att – på motsvarande sätt som gjorts i fråga om passagerarregistret – föreslå ett annat skaderekvisit för kommersiella intressen än vad som annars gäller inom den brottsbekämpande

verksamheten enligt 35 kap. 1 §. Sammanfattningsvis menar vi att det inte finns behov av ändrad sekretessreglering för att skydda PNR-uppgifter hos enheten för passagerarinformation eller annan PNR-information som enheten för passagerarinformation genererar i sitt arbete eller mottar från andra medlemsstater.

24.3.2 Skyddet för PNR-information hos behöriga myndigheter

Vår bedömning: PNR-information som enheten för passagerarinformation överför till verksamhet vid brottsbekämpande behöriga myndigheter – självmant efter sin förhandsbedömning eller på begäran från den behöriga myndigheten – omfattas av samma sekretess som gäller för andra uppgifter i den verksamhet vari PNR-informationen används. Detsamma gäller för sådan PNR-information som sänts från enheter i andra medlemsstater via enheten för passagerarinformation eller, i undantagsfall, direkt till myndigheten. Någon ny eller ändrad sekretessreglering behövs därför inte.

Brottsbekämpande myndigheter

Vi har ovan relativt ingående redogjort för de sekretessbestämmelser som i huvudsak gäller i aktuell verksamhet vid sådana brottsbekämpande myndigheter som utsetts eller kommer att utses till behöriga myndigheter. Dessa kommer att få PNR-information från enheten efter dennas eller någon annan medlemsstats förhandsbedömning, på egen begäran eller undantagsvis direkt från en enhet i annan medlemsstat. I samtliga fall sker detta därför att de ska använda PNR-informationen i sin verksamhet med att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Vi ser det som den enda rimliga ordningen att samma sekretessbestämmelser bör gälla för PNR-informationen som för andra uppgifter som myndigheterna har eller hämtar in och använder i denna verksamhet. Dessa sekretessbestämmelser ger ett tillfredsställande skydd. Det saknas därför anledning att föreslå någon ny eller ändrad reglering i sekretesslagstiftningen.

Försvarsmakten

Vad gäller Försvarsmakten såsom behörig myndighet är det i verksamhet inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (Must) som det kan bli aktuellt att motta och använda PNR-information för något av de syften som anges i den nya lagen. I den verksamheten finns t.ex. behov av uppgifter om in- och utresande individer för att följa upp sådan säkerhetshotande verksamhet som omfattas av lagens definition av terroristbrottslighet eller, i viss utsträckning, grov brottslighet.

Försvarsmaktens verksamhet inom Must omfattas inte direkt av sekretessregleringen enligt de ovan redovisade bestämmelserna i 18 kap. 1 och 2 §§ eller 35 kap. 1 § OSL. Däremot utgör PNR-informationen uppgifter som, enligt det tidigare sagda, hänför sig till sådan verksamhet hos enheten för passagerarinformation som avses i 18 kap. 1 och 2 §. Den sekretessregleringen kommer, som framgått ovan, att vara tillämplig även hos Försvarsmakten efter det att PNR-informationen mottagits från enheten.

Det är vidare vår uppfattning att även sekretessregleringen i 15 kap. 1 § (utrikessekretess) eller 2 § (försvarssekretess) OSL kan omfatta mottagen PNR-information i Musts verksamhet på samma sätt som dessa bestämmelser gäller i övrigt inom Musts verksamhet. Det har särskild betydelse för sådan PNR-information som Must i vissa undantagsfall kan begära direkt från en enhet i en annan medlemsstat. Båda dessa bestämmelser innehåller emellertid raka skaderekvisit med en presumtion för offentlighet. För sekretess enligt 15 kap. 1 § krävs att ett röjande kan antas störa Sveriges mellanfolkliga förbindelser eller på annat sätt skada landet, För sekretess enligt 15 kap. 2 § gäller att det ska kunna antas att ett röjande skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Beroende på sammanhanget eller uppgifternas karaktär är det alltså inte givet att PNR-information kan anses sekretessbelagd vid en prövning i det enskilda fallet gentemot dessa skaderekvisit.

För Musts verksamhet finns därutöver en särskild sekretessbestämmelse, 38 kap. 4 § OSL, till skydd för enskilds intresse. Enligt bestämmelsen gäller sekretess hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten i underrättelse- och säkerhetsverksamheten för uppgift om enskilds personliga eller eko-

nomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider skada eller men. Skaderekvisitet är, liksom enligt 35 kap. 1 § OSL, omvänt med en presumtion för sekretess. Den bestämmelsen kommer att även vara tillämplig på PNR-information som mottas för att användas i Musts verksamhet. Vidare gäller 21 kap. 5 § OSL om sekretess till skydd för utlännings säkerhet även hos Försvarmakten.

Mot bakgrund av ovanstående är det vår uppfattning att PNR-information som överförs till Försvarmakten såsom behörig myndighet enligt artikel 7 i direktivet kommer att åtnjuta ett tillfredsställande sekretesskydd hos Försvarmakten.

24.3.3 Behövs nya sekretessbrytande bestämmelser?

Vår bedömning: Det uppgiftsutlämnande av PNR-information som PNR-direktivet medför för enheten för passagerarinformation är förenligt med nuvarande sekretessreglering och sekretessbrytande undantag. Det behövs ingen särskild bestämmelse om sekretessgenombrott i offentlighets- och sekretesslagen eller i den nya lagen.

PNR-direktivet medför att enheten för passagerarinformation ska sända sekretessreglerad PNR-information vidare till behöriga myndigheter, till mottagare i andra medlemsstater och till Europol. Den nya lagen och den anslutande förordningen kommer att innehålla ett flertal bestämmelser om uppgiftsflödet ut från enheten till olika behöriga mottagare i Sverige eller övriga EU. Under vissa begränsade förutsättningar ska enheten vidare få överföra PNR-information till tredjeland.

Det är vår bedömning att skaderekvisiten i bestämmelserna om sekretess till skydd för den brottsbekämpande verksamheten normalt inte kommer att ”slå till” vid uppgiftsutbytet enligt PNR-direktivet och därmed kräva tillämpning av någon sekretessbrytande bestämmelse. Däremot är sekretessen i 35 kap. 1 § OSL till skydd för i första hand uppgifter om berörda passagerares personliga förhållanden sådan att tillämpning av sekretessbrytande bestämmelser krävs för att möjliggöra utbytet av PNR-information. Det ska observeras att det nedan sagda inte tar sikte på Polismyndigheten såsom behörig myn-

dighet, utan enbart på andra myndigheter. Enhetens uppgiftslämnande till Polismyndigheten såsom behörig myndighet enligt den nya lagen och vice versa är en intern överföring inom myndigheten som inte korsar någon sekretessgräns eller kräver stöd i sekretessbrytande bestämmelser, se avsnitt 10.4. Beträffande Säkerhetspolisen som mottagande behörig myndighet framgår vidare av 35 kap. 10 a § OSL att sekretessen enligt 35 kap. 1 § inte utgör något hinder för utlämnande, se ovan.

Vad beträffar andra behöriga myndigheter än Polismyndigheten är, som tidigare angetts, informationsförsörjning till verksamhet med att bekämpa terroristbrottslighet eller grov brottslighet en helt central uppgift för enheten. Vi bedömer därför att det finns ett tänkbart utrymme för att den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL om nödvändigt uppgiftslämnande kan tillämpas vid åtminstone utlämnande till behöriga myndigheter av träffar beträffande passagerare som enheten vid sina förhandsbedömningar finner behöver granskas närmare av mottagande behörig myndighet eller behörig mottagare i annan medlemsstat eller Europol. Även vidarebefordran till behöriga myndigheter av PNR-information som andra länders enheter ansett böra granskas vidare är en central uppgift för den svenska enheten liksom att besvara andra medlemsstaters framställningar med begäran om utfående av PNR-information. I och med att det på nuvarande stadium dock är något vanskligt att exakt se framför sig hur informationsutbytet kommer att gestalta sig och vilken prövning inför utlämnanden som enheten kommer att behöva göra i olika fall, förefaller det dock långt ifrån säkert att 10 kap. 2 § räcker till för allt det utlämnande till behöriga myndigheter som bör äga rum.

De bestämmelser vi föreslagit i avsnitt 15.2–15.4 innebär att enheten *ska* överföra PNR-information till behöriga mottagare, dvs. behöriga myndigheter, andra medlemsstaters enheter eller, undantagsvis, utsedda behöriga myndigheter i andra medlemsstater eller Europol. Förutsatt att enheten finner att villkoren enligt bestämmelserna är uppfyllda, har enheten således en skyldighet att överföra PNR-informationen som mottagaren behöver för sin verksamhet med att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Som vi ser det innebär detta att det visavi de svenska behöriga myndigheterna föreligger en sådan uppgiftsskyldighet som aktualiserar en tillämpning av 10 kap. 28 § OSL.

Den bryter sekretess oavsett vilken materiell sekretessbestämmelse som gäller för en uppgift i fråga. Det ska dock påpekas att det ytterst är enhetens sak – dvs. Polismyndighetens i strikt mening utifrån sekretesslagstiftningens systematik – att bedöma vilka uppgifter mottagaren behöver för den aktuella bekämpningen avseende terroristbrottslighet eller grov brottslighet som mottagna uppgifter är tänkta att användas för. Självfallet är det därför inte tillåtet för enheten att med åberopande av uppgiftsskyldighet och 10 kap. 28 § OSL lämna fler eller andra uppgifter som en mottagande myndighet inte alls verkar behöva. Att så inte får ske följer emellertid redan av andra bestämmelser i den föreslagna lagen.

Regleringen i den nya lagen om förutsättningarna för att lämna ut PNR-information till andra medlemsstater och Europol är detaljerade. Detsamma gäller bestämmelserna om utlämnande till tredjeland. Vi bedömer att det utlämnande som kommer i fråga till utländska myndigheter enligt den nya lagen sker i enlighet med sådana särskilda föreskrifter i lag eller förordning som avses i 8 kap. 3 § 1 OSL. Även beträffande behöriga mottagare i utlandet finns således förutsättningar att med stöd av offentlighets- och sekretesslagen sända över PNR-information som omfattas av sekretess enligt 35 kap. 1 § OSL eller någon annan materiell sekretessbestämmelse.

Det är alltså vår samlade bedömning att sekretess inte utgör hinder för det utbyte av information som kommer att vara en integrerad del av verksamheten vid enheten för passagerarinformation. Vi ser heller inte skäl för att tydliggöra detta genom någon upplysande bestämmelse i vare sig den nya lagen eller i offentlighets- och sekretesslagstiftningen. Den typen av tydliggörande kan nämligen leda till osäkerhet om vad som gäller på andra områden som saknar motsvarande upplysningsbestämmelser.

Vad särskilt gäller överföring till tredjeland kan avslutningsvis tilläggas att bestämmelserna i PNR-direktivet är formellt neutrala i den meningen att det principiellt sett inte påverkar tillämpningen av överföringsbestämmelserna om PNR-information, som enheten överför till tredjeland, omfattas av sekretess eller inte hos Polismyndigheten. Det är en annan sak att sekretess för överförda uppgifter kan påverka vilken skyddsnivå i mottagarlandet eller vilka skyddsåtgärder eller villkor om användningsbegränsning som krävs i den enskilda situationen.

25 PNR-direktivets betydelse för den nuvarande regleringen

25.1 Nuvarande reglering

Som framgått i avsnitt 5.2 finns det redan i dag bestämmelser som innebär att PNR-uppgifter kan användas i den brottsbekämpande verksamheten. Enligt dessa regelverk har Polismyndigheten, Säkerhetspolisen och Tullverket möjlighet att få ta del av bokningsuppgifter redan innan misstanke om ett visst konkret brott har uppstått. Bestämmelser härom finns i 25 och 26 §§ polislagen (1984:387), 4 kap. 6–8 §§ tullagen (2016:253) och i 15 och 16 §§ lagen (1996:701) om Tullverkets befogenhet vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränslagen). Regleringen är i huvudsak utformad på samma sätt i de olika lagarna. På begäran av någon av de angivna myndigheterna ska ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter som företaget har tillgång till. Transportföretaget har endast skyldighet att lämna de uppgifter om passagerare som avser namn, resrutt, bagage, medpassagerare samt sättet för betalning och bokning. Uppgifterna får bara begäras in om de kan antas ha betydelse för den brottsbekämpande verksamheten. I övrigt innehåller regleringen ingen begränsning i fråga om för vilken slags brottslighet uppgifterna får användas. Uppgifterna får lämnas på så sätt att de görs läsbara genom direktåtkomst. De aktuella myndigheterna får ta del av uppgifter genom direktåtkomst endast i den omfattning och under den tid som behövs för att kontrollera transporter. De får inte ändra eller på annat sätt bearbeta eller lagra uppgifter som hålls tillgängliga på detta sätt. Uppgifter om enskilda som lämnats på annat sätt än genom direktåtkomst ska omedelbart förstöras, om de visar sig sakna betydelse för utredning och lagföring av brott.

För Tullverkets del finns det kompletterande bestämmelser i 4 kap. 4–9 §§ tullförordningen (2016:287) och i 3–7 §§ förordningen (1996:702) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränsförordningen). Bl.a. anges att information om innehållet i inhämtade bokningsuppgifter får lämnas till andra tulltjänstemän, andra enheter inom Tullverket, Polismyndigheten och Kustbevakningen om uppgiften behövs i Tullverkets brottsbekämpande verksamhet för att klarlägga om brott eller brottslig verksamhet har förekommit, pågår eller planeras. Sådan information får också lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en konvention som Sverige har tillträtt eller en överenskommelse som Sverige har ingått.

Den kommande tullbrottsdatalagen, som ska träda i kraft den 1 juli 2017, innehåller bestämmelser om den vidare behandlingen av bokningsuppgifter vid Tullverket (se prop. 2016/17:91). Enligt 2 kap. 8 § TBL får personuppgifter som har lämnats till Tullverket från transportföretag enligt 4 kap. 6 § tullagen eller 15 § inregränslagen behandlas i den utsträckning det är tillåtet enligt de lagarna och enbart i den utsträckning det behövs för planering av kontrollverksamheten och urval av kontrollobjekt. Endast om det behövs i ett enskilt fall får sådana personuppgifter behandlas även för något av lagens primära ändamål och göras gemensamt tillgängliga. I 2 kap. 9 § TBL finns en bestämmelse som reglerar hur en sökning bland bokningsuppgifterna får gå till.

I detta avsnitt kommer vi att analysera hur bestämmelserna om transportföretags skyldighet att lämna uppgifter om transporter och om de berörda myndigheternas behandling av dessa uppgifter berörs av genomförandet av PNR-direktivet.

Utöver de ovan nämnda bestämmelserna regleras i 9 kap. 3 a–f §§ utlänningslagen (2005:716) skyldigheter för transportörer som luftvägen transporterar passagerare till Sverige att på begäran överföra API-uppgifter till Polismyndigheten. De överförda uppgifterna kan enligt 6 § lagen (2006:444) om passagerarregister på begäran lämnas ut från Polismyndigheten till Säkerhetspolisen och Tullverket för att underlätta verkställandet av personkontroller vid Sveriges gräns. De angivna bestämmelserna genomför API-direktivet i svensk rätt. Som framgått av vår analys och våra överväganden i avsnitt 14 innebär PNR-direktivets genomförande inte att genomförandet av API-direktivet i svensk rätt påverkas. PNR-direktivets förhållande till

API-direktivet och de bestämmelser som genomför det direktivet berörs därför inte närmare i detta avsnitt.

25.2 Våra överväganden och förslag

Vårt förslag: Det förs i polislagen, tullagen och inregränslagen i bestämmelser som innebär att transportföretags skyldigheter enligt de lagarna att överföra bokningsuppgifter till Polismyndigheten, Säkerhetspolisen och Tullverket inte ska gälla när lagen om flygpassageraruppgifter i brottsbekämpningen är tillämplig.

PNR-direktivet påverkar inte samtliga transportörer

PNR-direktivet innehåller endast bestämmelser om insamling och behandling av sådana PNR-uppgifter som lagras hos lufttrafikföretag. Direktivet innehåller således inga bestämmelser om insamling av PNR-uppgifter från transportörer som utför exempelvis buss-, färje-, eller tågtransporter. I skäl 33 anges att direktivet inte påverkar medlemsstaternas möjligheter att tillhandahålla system för insamling och behandling av PNR-uppgifter från andra transportföretag, under förutsättning att den nationella rätten är förenlig med unionsrätten. PNR-direktivet påverkar således inte insamling och behandling av PNR-uppgifter från andra transportörer än lufttrafikföretag. Våra författningsförslag innehåller inte heller bestämmelser som påverkar andra transportörsslag.

Författningsförslagen berör inte heller samtliga lufttrafikföretag. För att omfattas av överföringsskyldigheten enligt den föreslagna lagen fordras nämligen att lufttrafikföretagen i sin normala verksamhet samlar och hanterar PNR-uppgifter i någon form av reservationssystem med systematiserad behandling av standardiserade PNR-uppgifter. Som utgångspunkt utesluts från överföringsskyldighet härigenom flertalet mindre lufttrafikföretag som utför taxifygningar från mindre flygstationer.

För de transportörer som inte omfattas av våra författningsförslag bör bestämmelserna i polislagen, tullagen och inregränslagen om transportörers överföring av bokningsuppgifter gälla även efter det att PNR-direktivet är genomfört.

PNR-direktivet påverkar dagens insamling av bokningsuppgifter från lufttrafikföretag

När direktivet är genomfört i svensk rätt ska de lufttrafikföretag som omfattas av överföringsskyldigheten föra över PNR-uppgifter till enheten för passagerarinformation inför varje flygning till eller från Sverige. Listan över de PNR-uppgifter som ska överföras är lång och omfattar de uppgifter som transportörer i dag är skyldiga att lämna om sina passagerare enligt bestämmelserna i polislagen, tullagen och inregränslagen. De överförda PNR-uppgifterna får där- efter endast användas, lagras och utbytas enligt de bestämmelser som genomför direktivet. Av artikel 1.2 framgår att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Däremot får PNR-uppgifter som samlas in enligt direktivet användas av behöriga myndigheter om det i samband med en insats som baserats på PNR-uppgifter har kommit fram uppgifter om annan brottslighet. Vi har i avsnitt 16.2.3 föreslagit en bestämmelse som tillåter en behörig myndighet att i en sådan situation använda PNR-information för att förhindra, utreda eller lagföra brottet.

Som tidigare har angetts har PNR-direktivet dubbla syften. Ett av dessa är att skydda människor mot att deras personliga integritet kränks vid behandling av uppgifter om dem. Direktivet ska således sätta en rättslig ram till skydd av PNR-uppgifterna vid behöriga myndigheters behandling av dem (se skäl 5). Vid framtagandet av direktivet har en generell insamling och användning av PNR-uppgifter ansetts vara förenlig med enskildas rätt till privatliv och skyddet av personuppgifter endast om de bestämmelser till skydd för enskilda som anges i direktivet är uppfyllda. Kommissionen har uttalat starka reservationer mot nationella lösningar innebärande att PNR-uppgifter samlas in och behandlas utanför direktivets ramverk baserat på annan nationell reglering.¹ Vi delar den bedömningen.

Den reglering om inhämtande av bokningsuppgifter från transportföretag som gäller i dag uppfyller inte direktivets krav. För det fall det framöver skulle vara möjligt för de brottsbekämpande myndigheterna att, då uppgifterna överförs till enheten för passagerar-

¹ Com, Report of the fourth meeting on the implementation of the PNR Directive, 8 March 2017.

information, även hämta in dem direkt från lufttrafikföretagen, skulle PNR-uppgifterna inte behandlas i enlighet med direktivets bestämmelser. Ett av direktivets grundläggande syften skulle därmed falla och de bestämmelser som genomför direktivet skulle mista sin funktion.

En fortsatt möjlighet för de brottsbekämpande myndigheterna att, då uppgifterna samlas in av enheten för passagerarinformation, hämta in bokningsuppgifter direkt från lufttrafikföretag skulle alltså inte stå i överensstämmelse med PNR-direktivet. Det sagda gäller oavsett om det skulle ske för att bekämpa sådan brottslighet som avses i direktivet eller inte.

Med hänsyn härtill föreslår vi att det i bestämmelserna i polislagen, tullagen och inregränslagen om transportföretags skyldigheter att överföra bokningsuppgifter förs in ett tillägg som anger att dessa bestämmelser inte ska gälla när lagen om flygpassageraruppgifter i brottsbekämpningen är tillämplig. Sådana tillägg kan göras i ett nytt tredje stycke i 25 § polislagen och i 15 § inregränslagen samt i en ny paragraf, 4 kap. 6 a §, i tullagen.

Ytterligare författningsändringar bedöms inte nödvändiga

Som framgått i avsnitt 8.5 föreslår vi att det i de behöriga myndigheternas allmänna registerförfattningar förs in bestämmelser som anger att det i den av oss föreslagna lagen och i föreskrifter som meddelats med stöd av den lagen finns bestämmelser om personuppgiftsbehandling som ska tillämpas i stället för bestämmelserna i aktuell registerförfattning. För Tullverkets del har vi föreslagit en sådan bestämmelse genom ett tillägg i 2 kap. 8 § TBL. Genom att lägga bestämmelsen i anslutning till den lagens bestämmelser om behandling av bokningsuppgifter som hämtas in med stöd av tullagen eller inregränslagen tydliggörs att andra bestämmelser ska tillämpas för det fall det är fråga om bokningsuppgifter som överförs till Tullverket från enheten för passagerarinformation eller från en motsvarande enhet i en annan medlemsstat.

De bokningsuppgifter som Tullverket och övriga behöriga myndigheter kommer att få tillgång till via enheten för passagerarinformation kommer att bestå av PNR-information som enheten har bedömt vara intressant för vidare granskning hos den behöriga myn-

digheten. De bokningsuppgifter som har bedömts sakna intresse för den brottsbekämpande verksamheten har således redan sållats bort. Några ytterligare bestämmelser om behandling av mottagen PNR-information, motsvarande de som gäller för bokningsuppgifter enligt 2 kap. 8 och 9 §§ TBL om ändamåls- och sökbegränsningar, bedöms därför inte behöva föras in i tullbrottsdatalagen.

Den PNR-information som överförs från enheten för passagerarinformation kommer att kunna behandlas av Tullverket för de syften som anges i portalparagrafen i den nya lag som vi föreslår. Vidare kommer lagens bestämmelser om gallring och förbud mot behandling av PNR-uppgifter som utgör känsliga personuppgifter att gälla även för Tullverket. Mot den bakgrunden ser vi inga problem med att den mottagna PNR-informationen därutöver får behandlas enligt tullbrottsdatalagens allmänna bestämmelser i den mån dessa är förenliga med de skyldigheter som följer av den nya lagen med anslutande förordning.

Med hänsyn till den föreslagna bestämmelsen i tullbrottsdatalagen bedömer vi inte att det behövs föras in några förändringar i tullförordningen eller inregränsförordningen med anledning av genomförandet av PNR-direktivet.

26 Konsekvenser

26.1 Inledning

Förslaget till ny lag om flygpassageraruppgifter i brottsbekämpningen och den tillhörande förordningen syftar till att genomföra PNR-direktivet i svensk rätt och att uppfylla den överenskommelse som medlemsstaterna har ingått om att direktivet även ska tillämpas på flygningar inom EU. Målen för PNR-direktivet är bl.a. att trygga säkerheten, skydda personers liv och säkerhet och att inrätta en rättslig ram till skydd av PNR-uppgifter vid behöriga myndigheters behandling av dessa.¹ Bakgrunden till och en översikt av direktivet finns i kapitel 3.

Medlemsstaterna ska säkerställa att reglerna i direktivet genomförs i nationell rätt. Om så inte sker eller om de till följd av direktivet nödvändiga anpassningarna av gällande rätt inte görs, riskerar Sverige att kommissionen inleder ett förfarande om fördragsbrott. Att avstå från ett genomförande utgör alltså inte något alternativ. De förslag som lämnas i betänkandet är enligt vår mening nödvändiga för att genomföra direktivet och för att uppfylla den nämnda överenskommelsen.

PNR-direktivet ger en begränsad möjlighet till nationell särreglering. En sådan möjlighet finns främst vid valet av sanktionsformer. I denna fråga har vi valt att följa det motsvarande regelverk om sanktionsavgift som gäller i dag för lufttrafikföretag som underlåter att överföra API-uppgifter och det sanktionssystem som föreslås av Utredningen om 2016 års dataskyddsdirektiv.

En allmän utgångspunkt för utredningen har varit att tolka direktivets bestämmelser snävt och på det sätt som ger minst utrymme för intrång i den personliga integriteten. I den mån det har bedömts

¹ Se skäl 5 i PNR-direktivet.

finnas val- eller tolkningsmöjligheter har vi valt att i anslutning till lämnade förslag beskriva alternativa lösningar och motivera varför den valda lösningen har föreslagits. I detta kapitel ges en mer övergripande och sammanfattande beskrivning av de nya reglernas förväntade konsekvenser.

26.2 En effektiv användning av PNR-uppgifter i brottsbekämpningen

Vår bedömning: Förslagen förväntas få positiva konsekvenser för arbetet med att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrottslighet och grov brottslighet.

Förslagen innebär införandet av ett system för att samla in PNR-uppgifter och behandla dessa för vissa syften. PNR-uppgifterna kan användas av behöriga myndigheter för att göra en bedömning av passagerare redan innan de har anlänt till eller avrest från en medlemsstat. Syftet med en sådan användning är att övervaka eller gripa personer innan ett brott har begåtts. Uppgifterna kan även användas för att ingripa mot personer på grund av att ett brott har begåtts eller håller på att begås. PNR-uppgifterna kan således vara ett användbart verktyg för de behöriga myndigheterna i realtid. Uppgifterna kan även användas reaktivt efter det att ett brott har begåtts för att ta fram bevisning och, i förekommande fall, hitta medbrottslingar och nysta upp kriminella nätverk. I brottsutredningar kan äldre PNR-uppgifter användas exempelvis för att kartlägga var en misstänkt har befunnit sig vid vissa tidpunkter, vem personen har rest med och vem som har betalat för resan. PNR-uppgifterna kan även användas för att förbättra urvalet av de passagerare som kan komma att vara intressanta för vidare granskning.

För de behöriga myndigheter som i dag använder sig av PNR-uppgifter kommer PNR-systemet att innebära en mer effektiv användning av uppgifterna och att ett större antal passagerare kan kontrolleras. Även för sådana behöriga myndigheter som inte tidigare har använt sig av PNR-uppgifter kommer tillgången till PNR-information att medföra effektivitetsvinster.

Förslagen innebär också en stor möjlighet till utbyte av PNR-information mellan medlemsstaterna. Särskilt för Polismyndig-

heten har olika initiativ till utökat samarbete inom EU och med de andra nordiska länderna visat sig ha en positiv effekt. Det gäller exempelvis det utökade utbytet av DNA-uppgifter, fingeravtrycksuppgifter och kriminalregisterutdrag. Även ett utbyte av PNR-uppgifter mellan medlemsstaterna kommer, enligt vår bedömning, att leda till en effektivare brottsbekämpning.

Det nya systemets potential att tidigt hitta passagerare som kan misstänkas för inblandning i allvarlig brottslighet bör kunna medföra att fler sådana brott kan förhindras. T.ex. kan en analys av PNR-uppgifterna medföra att en misstänkt terrorist kan upptäckas och terroristbrottslighet därmed undvikas. Vidare kan en flygresa vara en förutsättning för genomförandet av ett brott eller i vart fall underlätta brottsligheten. En ökad risk för att kontrolleras av de behöriga myndigheterna i samband med en flygresa torde kunna ha en viss avskräckande effekt för en potentiell gärningsman och få denne att avstå från att t.ex. smugla narkotika. Förslagen får därför antas leda till en viss minskning av antalet begångna grova brott.

26.3 Konsekvenser för lufttrafikföretagen

Vår bedömning: Förslagen kommer att belasta lufttrafikföretagen arbets- och kostnadsmässigt.

Lufttrafikföretagens konkurrensförhållanden kommer inte att påverkas i någon större omfattning.

De enskilda aktörer som främst berörs av våra förslag är de lufttrafikföretag som åläggs att överföra PNR-uppgifter till enheten för passagerarinformation och att informera passagerarna om överföringen. Systemet med överföring av PNR-uppgifter kommer att beröra samtliga lufttrafikföretag som flyger till eller från någon av medlemsstaterna. Den av oss föreslagna regleringen kommer att omfatta såväl svenska flygbolag som flygbolag från andra länder inom och utom EU som flyger till eller från Sverige. År 2016 var det 240 flygbolag som utförde flygningar till eller från Sverige antingen i linjefart eller som charterflyg. Av dessa utförde 100 flygbolag fem

eller färre sådana resor.² Det finns inte några samlade uppgifter om storleken på de aktuella lufttrafikföretagen. Det kan dock sägas att storleken på företagen varierar stort. De minsta charterflygbolagen har endast ett fåtal anställda medan exempelvis konsortiet SAS har mer än 10 000 anställda. Det är främst större bolag som bedriver reguljär flygtrafik och som arbetar globalt.

PNR-direktivet har föregåtts av ett omfattande arbete på EU-nivå där berörda aktörer har haft möjlighet att yttra sig. Det har i utformningen av systemet tagits i beaktande att överföringsskyldigheten inte i onödan ska belasta lufttrafikföretagens arbets- eller kostnadsmissigt. Således ska lufttrafikföretagen endast överföra sådana PNR-uppgifter som de redan i dag samlar in av kommersiella och operativa skäl.

Lufttrafikföretagen har förklarat att det främst är formen för överföringarna som har betydelse för hur stora kostnader genomförandet av PNR-systemet kommer att ha för dem. Kommissionen har därför tagit fram en förteckning över gemensamma protokoll och understödda dataformat som ska användas vid överföringarna till de olika medlemsstaternas enheter för passagerarinformation. Lufttrafikföretagen får utifrån förteckningen själva välja vilka protokoll och format som de vill använda vid överföringarna. Genom att använda standardformat kan kostnaderna för lufttrafikföretagen hållas nere. I den mån överföringar kommer att ske från mindre lufttrafikföretag som inte flyger i linjetrafik och som inte har den nödvändiga tekniska infrastrukturen för att använda de gemensamma protokollen och understödda formaten, ska dessa, enligt kommissionens beslut, överföra sina uppgifter på något annat elektroniskt sätt som ska överenskommas med varje medlemsstat. Detta gäller så länge överföringarna sker på ett säkert sätt. Även kostnaderna för sådana mindre aktörer kommer därmed att kunna begränsas.

Enligt Polismyndighetens beräkningar är cirka 80 flygbolag av den storleken att de kommer att överföra PNR-uppgifter till den svenska enheten för passagerarinformation med hjälp av de gemensamma protokollen och standardformaten. De mindre bolagen som inte flyger i linjetrafik kan komma att få överföra sina uppgifter på annat sätt, t.ex. via en webbsida.

² Enligt Transportstyrelsens statistik.

Dock kommer självklart införandet av ett PNR-system att medföra omställningskostnader för lufttrafikföretagen. Bl.a. kommer det att krävas investeringar i och för löpande drift av nya och ändrade tekniska och administrativa system och rutiner. Därutöver uppstår kostnader till följd av administrativt och juridiskt merarbete, främst i samband med uppkopplingen mot enheten för passagerarinformation. Kommissionen har i sin konsekvensanalys angett att kostnaden för att införa en möjlighet att överföra PNR-uppgifter från lufttrafikföretag till enheterna för passagerarinformation kommer att uppgå till 100 000 euro per lufttrafikföretag. Den årliga kostnaden för överföringarna beräknades uppgå till 33 500 euro per lufttrafikföretag.³ Därtill kommer extra resurser att krävas för att administrera och underhålla överföringssystemen och för att vara tillgängliga för uppföljning. Det bör dock i sammanhanget påpekas att många lufttrafikföretag redan överför PNR-uppgifter till länder som kräver tillgång till sådana uppgifter. Det finns således redan internationellt standardiserad infrastruktur upparbetad kring dessa frågor.

Enligt lufttrafikföretagens uppskattningar kommer det att ta upp till sex månader att genomföra den första uppkopplingen från ett lufttrafikföretag till en enhet för passagerarinformation. Senare uppkopplingar kommer att ta avsevärt kortare tid. Själva överföringarna av PNR-uppgifterna kommer att ske per automatik och bedöms av utredningen inte medföra någon tidsåtgång.

Lufttrafikföretagen har redan i dag och kommer även enligt data-skyddsförordningen att ha en skyldighet att lämna viss information till sina passagerare. Enligt vår bedömning kan information om överföringsskyldigheten till enheten för passagerarinformation lämnas tillsammans med denna information, exempelvis på flygbiljetten och/eller via en hemsida. Informationsskyldigheten bör enligt vår bedömning endast i försumbar omfattning leda till ytterligare kostnader.

De kostnader som överföringsskyldigheten innebär bör lufttrafikföretagen huvudsakligen kunna överföra på sina kunder. Det är således sannolikt att kostnaderna kommer att läggas till biljettpriset. Enligt kommissionens beräkningar kan överföringsskyldigheten som mest innebära att biljettpriserna höjs med mindre än 0,10 euro per

³ Se SEC (2011) 133 final, s. 7 f.

biljett,⁴ vilket får anses vara en försumbar del av kostnaden för en flygbiljett.

Privatresenärer dominerar utrikesmarknaden. Denna marknad är mindre priskänslig än inrikesmarknaden, bland annat beroende på skillnader i tillgång till alternativa färdmedel.⁵ Det är således osannolikt att efterfrågan på utrikes flygresor kommer att påverkas av genomförandet av PNR-systemet.

Vårt förslag omfattar inte sådana mindre lufttrafikföretag som strukturmässigt saknar reservationssystem för behandling av PNR-uppgifter. Det innebär att s.k. taxiflyg som utgångspunkt inte kommer att omfattas av överföringsskyldigheten enligt lagen, se avsnitt 11.3. Någon möjlighet att därutöver, och utöver vad kommissionen gjort vid antagandet av de gemensamma protokollen och formaten, ta någon särskild hänsyn till mindre lufttrafikföretag föreligger inte.

En utgångspunkt i PNR-systemet är att lufttrafikföretagen behandlas lika och att som huvudregel alla flygningar till och från EU samt mellan medlemsstaterna omfattas. Det innebär att konkurrensen mellan flygbolagen inte kommer att påverkas. Dock undantas, som tidigare angetts, de allra minsta lufttrafikföretagen, från vårt förslag. De företagen kan sägas få vissa konkurrensfördelar. Dock är det vår bedömning att de flygbolagen inte trafikerar de större flyglinjerna och därmed inte konkurrerar på samma marknad som övriga lufttrafikföretag.

Med undantag av några enstaka linjer är konkurrensen från land- och sjötransporter obetydlig⁶ och bedöms inte påverkas av våra förslag.

Eftersom vi inte föreslår några skyldigheter för resebyråer och researrangörer kommer förslagen inte att leda till några särskilda konsekvenser för dem såvitt vi kan bedöma.

⁴ Se a.a. s. 8.

⁵ Se SOU 2016:83 s. 182 f.

⁶ Se t.ex. a.a. s. 69.

26.4 Konsekvenser för staten

Vår bedömning: Förslagen innebär kostnader för Polismyndigheten kopplade till inrättandet av en enhet för passagerarinformation och till drivandet av enheten. Kostnaderna får i nuläget antas kunna rymmas inom befintliga budgetramar.

Förslagen kan även innebära kostnader för behöriga myndigheter, tillsynsmyndigheten och förvaltningsdomstolarna. Även dessa kostnader bör rymmas inom befintliga anslagsramar.

Genomförandet av direktivet medför att en enhet för passagerarinformation ska byggas upp dit lufttrafikföretagen ska överföra sina PNR-uppgifter, där uppgifterna ska behandlas och från vilken vissa av uppgifterna ska föras vidare ut till behöriga myndigheter. Denna enhet ska enligt våra utredningsdirektiv finnas inom Polismyndigheten och kommer att vara en egen enhet inom denna myndighet. Vidare kräver ett genomförande av direktivet att investeringar sker på så sätt att PNR-systemet kan fungera fullt ut. Systemet kommer därmed även att ta driftskostnader i anspråk. Enligt uppgifter från Polismyndigheten kommer införandet av en enhet för passagerarinformation innebära kostnader främst i form av utarbetandet av ett nytt it-system som kan ta emot och hantera de stora mängder PNR-uppgifter som kommer att överföras från lufttrafikföretagen på det sätt som följer av direktivet. Även bemannandet av enheten kommer att driva stora kostnader.

Av direktivets skäl 14 framgår att medlemsstaterna ska betala kostnaderna för användning, lagring och utbyte av PNR-uppgifter. Enligt artikel 4.3 ska medlemsstaterna ge enheterna för passagerarinformation tillräckliga resurser för att de ska kunna utföra sina uppgifter. Vidare ska enligt artikel 5.2 medlemsstaterna förse det dataskyddsombud som ska finnas vid enheten med de resurser som behövs för att utföra sina uppgifter på ett effektivt och oberoende sätt.

Arbetet med att införa en enhet för passagerarinformation och genomföra direktivets tekniska delar pågår parallellt med vår utredning. Enligt uppgifter från Polismyndigheten har kostnaderna för projektet fram till och med mars 2017 uppgått till cirka 3 miljoner kronor. Under resterande delen av år 2017 beräknas kostnaderna uppgå till omkring 6 miljoner kronor. Från januari 2018 till och

med december 2020 beräknar projektledningen att kostnaderna kommer att uppgå till 130–140 miljoner kronor. I denna kostnadsberäkning ingår kostnader för att bygga ut enheten för passagerarinformation till att bli fullt ut fungerande i frågor gällande profilering, ärendehantering, kommunikation med övriga medlemsstaters motsvarande enheter m.m. I kostnaderna ingår också att driva det operativa arbetet vid enheten från våren 2018 och framåt. I dessa beräkningar anges att enheten för passagerarinformation, när den är fullt utbyggd, kommer att vara bemannad av cirka 40 personer. En viss del av kostnaderna kan täckas av fondmedel från EU. Enligt uppgift kan i bästa fall cirka 63 miljoner erhållas i fondmedel för perioden 2018–2020. Summan kan dock även bli långt mycket lägre. Besked i denna fråga kommer inte förrän i december 2017.

Mycket arbete återstår innan PNR-systemet är till fullo genomfört i Sverige. Trots de uppgifter vi har fått från Polismyndigheten är det alltjämt mycket som är oklart kring projektets genomförande och kostnader. Vidare är det i nuläget oklart vilka långsiktiga effektivitetsvinster som kan bli följden av införandet av systemet hos Polismyndigheten. På nuvarande stadium är det därför vår uppfattning att kostnaderna får rymmas inom befintliga budgetramar. Dock kan det komma att krävas vissa omprioriteringar. Vi vill därför understryka att det är av stor vikt att arbetet med att införa även direktivets tekniska delar är nödvändigt för att Sverige ska kunna bedömas ha genomfört PNR-direktivet.

De behöriga myndigheter som kommer att få del av PNR-uppgifter kan komma att få ökade kostnader i form av administration av mottagandet av informationen. Även de frågor som ska ställas till enheten, i vissa fall efter beslut av åklagare, för att få tillgång till PNR-uppgifter t.ex. i pågående förundersökningar kommer att medföra viss administration. De analyser som ska göras av de mottagna uppgifterna kan också medföra kostnader. Mot detta får ställas den effektivitetsvinst som troligen blir resultatet av mottagandet av sådan PNR-information som kan vara av intresse för vidare granskning i den brottsbekämpande verksamheten. Enligt vår bedömning kommer en eventuell kostnadsökning i dessa delar endast att bli marginell.

Förslagen innebär vidare att Tullverkets arbete med PNR-uppgifter kommer att förenklas eftersom myndigheten inte längre på egen hand behöver administrera insamlandet av PNR-uppgifter från sådana lufttrafikföretag som berörs av den nya lagen. Detta kan

komma att leda till minskade kostnader för den myndigheten i denna del. Som angetts ovan kommer dock sannolikt volymen av PNR-uppgifter som ska kontrolleras att öka på ett sådant sätt att det inte kommer att bli fråga om någon generell kostnadsminskning.

En ökad användning av PNR-uppgifter i brottsbekämpningen skulle kunna leda till att kostnaderna ökar inom vissa sektorer av rättsväsendet. Om t.ex. polisen blir effektivare kan det leda till en ökad arbetsbörda med krav på ökade resurser för åklagare och domstolar. Men totalt sett torde rättsväsendets olika insatser vid utredning och lagföring av allvarlig brottslighet effektiviseras.

Vi bedömer att våra förslag i sig inte kommer att medföra så många tillkommande ärenden årligen att det på grund av detta finns behov av några resursförstärkningar för rättsväsendet.

När ny lagstiftning införs krävs det normalt utbildningsinsatser. Det är inte unikt för de förslag som utredningen presenterar utan uppkommer regelmässigt i olika lagstiftningsärenden. Kostnaderna för utbildning bör rymmas inom befintliga ramar. Ny lagstiftning kräver normalt också nya interna föreskrifter och styrande dokument. Det får anses ingå i de normala uppgifterna för myndigheterna.

Den tillsynsmyndighet som ska utses enligt det nya dataskyddsdirektivet kommer att få ytterligare arbetsuppgifter och därmed ökade kostnader då den även ska övervaka behandlingen av PNR-uppgifter vid bl.a. enheten för passagerarinformation. Förslaget att sanktionsbeslut ska kunna överklagas till allmän förvaltningsdomstol kan också innebära en viss ökad belastning för domstolarna. Enligt vår bedömning kommer dock dessa fall att bli få. Tillsynsmyndighetens och domstolarnas kostnader får i nuläget antas kunna rymmas inom anslagsramarna.

26.5 Konsekvenser för enskilda

Vår bedömning: Förslagen innebär att fler PNR-uppgifter avseende enskilda flygresenärer samlas in i syfte att motverka terroristbrottslighet och grov brottslighet men säkerställer också skyddet för enskildas personliga integritet vid de behöriga myndigheternas behandling av uppgifterna.

För allmänheten innebär den föreslagna regleringen att PNR-uppgifter om oss alla, i egenskap av utrikesresenärer, kommer att överföras och behandlas vid enheten för passagerarinformation. PNR-uppgifter har även tidigare använts av brottsbekämpande myndigheter. Dock innebär förslagen att uppgifter om samtliga utrikesresenärer ska samlas in och behandlas. Den föreslagna regleringen kan därmed sägas påverka resenärernas integritet. Insamlingen och behandlingen av uppgifterna kommer dock inte att märkas i praktiken, om de inte föranleder ingripanden gällande misstanke om allvarlig brottslighet eller terroristbrottslighet.

Samtliga inskickade PNR-uppgifter kommer att genomgå en automatisk analys vid enheten för passagerarinformation där de kan jämföras mot relevanta register eller andra uppgiftssamlingar eller med på förhand fastställda kriterier. Fler s.k. träffar kommer troligen att uppkomma än vid en rent manuell behandling av PNR-uppgifter. Detta kan i förlängningen innebära att fler individer anses vara intressanta för vidare kontroller och att PNR-information om dem sänds vidare från enheten för passagerarinformation till behöriga myndigheter. Den PNR-information som sänds vidare kan avse såväl skyldiga som oskyldiga personer. Systemet kan därmed innebära att många träffar skickas över till behöriga myndigheter för vidare granskning för att sedan konstateras inte vara relevanta. Enligt vårt förslag ska dock sådana träffar genast raderas av de behöriga myndigheterna.

Ur dataskyddssynpunkt kan det nya systemet även ses som positivt, eftersom det enbart är PNR-uppgifterna för de personer där det vid en automatiserad analys blir en träff som kommer att läsas av de tjänstemän som därefter ska göra en bedömning av uppgifterna. Det innebär att PNR-uppgifter från det stora flertalet resenärer aldrig kommer att granskas av en fysisk person. Behandlingen kan även väntas innebära att ett färre antal oskyldiga personer väljs ut för fysisk kontroll på en flygplats.

Regleringen innehåller stränga krav på hur de överförda PNR-uppgifterna får behandlas hos enheten för passagerarinformation och hos de behöriga myndigheter som senare tar del av uppgifterna. PNR-uppgifterna får endast behandlas för att bekämpa terroristbrottslighet eller grov brottslighet. PNR-uppgifter som avslöjar känsliga personuppgifter får inte behandlas över huvud taget. Vidare får och ska PNR-informationen endast överföras till behöriga myn-

digheter, andra medlemsstater, Europol och tredjeländer när vissa förutsättningar är uppfyllda. Regleringen ställer också krav på att PNR-uppgifterna behandlas på ett säkert sätt och ger enskilda rätt till information om behandlingen, att kräva rättelse av felaktig behandling samt begära skadestånd och överklaga beslut vid felaktig behandling. Enskilda kommer också ha rätt att vända sig till ett dataskyddsombud vid enheten för passagerarinformation för att få råd och information om behandlingen av PNR-uppgifterna. Förslagen ger således ett tillfredsställande skydd för enskildas personliga integritet vid de behöriga myndigheternas behandling av deras PNR-uppgifter.

Våra förslag innebär vidare att enskilda kommer att beröras i den utsträckning flygbiljetter blir dyrare. Som vi angett ovan förväntas dock biljettpriserna öka endast i försumbar omfattning.

26.6 Konsekvenser i övrigt

<p>Utredningens bedömning: Förslagen förväntas inte få några andra konsekvenser.</p>

Förslagen får inte några konsekvenser för kommuner eller landsting generellt eller för den kommunala självstyrelsen. Förslagen bedöms inte heller innebära några konsekvenser för jämställdheten eller miljön. Enligt utredningens bedömning medför förslagen i betänkandet inte heller några andra konsekvenser av det slag som anges i 15 §§ kommittéförordningen (1998:1474) och som inte kommenteras på andra ställen i detta kapitel.

27 Ikraftträdande

Vårt förslag: Författningsförslagen ska träda i kraft den 25 maj 2018.

Medlemsstaterna ska enligt artikel 18 i direktivet sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet senast den 25 maj 2018. Vid samma tidpunkt kommer dataskyddsförordningen att börja tillämpas. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att brottsdatalagen ska börja gälla den 1 maj 2018.

Med hänsyn till att vår reglering har betydelse för aktörer både inom och utom det brottsbekämpande området bör vår reglering lämpligen träda i kraft tidigast när samtliga de nya dataskyddsbestämmelserna i såväl dataskyddsförordningen som i de författningar som genomför det nya dataskyddsdirektivet har börjat gälla. Våra författningsförslag bör därför träda i kraft den 25 maj 2018.

Något behov av ytterligare ikraftträdandebestämmelser eller övergångsbestämmelser har vi inte identifierat.

28 Författningskommentar

28.1 Förslaget till lag om flygpassageraruppgifter i brottsbekämpningen

1 kap. Allmänna bestämmelser

Lagens innehåll

1 §

I paragrafen anges lagens innehåll. Bestämmelsen behandlas i avsnitt 9.1.

Första stycket innehåller en sammanfattande beskrivning av lagens innehåll. Bestämmelsen genomför, tillsammans med 5 §, artikel 1 i PNR-direktivet. Definitioner av lufttrafikföretag, PNR-uppgifter, terroristbrottslighet och grov brottslighet finns i 3 §. Med ordet behandling avses detsamma som 1 kap. 6 § BDL¹. Där i inbegrips insamling, användning, lagring och medlemsstaternas inbördes utbyte av PNR-uppgifter enligt artikel 1 b i PNR-direktivet. PNR-uppgifterna får användas för att förebygga, förhindra, upptäcka eller utreda terroristbrottslighet eller grov brottslighet. Uppgifterna kan enligt lagen således behandlas både i underrättelseverksamhet och i förundersökning. Vidare kan uppgifterna behandlas av åklagare och i domstol vid en lagföring. Den behandlingen regleras dock inte av denna lag. Angående lagens förhållande till annan central dataskyddsreglering på området, se avsnitt 8.5.

I *andra stycket* anges att lagen genomför Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga,

¹ Se förslag till brottsdatalag i SOU 2017:29.

förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

Lagens syfte

2 §

Paragrafen anger lagens övergripande syfte. Bestämmelsen behandlas i avsnitt 9.1.

Lagens syfte är tudelat. Den syftar till att dels ge behöriga myndigheter tillgång till PNR-uppgifter för användning i viss brottsbekämpning, dels värna de registrerades integritet vid insamlingen och den vidare användningen samt utbytet av uppgifter om dem. Bestämmelsen har främst en informativ och pedagogisk betydelse då den klargör den övergripande målsättningen med regleringen.

Definitioner

3 §

I paragrafen, som bl.a. genomför artikel 3, definieras vissa uttryck som används i lagen.

Avmaskerade PNR-uppgifter

Avmaskerade PNR-uppgifter definieras inte i direktivet. Uttrycket behandlas i avsnitt 13.3.

Med avmaskerade PNR-uppgifter avses sådana uppgifter som tidigare har gjorts osynliga i PNR-databasen för användare utan särskild behörighet, eftersom de har förvarats där under längre tid än sex månader och som därefter har gjorts synliga på nytt.

Behörig mottagare

Behörig mottagare definieras inte i direktivet. Uttrycket behandlas i avsnitt 10.2.

Med behörig mottagare avses samtliga aktörer som är behöriga att motta PNR-information från enheten för passagerarinformation. Mottagare i tredjeland omfattas inte av definitionen.

Behörig myndighet

Definitionen, som genomför artikel 7.2, behandlas i avsnitt 15.2.1.

Bestämmelsen avgränsar vad för slags myndighet som i Sverige kan utses till en behörig sådan och hur myndigheten utses. Med att en myndighet är behörig avses att den är behörig att ta emot PNR-information från enheten för passagerarinformation, antingen efter enhetens förhandsbedömning eller efter särskild begäran enligt lagens bestämmelser. Även andra kan dock komma att ha rätt att använda PNR-informationen, t.ex. åklagare eller allmän domstol i samband med utredning eller lagföring av terroristbrottslighet eller grov brottslighet. Dessa är dock inte i lagens mening behöriga att få PNR-information direkt från enheten.

Flygpassageraruppgifter eller PNR-uppgifter

Definitionen motsvarar artikel 3.5 i direktivet och behandlas bl.a. i avsnitt 11.4.3.

PNR-uppgifter utgörs av sådana uppgifter om resenärer som lämnas i samband med bokning eller köp av flygresor eller vid incheckning och som samlas och hanteras av lufttrafikföretag för deras kommersiella och operativa syften. PNR är en i resebranschen vedertagen benämning som står för Passenger Name Record. Det spelar ingen roll om PNR-uppgifterna samlas i lufttrafikföretagens system för hantering av reservationer, i avgångskonstrollsysteem som används för att checka in passagerare på flygningar eller i likvärdiga system med motsvarande funktioner. Vilka PNR-uppgifter som ska behandlas enligt lagen framgår av bilagan till lagen. Det ska observeras att även s.k. API-uppgifter (Advance Passenger Information) kan ingå bland dessa PNR-uppgifter.

Grov brottslighet

Definitionen motsvarar artikel 3.9 i direktivet och behandlas i avsnitt 9.4.

Med grov brottslighet avses sådana brott enligt nationell rätt i Sverige eller andra medlemsstater som har sin motsvarighet i bilaga II till direktivet och för vilka det ingår tre års fängelse i straffskalan. För att ett brott ska ses som grovt i denna lags mening ska det således omfattas av den angivna bilagan och kunna leda till tre års fängelse eller mer. Inom det svenska tillämpningsområdet faller t.ex. människohandel, våldtäkt, rån, grov stöld, narkotikabrott, narkotikasmuggling och grovt vapenbrott.

Definitionen och bilaga II till direktivet har betydelse för att närmare avgränsa i vilka fall PNR-information ska överföras från enheten för passagerarinformation till behöriga myndigheter för användning i deras verksamhet med att förebygga, förhindra, upptäcka, utreda eller lagföra aktuell brottslighet. För det fall PNR-information ska överföras till en annan medlemsstat på begäran bör det vara tillräckligt att den medlemsstat som begär tillgång till uppgifterna anger att aktuell brottslighet omfattas av bilagan och kan leda till tre års fängelse enligt den medlemsstatens nationella rätt. I de fall enheten för passagerarinformation mottar PNR-information från en annan medlemsstat efter en förhandsbedömning av passagerare gjord i den medlemsstaten, får informationen endast sändas vidare till behöriga myndigheter här om aktuell brottslighet omfattas av aktuell bilaga och kan leda till tre års fängelse i Sverige.

Det ska observeras att den svenska översättningen av bestämmelsen har rättats i direktivet genom ett särskilt beslut. Definitionen i 3 § genomför den rättade versionen.

Luftrafikföretag

Definitionen behandlas i avsnitt 11.3 och motsvarar delvis definitionen i artikel 3.1.

Med luftrafikföretag i lagens mening avses sådana luftrafikföretag som har en giltig operativ licens utfärdad enligt bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av luftrafik i gemenskapen och som ger rätt att mot betalning

och/eller hyra utföra lufttransporter av passagerare. Även sådana lufttrafikföretag som har en motsvarande licens utfärdad i en stat utanför EU innefattas. För att omfattas av överföringsskyldigheten enligt lagen fordras därutöver att lufttrafikföretagen i sin normala verksamhet samlar och hanterar PNR-uppgifter i någon form av reservationssystem med systematiserad behandling av standardiserade PNR-uppgifter. Som utgångspunkt utesluts från överföringsskyldighet härigenom flertalet mindre lufttrafikföretag som utför taxiflygningar från mindre flygstationer utan system för avgångskontroller av passagerare.

Maskerade PNR-uppgifter

Maskerade PNR-uppgifter definieras inte i direktivet. Uttrycket behandlas i avsnitt 13.3.

Med maskerade PNR-uppgifter avses sådana uppgifter som har gjorts osynliga i PNR-databasen för den vanliga användaren av databasen eftersom de har förvarats där under längre tid än sex månader.

Maskering

Definitionen, som avses i artikel 3.10, behandlas i avsnitt 13.3.

Genom en maskering görs sådana PNR-uppgifter som direkt kan hänföras till en fysisk person osynliga, dvs. oåtkomliga, för den användare av PNR-databasen som saknar särskild behörighet för att få ta del av maskerade uppgifter. Maskering ska ske sex månader efter det att PNR-uppgifterna har kommit in från lufttrafikföretagen, se 3 kap. 11 § där det också anges vilka uppgifter som ska maskeras.

Medlemsstat

Definitionen har ingen motsvarighet i direktivet. Uttrycket behandlas i avsnitt 15.3.1.

Med medlemsstat avses sådana stater som är bundna av direktivet, vilket gäller samtliga EU:s medlemsstater förutom Danmark.

Passagerare

Definitionen motsvaras av artikel 3.4 i direktivet. Uttrycket behandlas i avsnitt 11.4.3.

Med passagerare avses alla personer, även de i transfer eller transit, som finns upptagna i passagerarförteckningen och därmed transporteras eller kommer att transporteras med ett flygplan med lufttrafikföretagets godkännande. Besättningsmedlemmar omfattas dock inte. Sådana operatörsanställda som reser med flygplanet utan att tjänstgöra ombord transporteras med lufttrafikföretagets godkännande och ska stå med i passagerarlistan. De omfattas därmed av direktivets definition av passagerare.

PNR-information

Definitionen har ingen motsvarighet i direktivet. Uttrycket behandlas i avsnitt 10.2.

Med PNR-information avses såväl PNR-uppgifter som det resultat som framkommer när PNR-uppgifter behandlas vid en enhet för passagerarinformation och jämförs med uppgifter i relevanta register eller andra uppgiftssamlingar eller med på förhand fastställda kriterier.

Reservationssystem

Definitionen motsvarar artikel 3.6 i direktivet och behandlas i avsnitt 11.3.

Med reservationssystem avses ett sådant elektroniskt system där lufttrafikföretag systematiskt samlar PNR-uppgifter och hanterar reservationer. Det har ingen betydelse om reservationssystemet tillhör lufttrafikföretaget eller om PNR-uppgifterna samlas och hanteras i ett system som tillhandahålls av en tredjepart.

Terroristbrottslighet

Definitionen motsvarar artikel 3.8 i direktivet. Den behandlas i avsnitt 9.3.

Med terroristbrottslighet avses i lagen samtliga brott som har införts i eller har ansetts svara mot befintlig nationell rätt i Sverige eller andra medlemsstater på grund av de aktuella bestämmelserna i rambeslutet och de ändringar som har genomförts i det beslutet.

Precis som definitionen av grov brottslighet har definitionen av terroristbrottslighet betydelse för att närmare avgränsa i vilka fall PNR-information får behandlas och t.ex. ska överföras från enheten för passagerarinformation till behöriga mottagare.

Tredjeland

Tredjeland är inte definierat i direktivet. Definitionen täcker alla stater som inte är medlemsstater i lagens mening och utgår alltså från hur en medlemsstat är definierad. Danmark är således i lagens mening ett tredjeland. Uttrycket behandlas i avsnitt 17.3.1.

Enhet för passagerarinformation

4 §

I paragrafen behandlas enheten för passagerarinformation. Bestämmelsen genomför artikel 4.1 och 4.2 i direktivet. Den behandlas i avsnitt 10.2.

I bestämmelsen slås fast att den nationella enheten för passagerarinformation ska vara en enhet inom Polismyndigheten. Den kommer där att ingå i den verksamhetsgren som ägnar sig åt att förebygga, förhindra, upptäcka, utreda eller syftar till att lagföra brottslig verksamhet. Vidare anges enhetens övergripande uppgifter, som är att samla in, lagra och behandla PNR-uppgifter och att överföra dem och annan PNR-information till behöriga myndigheter. Bland de grundläggande uppgifterna ingår också att utbyta PNR-information med andra medlemsstaters motsvarande enheter, med Europol och, i undantagsfall, med sådana myndigheter som har utsetts som behöriga i andra medlemsstater. I 6 kap. finns bestämmelser som anger

att PNR-information får överföras även till tredjeland om vissa förutsättningar är uppfyllda.

Otillåten behandling av PNR-information

5 §

Paragrafen genomför bl.a. artikel 1.2, 7.4 och 9.2–4 i direktivet. Den behandlas i avsnitt 9.5.

I paragrafen föreskrivs ett förbud mot behandling av PNR-information för andra syften än att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Paragrafen kan ses som en portalbestämmelse som talar om vilken behandling av PNR-uppgifter och resultatet av behandlingen av dessa uppgifter som över huvud taget är tillåten enligt lagen. Det har ingen betydelse om PNR-uppgifterna har överförts till enheten för passagerarinformation från ett lufttrafikföretag eller från en annan medlemsstats motsvarande enhet. Det har inte heller någon betydelse om uppgifterna behandlas vid enheten för passagerarinformation eller vid en behörig myndighet. PNR-uppgifter som har samlats in i enlighet med PNR-direktivet får inte behandlas för andra syften än de som anges i bestämmelsen. Det finns dock ett undantag för behandling av uppgifter hos behöriga myndigheter i ett visst fall, se vidare i 5 kap. 3 §.

Förbud mot behandling av känsliga personuppgifter

6 §

Paragrafen genomför artikel 13.4 i direktivet. Den behandlas i avsnitt 18.5.

Genom bestämmelsen förbjuds behandling av PNR-uppgifter som utgör känsliga personuppgifter. Vilka personuppgifter som avses framgår av en motsvarande bestämmelse i 2 kap. 11 § BDL. Som känsliga personuppgifter avses sådana uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör, hälsa, sexualliv eller sexuell läggning. För det fall enheten för passagerarinformation mottar sådana uppgifter ska dessa omedelbart raderas, se vidare i 3 kap. 10 §.

Inte heller en behörig myndighet får behandla PNR-uppgifter som utgör känsliga personuppgifter. Även för det fall en sådan myndighet av misstag skulle motta sådana uppgifter ska de omedelbart raderas, se vidare i 5 kap. 2 §.

Förbudet mot behandling av PNR-uppgifter som utgör känsliga personuppgifter tar sikte på sådana personuppgifter där det direkt framgår – av uppgiften i sig själv – att det är fråga om en känslig personuppgift. Det krävs alltså inte att en mottagare av uppgifterna gör några närmare analyser och bedömningar av uppgifterna med jämförelser med övriga tillgängliga uppgifter osv, för att bedöma huruvida en PNR-uppgift indirekt utgör en känslig personuppgift.

2 kap. Lufttrafikföretagens skyldigheter

Överföring av PNR-uppgifter till enheten för passagerarinformation

1 §

I bestämmelsen behandlas skyldigheten för lufttrafikföretag att överföra PNR-uppgifter till den svenska enheten för passagerarinformation. Paragrafen genomför artikel 8.1 i direktivet samt medlemsstaternas överenskommelse om att tillämpa direktivet även på flygningar inom EU. Den behandlas i avsnitt 11.4.

Första stycket innebär att lufttrafikföretagen ska överföra PNR-uppgifter inför varje flygning ankommande till eller avgående från Sverige. Härmed omfattas alla flygningar mellan Sverige och ett annat land, oavsett om det är fråga om ett annat EU-land eller ett land utanför EU, och även för det fall det endast är fråga om en mellanlandning på svensk mark. Inrikesflygningar omfattas däremot inte. Av bestämmelsen framgår också den för direktivet gällande grundsatsen, nämligen att lufttrafikföretagen inte ska överföra fler uppgifter än de som de redan samlar in i sin normala verksamhet. Lagen ålägger alltså inte lufttrafikföretagen att hämta in ytterligare PNR-uppgifter om sina passagerare (från passagerarna själva, charterbolagen eller resebyråer m.fl.) utan endast att överföra sådana uppgifter som de redan har tillgång till. Vilka uppgifter som kan vara aktuella för en sådan överföring framgår av bilagan till lagen. Även API-uppgifter ingår bland de uppräknade uppgifterna i bilagan. I den anslutande

förordningen regleras att eventuella API-uppgifter ska överföras även om de inte lagras eller annars behandlas med hjälp av samma tekniska metoder som andra PNR-uppgifter.

I *andra stycket* anges att för det fall flera lufttrafikföretag samarbetar och har en gemensam linjebeteckning, s.k. code sharing, ska PNR-uppgifterna överföras av det lufttrafikföretag som utför själva flygningen.

2 §

Paragrafen genomför delar av artikel 8.3 samt artikel 8.4 i direktivet. Den behandlas i avsnitt 11.4.5.

Av bestämmelsen framgår att PNR-uppgifterna ska överföras vid två tillfällen, det första ett till två dygn före flygningens avgång och det andra omedelbart efter det att gatens dörrar har stängts, dvs. när passagerarna har stigit ombord på planet inför avgång och passagerare inte längre tillåts stiga ombord eller stiga av. Det är möjligt för ett lufttrafikföretag och enheten för passagerarinformation att komma överens om vid vilken närmare tidpunkt den första överföringen ska ske. Har lufttrafikföretaget överfört PNR-uppgifterna inom den i lagen angivna tidsramen har företaget dock uppfyllt sin överföringskyldighet enligt den första punkten.

I *andra stycket* framgår att den senare överföringen får begränsas till uppdateringar och kompletteringar av den information som överfördes vid det första tillfället. En sådan uppdatering kan avse såväl ändringar i tidigare lämnade PNR-uppgifter som helt nytillkomna PNR-uppgifter, t.ex. avseende passagerare inbokade samma dag som flygets avgång.

3 §

Bestämmelsen, som genomför artikel 8.5 i direktivet, behandlas i avsnitt 11.4.6.

Av bestämmelsen framgår att lufttrafikföretag, utöver vad som anges i 2 §, är skyldiga att överföra PNR-uppgifter även vid andra tidpunkter om det i ett enskilt fall bedöms nödvändigt för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet. Det är enheten för passagerarinforma-

tion som, i praktiken normalt efter framställan från en behörig myndighet, ska bedöma huruvida det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter vid andra tidpunkter än de som anges i 2 §. En sådan begäran kan bli aktuell då omständigheterna medför att tillgång till PNR-uppgifter avseende en viss person eller en viss flygresor är nödvändig för att reagera på en särskild risk för sådan brottslighet som direktivet avser.

4 §

Bestämmelsen genomför delar av artiklarna 8.1 och 8.3 i direktivet. Den behandlas i avsnitt 11.4.7.

Första meningen i bestämmelsen anger att PNR-uppgifterna ska överföras från lufttrafikföretagen till databasen vid enheten för passagerarinformation på elektronisk väg. Av andra meningen framgår att överföringen ska ske via den s.k. sändmetoden. Det är således inte tillåtet för enheten att via direktåtkomst ta del av PNR-uppgifter i lufttrafikföretagens reservationssystem eller liknande datoriserade bokningssystem. Närmare bestämmelser om formen för överföringarna finns i den anslutande förordningen.

5 §

Bestämmelsen motsvaras inte av någon bestämmelse i direktivet. Den behandlas i avsnitt 11.4.8.

Paragrafen erinrar om att ett lufttrafikföretag har möjlighet att låta t.ex. en systemleverantör av ett datoriserat bokningssystem överföra PNR-uppgifterna till enheten för passagerarinformation. Det är dock lufttrafikföretaget som har personuppgiftsansvaret för överföringen av uppgifterna, bl.a. att den kringgärdas av tillräckliga säkerhetsåtgärder. Det är även lufttrafikföretaget som riskerar sanktionsavgift om uppgiftsskyldigheten inte fullgörs enligt denna lag.

Information till passagerare

6 §

Bestämmelsen genomför direktivets skäl 29 och 37. Den behandlas i avsnitt 20.2.4.

Paragrafen innebär att lufttrafikföretag vars passagerare berörs av överföringen av PNR-uppgifter enligt lagen ska informera passagerarna om att uppgifterna överförs till enheten för passagerarinformation och om att detta sker till följd av ett författningsreglerat åläggande som genomför PNR-direktivet. Informationen kan lämpligen lämnas tillsammans med den övriga information som lufttrafikföretagen ska tillhandahålla enligt dataskyddsförordningen. Informationsskyldigheten fullgörs lämpligen både med en mer allmänt riktad metod, t.ex. en webbplats, och genom information till passageraren i fråga, t.ex. på biljett eller bokningsbekräftelse. Vid samarbete mellan lufttrafikföretag, s.k. code sharing, ansvarar respektive lufttrafikföretag för att informera sina passagerare.

Sanktionsavgift för lufttrafikföretag

7 §

Paragrafen reglerar för vilka överträdelser administrativ sanktionsavgift ska tas ut av ett lufttrafikföretag. Den genomför artikel 14 i direktivet. Paragrafen behandlas i avsnitt 22.3.5.

I paragrafen anges uttömmande vilka överträdelser som kan föranleda sanktionsavgift. Både överträdelser av bestämmelser i lagen och bestämmelser som har utfärdats i anslutning till lagen kan leda till sanktionsavgift. Sanktionsavgift kan t.ex. utgå om överföringar inte sker vid de tidpunkter som anges i lagen eller om de görs i ett annat format än de som godkänts av kommissionen. Polismyndigheten avgör dock i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, se 8 § andra stycket.

PNR-uppgifterna ska överföras av det lufttrafikföretag som utför själva flygningen. Sanktioner kommer således inte att drabba de lufttrafikföretag som endast delar linjebeteckning med det företag som utför flygningen. Det följer inte heller någon sanktionsavgift enligt lagen vid utebliven information till passagerarna om överföringen.

Ansvar för överträdelser är strikt. Det krävs alltså varken uppsåt eller oaktsamhet för att en sanktionsavgift ska kunna tas ut. Det är tillräckligt att en överträdelse har ägt rum.

8 §

Paragrafen behandlar sanktionsavgiftens storlek. Övervägandena finns i avsnitt 22.3.6.

I *första stycket* fastställs minimi- och maximibelopp för sanktionsavgift. Avgifter som motsvarar eller ligger i närheten av maximibeloppet är avsedda för de allvarligare fallen. Det kan röra sig om upprepade överträdelser eller fall som rör ett stort antal passagerare och där ingen rimlig förklaring finns till att de aktuella uppgifterna inte har lämnats. I andra fall bör en lägre avgift kunna fastställas. Direktivets föreskrift om att sanktionerna ska vara effektiva, proportionella och avskräckande ska dock alltid beaktas.

I *andra stycket* föreskrivs att sanktionsavgiften kan sättas ned helt eller delvis. Lufttrafikföretagen kommer normalt sett ha möjlighet att lämna uppgifter i enlighet med direktivets bestämmelser. Det kan emellertid finnas olika orsaker till att ett lufttrafikföretag inte har fullgjort sin överföringsskyldighet. Det kan t.ex. vara så att det har skett ett tekniskt fel vid överföringen av uppgifterna. Vidare kan ett flyg som inte var tänkt att anlända till Sverige oväntat ha om-dirigerats hit. Paragrafen ger möjlighet att sätta ned sanktionsavgiften, helt eller delvis, om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

9 §

Paragrafen behandlas i avsnitt 22.3.7. I *första stycket* föreskrivs att Polismyndigheten beslutar om sanktionsavgift. Av *andra stycket* framgår att sanktionsavgiften tillfaller staten.

10 §

Av paragrafen följer att den som avgiften ska tas ut av ska ges tillfälle att yttra sig innan Polismyndigheten beslutar om sanktionsavgift. Paragrafen behandlas i avsnitt 22.3.7. Möjligheten att besluta om sanktionsavgift bortfaller om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom två år efter överträdelsen.

11 §

Av bestämmelsen, som behandlas i avsnitt 22.3.7, framgår att Polismyndighetens beslut om sanktionsavgift får överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

Föreskrifter

12 §

I bestämmelsen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om lufttrafikföretagens överföring av PNR-uppgifter till enheten för passagerarinformation samt om handläggningen av beslut om och verkställighet av sanktionsavgifter.

3 kap. Behandling av PNR-information vid enheten för passagerarinformation

PNR-databas

1 §

Paragrafen behandlas i avsnitt 13.1. Den genomför bl.a. artikel 12.1 i direktivet.

Genom bestämmelsen föreskrivs att det ska finnas en databas för PNR-uppgifter vid enheten för passagerarinformation där de PNR-uppgifter som överförs från lufttrafikföretagen ska lagras. Begreppet databas används i lagen i en rättslig mening för att beteckna en

avgränsad uppgiftssamling med PNR-uppgifter. Någon särskild teknisk lösning för denna avgränsning föreskrivs inte.

Personuppgiftsansvar m.m.

2 §

Bestämmelsen, som inte motsvaras av någon artikel i direktivet, behandlas i avsnitt 19.1.3.

Bestämmelsen är av upplysande karaktär och anger att det är Polismyndigheten som är personuppgiftsansvarig för den behandling av personuppgifter som utförs vid enheten för passagerarinformation. Det är således Polismyndigheten som ska ansvara för att sådana skyldigheter som följer av bl.a. denna lag följs i den verksamhet som sker vid enheten för passagerarinformation.

3 §

Paragrafen genomför artikel 6.8 i direktivet. Den behandlas i avsnitt 19.2.4.

Bestämmelsen innebär ett förbud mot att enhetens lagring och annan behandling av PNR-uppgifter sker på ett territorium utanför en medlemsstat enligt direktivet. Den innebär inte nödvändigtvis ett krav på att enhetens behandling av PNR-uppgifter ska ske i Sverige. Huvudsaken är att uppgifterna garanteras den säkerhetsnivå och övrigt dataskydd som gäller i medlemsstaterna.

Tillåtna ändamål

4 §

Paragrafen innehåller de grundläggande ändamålen för vilka de PNR-uppgifter som har överförts från lufttrafikföretag får behandlas vid enheten för passagerarinformation. Bestämmelsen genomför artikel 6.2. Den behandlas i avsnitt 13.2.

Bestämmelsen ersätter de ändamålsbestämmelser som anges i 2 kap. 7 och 8 §§ PDL. Den exkluderar även en tillämpning av bestämmelsen om behandling av personuppgifter för nya ändamål i

2 kap. 4 § BDL. Uppräkningen i bestämmelsen är alltså uttömmande och innebär att endast sådan personuppgiftsbehandling som inryms i något av de i paragrafen angivna ändamålen får äga rum. Dock är behandling alltid tillåten för att uppfylla de syften som anges i 2 kap. TF. Vidare får PNR-uppgifterna alltid behandlas för att besvara en förfrågan från en enskild om huruvida dennes personuppgifter behandlas vid enheten eller för att ge tillsynsmyndigheten tillgång till behandlade uppgifter.

Enligt *första stycket punkten 1* får PNR-uppgifterna behandlas för att göra en förhandsbedömning av passagerare innan de har anlant till eller avrest från Sverige. En sådan realtidsbedömning har till syfte att identifiera personer som behöver utredas ytterligare av behöriga myndigheter eller Europol. En bedömning av PNR-uppgifterna innebär en möjlighet att välja ut personer som inte tidigare varit misstänkta för inblandning i grov brottslighet eller terrorism, men som enligt en analys av uppgifterna kan vara inblandade i sådan brottslighet och därför bör bli föremål för ytterligare utredning av de behöriga myndigheterna. Syftet med behandlingen enligt denna punkt är att PNR-informationen ska analyseras vidare av nationella behöriga myndigheter eller av Europol, för ställningstagande där till om den ger anledning till vidare insatser, t.ex. att en eller flera passagerare kontrolleras. Behandlingen ska således inte ske för att finna personer som bör behandlas vidare vid andra medlemsstaters enheter för passagerarinformation. För det fall enheten skulle finna att den framtagna informationen kan vara av intresse även för en annan medlemstat ska dock informationen sändas även till den medlemsstatens enhet för passagerarinformation enligt 4 kap. 2 §. Behandling av PNR-information för ett sådant ändamål behandlas i punkten 2.

Av *andra punkten* följer att enheten för passagerarinformation får behandla PNR-uppgifter för att fullgöra sina uppgifter enligt 4 kap. att besvara en begäran från en behörig mottagare om att få tillgång till äldre PNR-uppgifter och att överföra dem till den efterfrågande mottagaren. I brottsutredningar kan äldre PNR-uppgifter vara användbara för att exempelvis kartlägga var en misstänkt har befunnit sig vid vissa tidpunkter, vem personen har rest med och vem som har betalat för resan. PNR-uppgifter kan således även användas reaktivt efter det att ett brott har begåtts för att t.ex. ta fram bevisning eller, i förekommande fall, hitta medbrottslingar och nysta upp kriminella

nätverk. Behöriga mottagare kan därför ha ett intresse av att få del av sådana äldre PNR-uppgifter som bevaras vid enheten för passagerarinformation.

Enligt *tredje punkten* får PNR-uppgifterna behandlas för att skapa nya eller uppdatera gamla kriterier som ska användas vid förhandsbedömningarna enligt första punkten. Det är därmed möjligt för personalen inom enheten för passagerarinformation att gå igenom de PNR-uppgifter som finns samlade i databasen för att t.ex. leta efter mönster som kan indikera att personer kan vara av intresse för vidare kontroller.

I *andra stycket* upplyses om att det i 6 kap. finns bestämmelser som anger att PNR-uppgifter under vissa förutsättningar får överföras till ett tredjeland. PNR-uppgifterna får behandlas även för detta ändamål.

5 §

Paragrafen anger hur en förhandsbedömning av PNR-uppgifter får gå till. Bestämmelsen genomför artikel 6.3 och behandlas i avsnitt 13.2.2.

PNR-uppgifterna får enligt *första punkten* jämföras med sådana register eller andra uppgiftssamlingar som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Vilka register eller uppgiftssamlingar som ska användas är upp till varje medlemsstat. Dessa måste dock vara relevanta för direktivets syften, dvs. att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Enligt direktivet kan detta omfatta register över personer eller föremål som är eftersökta eller finns uppförda på en spärrlista.

Enligt *andra punkten* får PNR-uppgifterna behandlas i enlighet med på förhand utformade och fastställda kriterier. Uppgifterna får således jämföras med sådana i förväg bestämda profiler som kan ge anledning att kontrollera en viss person. En profil avser en icke personanknuten företeelse och kan omfatta uppgifter om exempelvis avreseort, resrutt, betalningsätt, bokningsrutin, bagage m.m. Profiler kan användas för att leta efter mönster som kan indikera att en person är av intresse för vidare kontroller. Enligt bestämmelsen ska sådana kriterier, eller profiler, vara riktade, proportionella och avgränsade och får inte grundas på känsliga personuppgifter. Det framgår

av förordningen att kriterierna ska fastställas och fortlöpande ses över av enheten för passagerarinformation i samarbete med behöriga myndigheter. Härigenom kan kriterierna kontinuerligt förbättras och träffsäkerheten öka.

6 §

Paragrafen reglerar enheten för passagerarinformations behandling av PNR-information som den mottagit från motsvarande enheter i andra medlemsstater. Den har ingen motsvarighet i direktivet. Bestämmelsen behandlas i avsnitt 13.2.5.

Enheten för passagerarinformation kommer inte bara att behandla PNR-uppgifter som har kommit in till enheten från lufttrafikföretag, utan kommer också att motta och behandla PNR-information som överförs från andra medlemsstaters motsvarande enheter. Av bestämmelsen framgår att enheten endast får behandla denna PNR-information i syfte att vidarebefordra den till en eller flera behöriga myndigheter för fortsatt användning enligt de syften som anges i 1 kap. 5 §. Den PNR-information som enheten för passagerarinformation mottagit från motsvarande enheter i andra medlemsstater kan således inte användas t.ex. för att enheten ska kunna verifiera sin egen databas eller finslipa sina kriterier etc. För det fall det kan konstateras att den mottagna informationen inte avser terroristbrottslighet och inte heller avser sådan brottslighet som definieras som grov brottslighet i Sverige, följer av 1 kap. 5 § att informationen inte får sändas vidare till behöriga myndigheter.

Tillgång till PNR-information

7 §

Paragrafen behandlas i avsnitt 10.4.3. Den begränsar antalet personer vid Polismyndigheten som är behöriga att ta del av uppgifterna i PNR-databasen och den övriga PNR-information som behandlas vid enheten för passagerarinformation. Endast de som arbetar vid enheten får ha tillgång till dessa uppgifter. Dessutom ska tillgången begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter vid enheten.

Vissa tjänstemän kan ha sin grundanställning på en annan behörig myndighet än Polismyndigheten men ha avdelats för att arbeta vid enheten för passagerarinformation. När de gör det anses de delta i Polismyndighetens verksamhet i den mening som avses i bl.a. 2 kap. 1 § OSL.

Förbud mot direktåtkomst

8 §

Paragrafen behandlas i avsnitt 10.4.1. Den innebär att andra myndigheter än Polismyndigheten inte får tillåtas ha direkt tillgång till uppgifterna i PNR-databasen vid enheten för passagerarinformation eller i övrigt till den PNR-information som behandlas vid enheten. Behöriga myndigheter får således endast tillgång till dessa uppgifter sedan de har överförts till dem från enheten för passagerarinformation. Tillgången inom Polismyndigheten regleras i 7 §.

Bevarande och gallring av PNR-uppgifter

9 §

Paragrafen behandlas i avsnitt 18.4. Den genomför delvis artikel 12.1 och 12.4 i direktivet.

I bestämmelsen föreskrivs att PNR-uppgifter som mottagits från lufttrafikföretagen ska lagras i databasen för PNR-uppgifter vid enheten för passagerarinformation i fem år. Det har ingen betydelse om PNR-uppgifterna levereras till enheten direkt från ett lufttrafikföretag eller från ett personuppgiftsbiträde, exempelvis en systemleverantör. Efter fem år ska PNR-uppgifterna gallras genom att raderas. Härmed avses i praktiken att uppgifterna utplånas.

För det fall PNR-uppgifter har överförts till behöriga myndigheter gäller samma gallringsregler för de uppgifterna som i övrigt är tillämpliga vid den myndigheten. Dock ska sådana PNR-uppgifter som har överförts från enheten för passagerarinformation efter enhetens förhandsbedömning och som inte är av intresse för vidare kontroller raderas genast, se 5 kap. 1 §.

10 §

Bestämmelsen behandlar radering av PNR-uppgifter som utgör känsliga personuppgifter. Den genomför artikel 13.4 i direktivet och behandlas i avsnitt 18.5.

Lufttrafikföretagen bör inte skicka in andra uppgifter än de som omfattas av deras uppgiftsskyldighet, därmed inte heller känsliga personuppgifter. Dock kan detta komma att ske av misstag, t.ex. därför att uppgiven kontaktadress röjer en svensk partitillhörighet som är obekant för det asiatiska lufttrafikföretaget i fråga. Enligt bestämmelsen ska enheten för passagerarinformation omedelbart gallra PNR-uppgifter som utgör känsliga personuppgifter genom att radera dem om enheten mottar sådana uppgifter från lufttrafikföretag eller från en enhet för passagerarinformation i en annan medlemsstat. Bestämmelsen kräver inte manuell genomgång av varje inkommen uppgift. Däremot krävs att det används tillgänglig informationsteknik för att genom automatiserade processer söka efter och radera känsliga personuppgifter när enhetens tekniska lösningar utformas och uppdateras.

En motsvarande bestämmelse för behöriga myndigheter finns i 5 kap. 2.§.

Maskering av PNR-uppgifter

11 §

Av bestämmelsen framgår vilka PNR-uppgifter som ska maskeras sex månader efter att de överförts från lufttrafikföretag och förts in i databasen för PNR-uppgifter vid enheten för passagerarinformation. Paragrafen genomför artikel 12.2 i direktivet och behandlas i avsnitt 13.3.

De PNR-uppgifter som ska maskeras avser sådana uppgifter som kan användas för att omedelbart identifiera passagerare. Uppräkningen motsvarar densamma i direktivet, dock med några språkliga justeringar. Med alla former av betalningsinformation enligt punkten 4 avses all sådan information som kan användas för att omedelbart identifiera en person, oavsett om denne är en passagerare eller inte.

Dataskyddsbud

12 §

Paragrafen genomför artikel 5.1 första ledet och artikel 6.7 första meningen i direktivet. Den behandlas i avsnitt 19.5.4.

Av *första stycket* följer att Polismyndigheten ska utse ett eget dataskyddsbud för enheten för passagerarinformation. Av *andra stycket* följer att detta ombud för sitt arbete ska ha tillgång till samtliga uppgifter som behandlas vid enheten för passagerarinformation. Genom en sådan tillgång kan lagligheten i behandlingen fortlöpande kontrolleras.

13 §

Paragrafen reglerar dataskyddsbudets uppgifter. Bestämmelsen genomför andra ledet av artikel 5.1 i direktivet. Den behandlas i avsnitt 19.5.4.

Dataskyddsbudets generella uppgifter regleras i brottsdatalagen. Av *första stycket* framgår att dataskyddsbudet, utöver vad som anges i 3 kap. 14 § BDL, även ska ansvara för genomförandet av relevanta skyddsåtgärder. Detta innebär att det ankommer på ombudet, vid sidan av Polismyndigheten, att ta initiativ till och lämna riktlinjer och förslag på lämpliga skyddsåtgärder samt att också se till att dessa genomförs i praktiken vid enheten för passagerarinformation.

Av *andra stycket* följer att enskilda ska ha rätt att vända sig till dataskyddsbudet i egenskap av enda kontaktpunkt i alla frågor som gäller behandlingen enligt lagen av PNR-uppgifter om denne. Den enskilde ska således kunna vända sig till och få hjälp eller information av dataskyddsbudet vid enheten även om behandlingen i det särskilda fallet helt eller delvis utförts av ett lufttrafikföretag, en behörig myndighet eller av utländska mottagare, dock bara såtillvida det varit fråga om en tillämpning av lagens bestämmelser. Om den enskilde har invändningar mot t.ex. lufttrafikföretags insamling av PNR-uppgifter får denne däremot vända sig till vederbörande lufttrafikföretag. Likaså får en enskild vända sig till vederbörande dataskyddsbud utanför enheten om det t.ex. handlar om användning av PNR-uppgifter i ett förundersökningsprotokoll. Dock bör

enhetens dataskyddsbud i sådana fall kunna lotsa en missnöjd eller undrande enskild vidare till rätt kontaktpunkt.

14 §

Paragrafen, som behandlas i avsnitt 19.5.4, reglerar dataskyddsbudets skyldighet att anmäla brister till tillsynsmyndigheten. Bestämmelsen genomför artikel 6.7 andra meningen.

Om den personuppgiftsansvarige inte följer regelverket för behandling av personuppgifter inom enheten för passagerarinformation ska dataskyddsbudet agera och anmäla detta till tillsynsmyndigheten. Någon rätt för den personuppgiftsansvarige att först vidta rättelse föreligger alltså inte. Däremot får det givetvis förutsättas att rättelse ändå sker snarast möjligt. Det är upp till dataskyddsbudet att bedöma om en anmälan ska ske. Att ett anställt dataskyddsbud med stöd av paragrafen gör en anmälan får inte leda till några konsekvenser för ombudet i arbetsrättsligt hänseende, eftersom det är fråga om en lagreglerad skyldighet.

Föreskrifter

15 §

I bestämmelsen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om utformande av kriterier, tillgång till PNR-information, dataskyddsbudets uppgifter, bevarande och gallring, dokumentation och loggning, information till dataskyddsbud samt enheten för passagerarinformations inhämtande av PNR-information från andra medlemsstater. Sådana bestämmelser finns i den till lagen anslutande förordningen.

4 kap. Överföring av PNR-information från enheten för passagerarinformation

Överföring till behöriga myndigheter

1 §

Paragrafen föreskriver i vilka situationer PNR-information ska överföras från enheten för passagerarinformation till en behörig nationell myndighet. Bestämmelsen, som delvis genomför artikel 6.2 a och b samt 6.5 och 6.6. i direktivet, behandlas i avsnitt 15.2.2.

Överföring till en behörig myndighet ska enligt *första stycket första punkten* ske för att vidarebefordra PNR-information avseende personer som vid den förhandsbedömning som görs av passagerare före deras beräknade ankomst till eller avresa från Sverige har ansetts vara intressanta för vidare granskning. Vidare ska enligt *andra punkten* PNR-information lämnas till en behörig myndighet som svar på en särskild motiverad förfrågan från den myndigheten. Förfrågan ska endast besvaras om den är motiverad och avser tillgång till PNR-information för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Om de begärda uppgifterna är äldre än sex månader och därför har maskerats ska även villkoren i 4 kap. 7 § vara uppfyllda för att en överföring av fullständiga, avmaskerade PNR-uppgifter ska kunna ske. Enligt *tredje punkten* ska enheten för passagerarinformation lämna över sådan PNR-information som har överförts från en motsvarande enhet i en annan medlemsstat.

Överföring från enheten för passagerarinformation till behöriga myndigheter ska endast ske i enskilda fall. PNR-information ska alltså inte per automatik föras vidare från enheten till en behörig myndighet. Vidare ska enligt *andra stycket* varje överlämnande till en behörig myndighet föregås av en bedömning av PNR-informationen utförd av en person som tjänstgör vid enheten för passagerarinformation. Granskningen ska ske för att t.ex., då en förhandsbedömning gett flera träffar, rensa bort information om personer som vid en snabb bedömning kan avfärdas såsom ointressanta för vidare granskning. Enheten bör också tillse att överföring bara sker till den behöriga myndighet som kan antas ha anledning att göra en vidare kontroll. Tanken är alltså inte att alla träffar som uppkommer vid en förhandsgranskning utan vidare ska skickas till alla befintliga be-

höriga myndigheter. Även då PNR-information ska lämnas vidare efter en begäran från en behörig myndighet ska en granskning göras, t.ex. för att säkerställa att uppgifterna går till den begärande myndigheten och att uppgifterna överensstämmer med vad begäran omfattat.

Överföring till andra medlemsstater

2 §

Bestämmelsen reglerar överföring till enheter för passagerarinformation i andra medlemsstater av sådan PNR-information som enheten för passagerarinformation väljer ut vid en förhandsbedömning av passagerare. Den genomför artikel 9.1 i direktivet och behandlas i avsnitt 15.3.2.

Resultatet av en förhandsbedömning av passagerare kan vara av intresse inte bara för behöriga nationella myndigheter utan även för en eller flera andra medlemsstater. Enligt bestämmelsen ska enheten för passagerarinformation därför självmant överföra resultatet av en förhandsbedömning till en motsvarande enhet i en annan medlemsstat. Bestämmelsen är formulerad som en uppgiftsskyldighet men en överföring ska dock endast ske om enheten bedömer att PNR-informationen är relevant och nödvändig för vidare granskning i den andra medlemsstaten för att där förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Det är först då det uppkommer en skyldighet att lämna PNR-informationen vidare. Det får därmed från fall till fall övervägas huruvida det är lämpligt att, utöver den överföring som ska ske till nationella behöriga myndigheter, även överföra PNR-informationen till en viss annan medlemsstat. En typisk situation när en överföring enligt bestämmelsen kan bli aktuell är när enheten för passagerarinformation har valt ut en viss person för vidare granskning inför dennes resa till en annan medlemsstat. Information om denne person ska då överföras till enheten för passagerarinformation i den medlemsstaten, om det bedöms relevant och nödvändigt med en vidare granskning där.

3 §

Paragrafen behandlar enheten för passagerarinformations behandling av förfrågningar från motsvarande enheter i andra medlemsstater om att få del av PNR-information. Den genomför artikel 9.2 och behandlas i avsnitt 15.3.2

Bestämmelsen innebär att enheten för passagerarinformation är skyldig att så snart som möjligt besvara en motiverad förfrågan från en enhet för passagerarinformation i en annan medlemsstat om att få del av PNR-information som bevaras i PNR-databasen och överföra de efterfrågade uppgifterna dit. För det fall enheten har tillgång till ett resultat av behandling av de aktuella PNR-uppgifterna som har tagits fram i samband med en förhandsbedömning av uppgifterna, och detta resultat ännu inte har gallrats, ska även det resultatet överföras. Enheten för passagerarinformation är dock inte skyldig att på begäran av en annan enhet exempelvis jämföra PNR-uppgifterna med uppgifter i något register eller någon annan uppgiftssamling. Endast för det fall en sådan förhandsbedömning redan är genomförd och alltså finns sparad vid enheten ska resultatet av den också överföras.

I att förfrågan ska vara motiverad ligger ett krav på att den ska innehålla tillräckliga uppgifter för att det ska gå att bedöma om PNR-informationen ska användas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet. Om så inte är fallet, ska PNR-informationen inte överföras.

Om den begärda PNR-informationen är äldre än sex månader och därför har maskerats ska även villkoren i 4 kap. 7 § vara uppfyllda för att en överföring av avmaskerade PNR-uppgifter ska kunna ske.

4 §

Paragrafen reglerar översändande från enheten för passagerarinformation direkt till en myndighet som har utsetts som behörig i en annan medlemsstat. Den genomför artikel 9.3 i direktivet och behandlas i avsnitt 15.3.3.

PNR-uppgifter ska som huvudregel utbytas mellan medlemsstaterna bara via deras enheter för passagerarinformation. PNR-direktivet innehåller dock en möjlighet för en medlemsstats behöriga

myndigheter att i undantagsfall vända sig direkt till enheten för passagerarinformation i en annan medlemsstat med en begäran om överföring av PNR-information. Av aktuell bestämmelse framgår att enheten för passagerarinformation endast i ett enskilt brådskande fall där det är absolut nödvändigt är skyldig att besvara en motiverad förfrågan från en myndighet som har utsetts som behörig i en annan medlemsstat och överföra PNR-information dit. Av artikel 7.3 i PNR-direktivet framgår att medlemsstaterna ska meddela kommissionen sin förteckning över behöriga myndigheter. Kommissionen ska offentliggöra dessa och eventuella ändringar i Europeiska unionens officiella tidning. När en myndighet vänder sig direkt till den svenska enheten för passagerarinformation ska det alltså vara enkelt för enheten att få fram uppdaterad information om myndigheten i fråga är en behörig myndighet enligt PNR-direktivet i sitt land.

Överföring av PNR-information direkt till en myndighet som har utsetts som behörig i en annan medlemsstat ska i övrigt ske endast under samma förutsättningar som överföring till en annan enhet för passagerarinformation. Det innebär bl.a. att endast motiverade förfrågningar ska besvaras. Om de begärda uppgifterna är äldre än sex månader och därför har maskerats ska även villkoren i 4 kap. 7 § vara uppfyllda för att en överföring av fullständiga, avmaskerade PNR-uppgifter ska kunna ske.

5 §

Paragrafen behandlar inhämtande av PNR-uppgifter från lufttrafikföretag på andra tider än normalt på begäran av en enhet för passagerarinformation i en annan medlemsstat. Bestämmelsen genomför artikel 9.4 i direktivet och behandlas i avsnitt 15.3.2.

Av 2 kap. 3 § framgår att enheten för passagerarinformation kan begära att lufttrafikföretag ska överföra PNR-uppgifter även vid andra tidpunkter än de som anges i 2 kap. 2 § om det i ett enskilt fall bedöms nödvändigt med tillgång till PNR-uppgifter för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet. Aktuell paragraf föreskriver att enheten för passagerarinformation under i övrigt samma omständigheter ska begära in PNR-uppgifter från lufttrafikföretag vid andra tidpunkter än normalt på begäran av en enhet för passagerarinformation i en

annan medlemsstat, för att därefter översända uppgifterna till den efterfrågande enheten.

Överföring till Europol

6 §

Paragrafen genomför artikel 10 och behandlas i avsnitt 15.4.

Av bestämmelsen framgår att enheten för passagerarinformation på begäran ska överföra efterfrågad PNR-information till Europol. Överföring enligt bestämmelsen kan ske såväl av förhandsinformation om passagerare som av äldre uppgifter som lagras i databasen över PNR-uppgifter. En begäran från Europol om att få ta del av PNR-information ska vara motiverad. I att begäran ska vara motiverad ligger ett krav på information som tydliggör att syftet med behandlingen av den mottagna informationen är att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Om de begärda PNR-uppgifterna är äldre än sex månader och därför har maskerats ska även villkoren i 4 kap. 7 § vara uppfyllda för att en överföring av avmaskerade PNR-uppgifter ska kunna ske.

Överföring av avmaskerade PNR-uppgifter

7 §

Paragrafen behandlar förutsättningarna för överföring av avmaskerade PNR-uppgifter från enheten för passagerarinformation. Den genomför artikel 12.3 i direktivet och behandlas i avsnitt 15.5.

Avmaskerade PNR-uppgifter definieras i 1 kap. 3 §. Enligt denna bestämmelse kan översändande av sådana äldre och fullständiga PNR-uppgifter ske på särskild begäran från en behörig mottagare eller ett tredjeland. En överföring får dock endast ske om det kan antas vara nödvändigt för att besvara begäran. Enheten ska före överföringen göra en egen prövning av motiven till begäran och bedöma om det rimligen kan antas vara nödvändigt för att besvara den korrekt att mottagaren i sin bekämpning av terroristbrottslighet eller grov brottslighet får tillgång inte bara till maskerade PNR-uppgifter utan även till de fullständiga uppgifterna. Prövningen kan göras täm-

ligen summariskt och inskränka sig till en kontroll av att det av begäran framgår att framställningen även omfattar utfående av avmaskerade, fullständiga uppgifter om en person. Därutöver ska, som vid samtliga överföringar från enheten, kontrolleras att mottagarens begäran sker i syfte att använda mottagna uppgifter för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottlighet. Som en ytterligare förutsättning för överföring av avmaskerade uppgifter krävs ett beslut eller tillstånd enligt 8 eller 9 §.

Enligt bestämmelsen får avmaskerade PNR-uppgifter överföras som svar på en begäran från en myndighet som har utsetts som behörig i en annan medlemsstat. Enligt 4 kap. 4 § ska dock enheten för passagerarinformation endast besvara en sådan begäran i ett enskilt brådskande undantagsfall. I praktiken torde det knappast vara nödvändigt att överföra äldre, avmaskerade PNR-uppgifter i en sådan situation.

8 §

Bestämmelsen behandlas i avsnitt 15.5.4.

För det fall en förundersökning har inletts ska en begäran från behöriga svenska myndigheter om att få tillgång till fullständiga, avmaskerade, PNR-uppgifter ha beslutats av allmän åklagare. Så är fallet även om allmän åklagare inte är förundersökningsledare. Åklagaren ska inför sitt beslut avgöra om tillgång till uppgifterna rimligen kan antas vara nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottlighet. Beslutet ska dokumenteras i förundersökningsmaterialet.

9 §

Bestämmelsen behandlas i avsnitt 15.5.4.

I de fall begäran om utfående av avmaskerade PNR-uppgifter framställs i underrättelsearbete eller om begäran kommer från en enhet för passagerarinformation i en annan medlemsstat, en myndighet som har utsetts som behörig i en annan medlemsstat, Europol eller ett tredjeland, ska enheten för passagerarinformation inhämta tillstånd till överföring av sådana fullständiga PNR-uppgifter från myndighetschefen för Polismyndigheten, dvs. rikspolischefen. Rätten

att fatta beslut om tillstånd får delegeras till en annan anställd vid myndigheten som har rätt kompetens, utbildning och erfarenhet. Delegation får dock inte ske till någon som själv deltar i den verksamhet som har begärt ut informationen. Inte heller får delegation ges till någon som arbetar vid enheten för passagerarinformation. Den som fattar beslutet ska avgöra om tillgång till fullständiga avmaskerade PNR-uppgifter rimligen kan antas vara nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet.

Av den till lagen hörande förordningen framgår att dataskyddsombudet vid enheten för passagerarinformation ska informeras och göra en efterhandsutvärdering av varje överföring av avmaskerade uppgifter enligt denna bestämmelse.

5 kap. Behöriga myndigheters behandling av PNR-information

Gallring av PNR-information

1 §

Bestämmelsen behandlar frågan om gallring av resultatet av förhandsbedömningar hos de behöriga myndigheterna. Den motsvaras inte av någon bestämmelse i direktivet och behandlas i avsnitt 18.8.

För det fall en behörig myndighet, som har mottagit PNR-information från enheten för passagerarinformation med resultat från enhetens förhandsbedömning av passagerare, vid sin granskning finner att informationen saknar betydelse för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet, ska denna information gallras av den behöriga myndigheten. Resultatet av sådana förhandsbedömningar av passagerare som visar sig sakna betydelse för den brottsbekämpande verksamheten ska således inte bevaras hos de behöriga myndigheterna. Motsvarande bestämmelser finns för bokningsuppgifter från transportörer i 26 § tredje stycket polislagen (1984:387), 4 kap. 8 § tredje stycket tullagen (2016:253 och 16 § tredje stycket lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen.

Det kan från fall till fall ta olika lång tid innan det går att konstatera om en uppgift saknar betydelse för den angivna brottslig-

heten. Så snart detta har konstaterats ska dock PNR-informationen gallras genom att raderas.

2 §

Paragrafen behandlar frågan om gallring av känsliga personuppgifter hos de behöriga myndigheterna. Bestämmelsen genomför artikel 13.4 i direktivet och behandlas i avsnitt 18.5.

Eftersom enheten för passagerarinformation inte får behandla PNR-uppgifter som utgör känsliga personuppgifter ska sådana uppgifter inte heller föras över från enheten till de behöriga myndigheterna. Med hänsyn till det stora antalet PNR-uppgifter som behandlas vid enheten kan det dock i något fall ändå av misstag förekomma att sådana uppgifter förs vidare. För det fall ett sådant misstag skulle inträffa och PNR-uppgifter som utgör känsliga personuppgifter skulle överföras till en behörig myndighet, ska den behöriga myndigheten omedelbart radera dessa. Bestämmelsen är utformad på samma sätt som motsvarande bestämmelse för enheten för passagerarinformation i 3 kap. 10 §.

Annan behandling av PNR-information

3 §

Paragrafen innehåller ett undantag från bestämmelsen om otillåten behandling av PNR-uppgifter i 1 kap. 5 §. Den genomför artikel 7.5 i direktivet och behandlas i avsnitt 16.2.3.

Bestämmelsen innebär en möjlighet för de behöriga myndigheterna att förhindra, utreda och lagföra mindre allvarlig eller annat slags brottslighet som upptäcks i samband med en brottsbekämpande insats som görs till följd av sådan PNR-information som myndigheten har fått från en enhet för passagerarinformation. Om denna PNR-information leder till att den behöriga myndigheten genomför en brottsbekämpande insats avseende terroristbrottslighet eller grov brottslighet och det vid denna insats framkommer misstankar om sådan brottslighet som faller utanför direktivet, har myndigheten alltså rätt att agera även på dessa misstankar för att förhindra, utreda eller lagföra brott.

Med en brottsbekämpande insats avses olika möjliga åtgärder som kan ske till följd av sådan misstänkt brottslighet som omfattas av direktivet. Det kan t.ex. röra sig om ett förhör, en husrannsakan, en brottsplatsundersökning, ett beslag eller en spaningsoperation. Huruvida en förundersökning har inletts är inte avgörande.

Automatiserade beslut

4 §

Paragrafen behandlar automatiserade beslut hos de behöriga myndigheterna. Den genomför artikel 7.6 och behandlas i avsnitt 16.2.4.

Av bestämmelsen framgår att de behöriga myndigheterna inte får fatta några beslut som har rättsliga konsekvenser för en person eller på annat sätt allvarligt påverkar denne endast på grund av den automatiska behandlingen av PNR-uppgifter. Ett beslut baserat på PNR-uppgifter måste således alltid föregås av en bedömning gjord av en tjänsteman vid myndigheten. Enligt bestämmelsen får besluten inte heller grunda sig på känsliga personuppgifter.

Föreskrifter

5 §

I bestämmelsen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om behöriga myndigheters inhämtande och behandling av PNR-information.

6 kap. Överföring till tredjeland

1 §

Bestämmelsen reglerar överföringen av PNR-information från enheten för passagerarinformation till ett tredjeland. Bestämmelsen genomför artikel 11.1 i direktivet och behandlas i avsnitt 17.3.2.

Av bestämmelsen framgår att enheten för passagerarinformation får överföra PNR-information till tredjeland. Det är däremot inte, som i brottsdatalagen, tillåtet att överföra PNR-information till internationella organisationer. Tredjeland definieras i 1 kap. 3 §. Vidare

får PNR-information endast överföras till en sådan myndighet i det tredjelandet som där är behörig att bedriva verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra brott motsvarande terroristbrottslighet eller grov brottslighet.

Samtliga villkor i bestämmelsen ska vara uppfyllda för att enheten ska få överföra PNR-information till ett tredjeland.

Enligt *första punkten* får uppgifterna endast överföras om förutsättningarna för överföring av PNR-information mellan medlemsstaterna är uppfyllda. Vidare ska de grundläggande förutsättningarna för överföring av personuppgifter enligt 8 kap. 1 § första stycket 3 och 2 § första stycket BDL vara uppfyllda. I de bestämmelserna anges bl.a. att en överföring ska omfattas av beslut om adekvat skyddsnivå, av tillräckliga skyddsåtgärder eller vara föremål för ett undantag för särskilda situationer. Där anges också att personuppgifter som har erhållits från en annan medlemsstat som huvudregel endast får överföras om den medlemsstat som har lämnat uppgifterna har medgett att de överförs. För det fall överföringen avser PNR-information som enheten för passagerarinformation har fått från en annan medlemsstat och något medgivande till överföringen inte har hunnits hämtas in från den medlemsstaten, ska även bestämmelsen i 2 § vara uppfylld.

Av *andra punkten* framgår att en överföring ska vara nödvändig för att förebygga, förhindra, upptäcka, utreda eller lagföra brott som motsvarar terroristbrottslighet eller grov brottslighet. Med att överföringen ska vara nödvändig menas att det är fråga om något som behövs. De PNR-uppgifter som överförs ska således behövas t.ex. för att en behörig myndighet i ett tredjeland ska kunna lagföra brott som motsvarar terroristbrottslighet eller grov brottslighet. Om en myndighet i ett tredjeland begär att få tillgång till PNR-uppgifter ska enheten för passagerarinformation således pröva om den utländska myndigheten behöver uppgifterna för ett syfte som omfattas av lagens tillämpningsområde.

Enligt *tredje punkten* ska det tredjelandet också godta att endast vidareöverföra uppgifterna till ett annat tredjeland om det är absolut nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra brott motsvarande terroristbrottslighet eller grov brottslighet och enheten för passagerarinformation har lämnat ett uttryckligt medgivande till vidareöverföringen. Medgivandet kan ske såväl muntligt

som skriftligt. För att det i efterhand ska gå att kontrollera bör dock medgivandet dokumenteras av enheten för passagerarinformation.

I den anslutande förordningen regleras att enheten för passagerarinformation i samband med en överföring av PNR-information till ett tredjeland ska uppställa villkor om användningsbegränsning i syfte att skydda PNR-informationen från användning i strid med PNR-direktivet.

2 §

Paragrafen behandlar frågan om överföring till tredjeland utan förhandsmedgivande. Den genomför artikel 11.2 i direktivet och behandlas i avsnitt 17.3.3.

Bestämmelsen innebär att för det fall den PNR-information som ska överföras har erhållits från en annan medlemsstat och något förhandsmedgivande till överföringen inte har hunnit inhämtas från den medlemsstaten, får informationen ändå överföras om det är absolut nödvändigt för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller grov brottslighet. Med uttrycket absolut nödvändigt markeras att undantaget ska tillämpas restriktivt och att det endast i undantagsfall kan bli fråga om överföring utan förhandssamtycke. Bestämmelsen kan bli tillämplig t.ex. om en överföring är nödvändig för att avvärja ett terroristattentat i en medlemsstat eller tredjeland. Eftersom det typiskt sett är fråga om en överhängande fara för att något ska hända får prövningen i dessa fall göras utifrån att åtgärden kan antas vara nödvändig för att avvärja faran. Att det sedan i efterhand visar sig att överföringen inte var nödvändig, t.ex. därför att faran aldrig realiserades, innebär inte att överföringen var otillåten.

I den anslutande förordningen anges att om PNR-information, som kommer från en annan medlemsstat, har överförts till ett tredjeland utan förhandsmedgivande, ska enheten för passagerarinformation utan dröjsmål informera den andra medlemsstaten om överföringen. I förordningen regleras också att överföringar utan förhandsmedgivande ska genomgå efterhandskontroll av dataskyddsombudet vid enheten för passagerarinformation.

3 §

Bestämmelsen, som reglerar förhållandet till brottsdatalagen, behandlas i avsnitt 17.3.4. Den motsvaras inte av någon artikel i direktivet.

8 kap. 8 § BDL föreskriver en möjlighet att i enskilda fall överföra personuppgifter till andra organ i ett tredjeland än behöriga myndigheter. Denna möjlighet är inte tillämplig vid överföring av PNR-information, som endast får överföras till en myndighet i ett tredjeland som där är behörig att bedriva verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra brott motsvarande terroristbrottslighet eller grov brottslighet (se 1 §).

4 §

I paragrafen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om information till en annan medlemsstat när personuppgifter, som enheten för passagerarinformation har fått från den andra medlemsstaten, har överförts till ett tredjeland utan förhandsmedgivande samt om uppställande av villkor om användningsbegränsning av PNR-information som överförts till ett tredjeland.

7 kap. Övriga bestämmelser

Enskildas rättigheter

1 §

Paragrafen reglerar rätten till radering eller begränsning av behandling av personuppgifter. Den behandlas i avsnitt 20.3.3. Bestämmelsen genomför till viss del artikel 13.1 i direktivet.

4 kap. 10 § BDL innehåller bestämmelser om en registrerads rätt till radering eller begränsning av behandling av personuppgifter. Av *första stycket* följer att de aktuella bestämmelserna även ska gälla för det fall personuppgifter behandlas i strid med vissa centrala bestämmelser i denna lag. Bestämmelserna avser lagens portalbestämmelse om otillåten behandling av personuppgifter, förbudet mot behandling av känsliga personuppgifter samt förpliktelsen att gallra PNR-uppgifter som har överförts från lufttrafikföretag efter fem år.

Av *andra stycket* följer att sådana beslut om radering eller begränsning av uppgifter som anges i bestämmelsen kan överklagas till allmän förvaltningsdomstol.

2 §

Paragrafen behandlar skadestånd vid otillåten behandling av personuppgifter. Den genomför till viss del artikel 13.1 i direktivet och behandlas i avsnitt 20.4.3.

Av bestämmelsen följer att brottsdatalagens bestämmelser om skadestånd ska gälla även när personuppgifter behandlas i strid med denna lag eller föreskrifter som meddelats med stöd av den. Bestämmelsen är bara tillämplig för överträdelser av lagens bestämmelser som avser att ge skydd för personuppgifter. Om ett lufttrafikföretag bryter mot bestämmelserna i 2 kap. genom att inte överföra PNR-uppgifter till enheten för passagerarinformation eller när enheten för passagerarinformation bryter mot sin skyldighet att besvara förfrågningar från behöriga myndigheter eller fullgöra sina förpliktelser om informationsutbyte med andra medlemsstater enligt 4 kap. ska skadeståndsbestämmelsen inte tillämpas.

Tillsyn

3 §

Paragrafen behandlas i avsnitt 21.3. Den genomför artikel 15 i direktivet.

Bestämmelsen föreskriver att den tillsynsmyndighet som avses i brottsdatalagen ska ha tillsyn över all personuppgiftsbehandling enligt lagen. Det har således ingen betydelse om personuppgiftsbehandlingen har utförts av enheten för passagerarinformation, ett lufttrafikföretag eller en behörig myndighet. Tillsynsmyndighetens uppgifter och befogenheter regleras i brottsdatalagen.

Sanktionsavgifter vid överträdelser av enheten för passagerarinformation eller en behörig myndighet

4 §

Paragrafen reglerar vid vilka överträdelser av lagens bestämmelser som administrativ sanktionsavgift får tas ut av en personuppgiftsansvarig myndighet. Den genomför artikel 14.1 och innebär att sanktioner kan tillgripas vid överträdelser av de bestämmelser i lagen som har till syfte att skydda enskildas integritet. Bestämmelsen behandlas i avsnitt 22.4.3.

Tillsynsmyndigheten avgör i det enskilda fallet om sanktionsavgift bör tas ut, vilket framgår av formuleringen att avgift får tas ut. Paragrafen föreskriver att sanktionsavgift får tas ut av den personuppgiftsansvariga myndigheten, oavsett om en överträdelse har skett vid enheten för passagerarinformation eller vid en behörig myndighet.

I paragrafen anges uttömmande vilka överträdelser som kan föranleda sanktionsavgift. Enligt *punkten 1* kan sanktionsavgift tas ut vid överträdelser av bestämmelsen om att PNR-uppgifter inte får behandlas för andra syften än att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller grov brottslighet samt vid överträdelser av förbudet mot behandling av känsliga personuppgifter. Enligt *punkten 2* kan sanktionsavgift utgå för överträdelse av flertalet av bestämmelserna i 3 kap. om hur PNR-information får behandlas vid enheten för passagerarinformation. Det innebär bl.a. att behandling av PNR-uppgifter för andra ändamål än de som anges i lagen kan leda till sanktionsavgift. Detsamma gäller vid överträdelse av de bestämmelser som begränsar tillgången till PNR-information och förbjuder direktåtkomst. Även överträdelser av lagens bestämmelser om maskering av PNR-uppgifter, bevarande och gallring kan föranleda sanktionsavgift. Av *punkten 3* framgår att överträdelser av bestämmelserna om överföring av avmaskerade PNR-uppgifter kan föranleda sanktionsavgift. Även överträdelser av vissa bestämmelser om hur PNR-uppgifter får användas vid de behöriga myndigheterna kan enligt *punkten 4* bli föremål för sanktionsavgift. Vid överträdelser av regler om överföring till tredjeland kan enligt *punkten 5* sanktionsavgift också tas ut.

5 §

Bestämmelsen behandlas i avsnitt 22.4.3. I *första stycket* föreskrivs att sanktionsavgiftssystemet i brottsdatalagen och den tillhörande förordningen ska tillämpas även vid överträdelser enligt denna lag.

Av *andra stycket* framgår att de i brottsdatalagen föreslagna minimi- och maximibeloppen för allvarigare överträdelser ska tillämpas när sanktionsavgiften ska bestämmas. Utgångspunkten vid bestämmandet av sanktionsavgift är den behandling som skett av personuppgifterna.

I *tredje stycket* upplyses om att beslut om sanktionsavgift kan överklagas till allmän förvaltningsdomstol enligt 7 kap. 4 § BDL

28.2 Förslaget till lag om ändring i polislagen (1984:387)

25 §

Paragrafen, som behandlas bl.a. i avsnitt 25, reglerar skyldigheten för transportörer av varor, passagerare eller fordon till eller från Sverige att på begäran lämna vissa bokningsuppgifter till Polismyndigheten eller Säkerhetspolisen.

Första och andra stycket är oförändrade.

I *tredje stycket* anges att första och andra stycket inte ska gälla för det fall lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen är tillämplig.

28.3 Förslaget till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen

15 §

Paragrafen, som behandlas bl.a. i avsnitt 25, reglerar skyldigheten för transportörer av varor, passagerare eller fordon till eller från Sverige att på begäran lämna vissa bokningsuppgifter till Tullverket.

Första och andra stycket är oförändrade.

I *tredje stycket* anges att första och andra stycket inte ska gälla för det fall lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen är tillämplig.

28.4 Förslaget till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

1 kap.

1 a §

Paragrafen, som behandlas i avsnitt 8.5, reglerar förhållandet till lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen. Bestämmelsen är ny.

Genom paragrafen föreskrivs att för det fall det i lagen om flygpassageraruppgifter i brottsbekämpningen finns avvikande bestämmelser, ska dessa tillämpas i stället för bestämmelserna i denna lag.

28.5 Förslaget till lag om ändring i polisdatalagen (2010:361)

1 kap.

4 a §

Paragrafen, som behandlas i avsnitt 8.5, reglerar förhållandet till lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen. Bestämmelsen är ny.

Genom paragrafen föreskrivs att för det fall det i lagen om flygpassageraruppgifter i brottsbekämpningen finns avvikande bestämmelser, ska dessa tillämpas i stället för bestämmelserna i polisdatalagen. Det gäller oavsett om det handlar om personuppgiftsbehandling vid enheten för passagerarinformation eller en behörig myndighet som omfattas av polisdatalagens tillämpningsområde.

28.6 Förslaget till lag om ändring i tullagen (2016:253)

4 kap.

6 a §

Paragrafen, som behandlas i avsnitt 25, reglerar förhållandet mellan lagens bestämmelser om Tullverkets tillgång till transportörers bokningsuppgifter och lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen. Bestämmelsen är ny.

Av bestämmelsen framgår att skyldigheten enligt 4 kap. 6 § tullagen för transportörer av varor, passagerare eller fordon till eller från Sverige att på begäran lämna vissa bokningsuppgifter till Tullverket inte ska gälla för det fall lagen om flygpassageraruppgifter i brottsbekämpningen är tillämplig.

28.7 Förslaget till lag om ändring i tullbrottsdatalagen (2017:000)

2 kap.

8 §

Paragrafen, som behandlas bl.a. i avsnitt 8.5, reglerar behandling av personuppgifter som har lämnats till Tullverket från transportföretag. I ett nytt *tredje stycke* föreskrivs att för det fall det i lagen (2018:000) om flygpassageraruppgifter i brottsbekämpningen finns avvikande bestämmelser ska dessa tillämpas i stället. Paragrafen är i övrigt oförändrad.

Särskilt yttrande

**av experterna Kurt Alavaara, Britt-Louise Wahlberg
och Eric Åmell**

Av utredningen framgår att cirka 60 procent av alla bokningar av flygbiljetter inom EU och internationellt utförs av resebyråer. Sannolikt kommer denna typ av bokningar att öka i framtiden i takt med att användandet av internet ökar globalt. I samband med att PNR-direktivet antogs gjorde Europeiska unionens råd ett uttalande av vilket framgår att medlemsstaterna förklarar att de i enlighet med Europaparlamentets önskemål åtar sig att i enlighet med sin nationella lagstiftning utvidga insamlingen av PNR-uppgifter till att omfatta aktörer som inte är lufttrafikföretag. Som sådana aktörer nämns särskilt resebyråer och researrangörer.

Vi anser att det redan nu finns mycket goda skäl att införa en ökad skyldighet för dessa aktörer att överföra PNR-uppgifter till den svenska enheten för passagerarinformation. Utredningen har dock inte lagt fram något sådant förslag. Ur ett brottsbekämpningsperspektiv är det väldigt olyckligt och kan leda till att den nya regleringen inte blir så framgångsrik som det var tänkt. Vi vill framhålla att det är av mycket stor vikt att även dessa aktörer inom kort omfattas av samma överföringsskyldighet. Vi vill också betona vikten av att arbetet med att ta fram en sådan reglering inleds snarast.

Kommittédirektiv 2016:22

Genomförande av direktiv om användning av passageraruppgiftssamlingar

Beslut vid regeringssammanträde den 17 mars 2016

Sammanfattning

En särskild utredare ska föreslå hur direktivet om användning av passageraruppgiftssamlingar för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (PNR-direktivet) ska genomföras i svensk rätt. Utredaren ska föreslå ett system för hanteringen av flygpassageraruppgifter och den reglering för personuppgiftsbehandling och sekretess som detta kräver. Utredaren ska också lämna de författningsförslag som krävs för att svensk lagstiftning ska leva upp till direktivet och den deklaration som medlemsstaterna ska anta samtidigt som direktivet. Vid utformningen av regleringen ska skyddet för enskildas personliga integritet särskilt beaktas.

Uppdraget ska redovisas senast den 31 maj 2017.

PNR-direktivet

Passageraruppgiftssamlingar består av uppgifter som lämnats av passagerare (Passenger Name Records – PNR) och samlats in av lufttrafikföretag (härefter benämnda flygbolag) i samband med beställning och bokning av biljetter samt vid incheckning, t.ex. namn, betalningsätt, bagageinformation, destination och resebolag. Flyg-

bolag samlar redan i dag in och behandlar sådana uppgifter om sina passagerare för kommersiella syften.

Ett direktiv om användning av passageraruppgiftssamlingar för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (PNR-direktivet) kommer att antas inom kort. Medlemsstaterna måste genomföra direktivet i nationell rätt inom två år efter att det trätt i kraft.

Direktivet reglerar skyldigheten för flygbolag att överföra passageraruppgiftssamlingar till enheter för passagerarinformation i medlemsstaterna, för vilka ändamål uppgifterna får behandlas, hur länge uppgifterna får lagras och under vilka förutsättningar de får lämnas ut. Flygpassageraruppgifterna får endast behandlas för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Terroristbrott definieras som de brott enligt nationell rätt som avses i artiklarna 1–4 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism. Med grov brottslighet avses de brott som listas i bilaga II till direktivet, t.ex. människohandel, olaglig handel med narkotika, våldtäkt och sabotage, om de kan bestraffas med fängelse eller annan frihetsberövande åtgärd i minst tre år enligt nationell rätt.

Direktivet innehåller även andra bestämmelser om dataskydd.

Utredningsuppdraget

Allmänna utgångspunkter

Utredarens övergripande uppdrag är att analysera direktivet och föreslå de författningsändringar och andra åtgärder som krävs för att PNR-systemet ska kunna genomföras i svensk rätt. Förslagen ska sammantaget ge en väl balanserad reglering. I det ligger att utredaren ska ta hänsyn till intresset av en rättssäker och effektiv brottsbekämpning samtidigt som skyddet för den personliga integriteten och andra grundläggande fri- och rättigheter säkerställs. Vid utformningen av de författningsförslag som lämnas ska utredaren beakta EU:s stadga om de grundläggande rättigheterna (EUT C 83, 30.3.2010, s. 389) och de internationella konventioner på området som Sverige är förpliktat att följa. Utredaren ska vidare eftersträva kostnadseffektiva lösningar för dem som berörs av direktivet.

Direktivet kräver endast att flygbolagen lämnar passageraruppgiftssamlingar för flygtransporter som anländer från eller avgår till ett land utanför Europeiska unionen (EU). Medlemsstaterna har också möjlighet att tillämpa det på flygningar inom EU. Medlemsstaterna kommer i en deklARATION som ska antas samtidigt som direktivet åta sig att utnyttja denna möjlighet. Genom deklARATIONEN har medlemsstaterna även uttalat att man ska eftersträva att, med hänsyn till nationellt parlamentariskt förfarande, införa nationella bestämmelser som innebär skyldighet att överföra flygpasageraruppgifter även för ekonomiska aktörer som inte är transportörer, t.ex. de resebyråer och researrangörer som erbjuder bokningsförmedling vid vilken sådana uppgifter samlas in och behandlas. Utgångspunkten för uppdraget är därför att direktivet även ska tillämpas på flygningar inom EU och att skyldigheten att föra över flygpasageraruppgifter till de nationella enheterna i medlemsstaterna även ska omfatta resebyråer och researrangörer.

Utredaren ska föreslå ett system för hanteringen av flygpasageraruppgifter och den reglering för personuppgiftsbehandling och sekretess som detta kräver. Utredaren ska även analysera om och i så fall hur PNR-direktivet påverkar det svenska genomförandet av rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare (API-direktivet).

Ett system för hantering av flygpasageraruppgifter

PNR-direktivet ställer krav på medlemsstaterna att se till att det finns ett fungerande system för att hantera flygpasageraruppgifter. Enligt direktivet ska flygbolag överföra flygpasageraruppgifter för ankommande och avgående transporter till den medlemsstat som flyget ankommer till eller avgår ifrån. I enlighet med den deklARATION som medlemsstaterna ska anta ska det eftersträvas att det i nationell rätt föreskrivs samma skyldighet för resebyråer och researrangörer. Medlemsstaterna ska säkerställa att det i nationell rätt införs effektiva proportionella och avskräckande sanktioner, inklusive ekonomiska sådana, för flygbolag som inte uppfyller sina skyldigheter enligt direktivet vad gäller överföring av uppgifter eller som inte översänder uppgifterna i det fastställda formatet. För svenskt vidkommande bör ett sådant system vara uppbyggt enligt den struktur som redan gäller

i dag, dvs. att en myndighets beslut om sanktioner kan överklagas till allmän förvaltningsdomstol.

Varje medlemsstat ska inrätta eller utse en myndighet eller del av myndighet med behörighet att förebygga, upptäcka, utreda och lagföra terroristbrott och grov brottslighet som ska fungera som medlemsstatens enhet för passagerarinformation. Enheten ska ansvara för att samla in flygpassageraruppgifter från flygbolagen, lagra, behandla och överföra dessa uppgifter eller resultatet av behandlingen av dem till behöriga brottsbekämpande myndigheter. Enheten ska också ansvara för att utbyta flygpassageraruppgifter och resultatet av behandlingen av sådana uppgifter med andra medlemsstaters enheter för passagerarinformation och med Europol. Enheten ska lagra uppgifterna i fem år. Efter sex månader ska uppgifterna maskeras på ett sådant sätt att passageraren inte kan identifieras. De insamlade uppgifterna får endast behandlas för vissa angivna ändamål och lämnas ut under vissa förutsättningar. Polismyndigheten har till uppgift att förebygga, upptäcka och utreda de flesta av de brott som omfattas av direktivet. Utgångspunkten för uppdraget är därför att den nationella enheten ska placeras vid Polismyndigheten. Myndigheten ska även ansvara för genomförandet av direktivets tekniska bestämmelser.

Medlemsstaterna ska utse de myndigheter som ska vara behöriga att begära eller ta emot flygpassageraruppgifter och underrätta Europeiska kommissionen om dessa senast ett år efter det att direktivet trätt i kraft. Regeringen kommer inom kort att utse dessa myndigheter och det ingår därför inte i uppdraget att föreslå vilka myndigheter som ska anses behöriga enligt direktivet.

Utredaren ska föreslå

- ett system för hur flygpassageraruppgifter ska hanteras i Sverige,
- hur enheten för passagerarinformation ska organiseras,
- vilka sanktioner som ska kunna åläggas flygbolag som inte uppfyller sina skyldigheter enligt direktivet, och
- de författningsändringar som behövs.

Behandling av personuppgifter och sekretess

Ett effektivt system för hantering av flygpassageraruppgifter förutsätter att uppgifter kan överföras inom systemet. Samtidigt måste skyddet för enskildas personliga integritet säkerställas.

För att myndigheter ska kunna utbyta information krävs att informationen inte omfattas av sekretess eller att sekretessen kan brytas. Vidare krävs att det finns stöd för att uppgifterna får lämnas ut. Regler om utlämnande av uppgifter från en myndighet till en annan finns, vad gäller den behandling som direktivet föreskriver, dels i offentlighets- och sekretesslagen (2009:400), dels i de författningar som reglerar myndigheternas personuppgiftsbehandling. Dessa är polisdatalagen (2010:361) och lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Enligt direktivet ska medlemsstaterna säkerställa att den behandling av personuppgifter som sker vid den nationella enheten och vid behöriga brottsbekämpande myndigheter omfattas av nationella dataskyddsbestämmelser som överensstämmer med rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) och de dataskyddsbestämmelser som finns angivna i PNR-direktivet. Med hänvisningen till dataskyddsrambeslutet ska förstås såväl nuvarande lagstiftning som de framtida bestämmelser som kommer att ersätta detta. Inom kort kommer nämligen ett nytt direktiv att antas med regler om skydd av personuppgifter när myndigheter behandlar sådana uppgifter vid brottsbekämpning, brottmålshantering eller straffverkställighet (det nya dataskyddsdirektivet).

Utredaren ska därför

- analysera vilken personuppgiftsbehandling som aktualiseras vid tillämpningen av direktivet,
- ta ställning till om reglerna i offentlighets- och sekretesslagen innebär ett tillräckligt skydd för de uppgifter som ska utbytas enligt direktivet eller om nuvarande lagstiftning behöver ändras för att Sverige ska leva upp till bestämmelserna i direktivet,
- föreslå en reglering för personuppgiftsbehandling och sekretess som passar in i den befintliga svenska strukturen och ger en rätts-

säker och mer effektiv brottsbekämpning samtidigt som skyddet för den personliga integriteten säkerställs, och

- i den utsträckning det är möjligt, beakta det arbete som genomförs av den utredning som kommer att få i uppdrag att genomföra det nya dataskyddsdirektivet.

Påverkar PNR-direktivet det svenska genomförandet av API-direktivet?

Enligt bilaga I till direktivet omfattar flygpassageraruppgifter bl.a. förhandsuppgifter om passagerare (Advance Passenger Information, API). Inhämtandet av sådana uppgifter regleras i direktiv 2004/82/EG om skyldighet för transportörer att lämna uppgifter om passagerare (API-direktivet). API-direktivet har genomförts i svensk rätt genom en bestämmelse i 9 kap. 3 a § utlänningslagen (2005:716) och genom lagen (2006:444) om passagerarregister. Bestämmelsen i utlänningslagen innebär att en transportör som luftvägen transporterar passagerare till Sverige från en stat utanför Schengenområdet, på begäran av Polismyndigheten ska överföra uppgifter om de ankommande passagerarna så snart incheckningen avslutats. Informationen ska föras över till Polismyndigheten som ska spara uppgifterna i ett passagerarregister.

PNR-direktivet innebär en skyldighet för flygbolag att överföra de förhandsuppgifter om passagerare och flygpassageraruppgifter som framgår av bilaga I till direktivet. Tillämpningen av bestämmelserna i PNR-direktivet ska i övrigt inte påverka tillämpningen av API-direktivet.

I regeringens skrivelse Förebygga, förhindra, försvåra – den svenska strategin mot terrorism (skr. 2014/15:146) anges att systemet för hantering av flygpassageraruppgifter bör samordnas med systemet för API-uppgifter, eftersom de tillsammans kan vara ett användbart verktyg i terrorismbekämpningen.

Utredaren ska därför

- analysera hur PNR-direktivet förhåller sig till regleringen i 9 kap. 3 a § utlänningslagen och lagen om passagerarregister,
- föreslå hur systemet för flygpassageraruppgifter ska möjliggöra hantering av både PNR-uppgifter och API-uppgifter, och

- föreslå de författningsändringar som bedöms nödvändiga.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för de behöriga brottsbekämpande myndigheterna och konsekvenserna i övrigt av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska även bedöma vilka konsekvenser förslagen får för enskilda.

Samråd och redovisning av uppdraget

Utredaren ska inhämta synpunkter från berörda myndigheter, särskilt Polismyndigheten, Säkerhetspolisen, Tullverket, Ekobrottsmyndigheten, Transportstyrelsen, Säkerhets- och integritetsskyddsnämnden och Datainspektionen. I lämplig omfattning ska utredaren även inhämta synpunkter från berörda flygbolag, andra ekonomiska aktörer och branschorganisationer. Utredaren ska vidare hålla sig informerad om arbetet med att genomföra det nya dataskyddsdirektivet och Polismyndighetens arbete med att genomföra PNR-direktivet i dess tekniska delar.

Uppdraget ska redovisas senast den 31 maj 2017.

(Justitiedepartementet)

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/681**av den 27 april 2016****om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet**

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 82.1 d och 87.2 a,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ⁽²⁾, och

av följande skäl:

- (1) Den 6 november 2007 antog kommissionen ett förslag till rådets rambeslut om användning av passageraruppgiftssamlingar (PNR-uppgifter) i brottsbekämpningssyfte. Ikraftträdandet av Lissabonfördraget den 1 december 2009 ledde dock till att kommissionens förslag, som ännu inte hade antagits av rådet, blev inaktuellt.
- (2) I *Stockholmsprogrammet – ett öppet och säkert Europa i medborgarnas tjänst och för deras skydd* ⁽³⁾ uppmanades kommissionen att lägga fram ett förslag om användning av PNR-uppgifter för att förebygga, förhindra, upptäcka, utreda och lagföra terrorism och grov brottslighet.
- (3) I sitt meddelande av den 21 september 2010 om en övergripande strategi när det gäller överföring av passageraruppgiftssamlingar (PNR-uppgifter) till tredjeländer skisserade kommissionen ett antal huvuddrag i en ny unionsstrategi på detta område.
- (4) I rådets direktiv 2004/82/EG ⁽⁴⁾ regleras transportörers översändande av förhandsinformation om passagerare (API-uppgifter) till behöriga nationella myndigheter i syfte att förbättra gränskontrollerna och bekämpa olaglig invandring.
- (5) Målen för detta direktiv är bland annat att trygga säkerheten, skydda personers liv och säkerhet och att inrätta en rättslig ram för skydd av PNR-uppgifter vid behöriga myndigheters behandling av dessa.
- (6) En effektiv användning av PNR-uppgifter, exempelvis genom att jämföra PNR-uppgifter med uppgifter i olika databaser över eftersökta personer och föremål, är nödvändig för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten, för att samla in bevisning och i förekommande fall för att hitta medbrottslingar och avslöja kriminella nätverk.
- (7) Bedömningen av PNR-uppgifter gör det möjligt att identifiera personer som tidigare inte har varit misstänkta för delaktighet i terroristbrott eller grov brottslighet innan en sådan bedömning görs och som bör undersökas

⁽¹⁾ EUT C 218, 23.7.2011, s. 107.

⁽²⁾ Europaparlamentets ståndpunkt av den 14 april 2016 (ännu ej offentliggjord i EUT) och rådets beslut av den 21 april 2016.

⁽³⁾ EUT C 115, 4.5.2010, s. 1.

⁽⁴⁾ Rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare (EUT L 261, 6.8.2004, s. 24).

närmare av de behöriga myndigheterna. Genom att använda PNR-uppgifter är det möjligt att möta hotet från terroristbrott och grov brottslighet från en annan utgångspunkt än vid behandling av andra kategorier av personuppgifter. För att säkerställa att behandlingen av PNR-uppgifter begränsas till vad som är nödvändigt, bör emellertid utformning och tillämpning av bedömningskriterierna begränsas till att endast omfatta terroristbrott och grov brottslighet för vilka användningen av sådana kriterier är relevant. Bedömningskriterierna bör dessutom fastställas på ett sätt som gör att så få oskyldiga människor som möjligt identifieras felaktigt av systemet.

- (8) Redan nu samlar lufttrafikföretagen in och behandlar PNR-uppgifter om sina passagerare för sina egna kommersiella syften. Detta direktiv bör inte medföra någon skyldighet för lufttrafikföretagen att samla in eller lagra några ytterligare uppgifter om passagerare eller någon skyldighet för passagerare att tillhandahålla några uppgifter utöver dem som redan tillhandahålls lufttrafikföretagen.
- (9) Vissa lufttrafikföretag lagrar insamlade API-uppgifter som en del av PNR-uppgifterna, andra gör det inte. Att använda PNR-uppgifter tillsammans med API-uppgifter tillför ett mervärde, genom att det hjälper medlemsstaterna att kontrollera en individs identitet, vilket ökar PNR-uppgifternas betydelse för brottsbekämpningen och minimerar risken för att man kontrollerar och utreder oskyldiga människor. Därför är det viktigt att säkerställa att lufttrafikföretag, om de samlar in API-uppgifter, överför dessa, oavsett om de lagrar API-uppgifter med hjälp av andra tekniska metoder än andra PNR-uppgifter.
- (10) För att det ska gå att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet är det av största vikt att alla medlemsstater inför bestämmelser om skyldigheter för lufttrafikföretag som tillhandahåller flygförbindelser utanför EU att överföra de PNR-uppgifter, inklusive API-uppgifter, som de samlar in. Medlemsstaterna bör även ha möjlighet att utsträcka denna skyldighet till lufttrafikföretag som tillhandahåller flygförbindelser inom EU. De bestämmelserna bör inte påverka tillämpningen av direktiv 2004/82/EG.
- (11) Behandlingen av personuppgifter bör stå i proportion till de särskilda säkerhetsmål som detta direktiv syftar till att uppfylla.
- (12) Den definition av terroristbrott som tillämpas i detta direktiv bör vara densamma som i rådets rambeslut 2002/475/RIF⁽¹⁾. Definitionen av allvarlig brottslighet bör omfatta de brottskategorier som förtecknas i bilaga II till detta direktiv.
- (13) PNR-uppgifter bör överföras till en särskild enhet för passagerarinformation i den berörda medlemsstaten, för att säkerställa klarhet om vad som gäller och för att minska kostnaderna för lufttrafikföretagen. Enheten för passagerarinformation får ha olika avdelningar i en medlemsstat och medlemsstater får också gemensamt inrätta en enhet för passagerarinformation. Medlemsstaterna bör utbyta information med varandra genom relevanta nät för informationsutbyte för att underlätta informationsutbyte och säkerställa driftskompatibilitet.
- (14) Medlemsstaterna bör betala kostnaderna för användning, lagring och utbyte av PNR-uppgifter.
- (15) En förteckning över PNR-uppgifter som ska vidarebefordras till en enhet för passagerarinformation bör utformas i syfte att återspegla de offentliga myndigheternas legitima krav på att kunna förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten i unionen, samtidigt som grundläggande rättigheter skyddas, särskilt rätten till skydd av privatlivet och rätten till skydd av personuppgifter. I detta syfte bör höga standarder tillämpas, i enlighet med Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*), konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (nedan kallad *konvention nr 108*) och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad *Europakonventionen*). En sådan förteckning bör inte grundas på en persons ras eller etniska ursprung, religion eller övertygelse, politiska eller annan åskådning, medlemskap i fackförening, hälsotillstånd, sexualliv eller sexuella läggning. PNR-uppgifterna bör endast omfatta sådan information om passagerarens bokning och resrutt som gör det möjligt för de behöriga myndigheterna att identifiera flygpasagerare som utgör ett hot mot den inre säkerheten.
- (16) Det finns för närvarande två möjliga metoder för överföring av uppgifter: direktåtkomstmetoden (*pull*-metoden), som innebär att de behöriga myndigheterna i den medlemsstat som begär PNR-uppgifterna kan få direkt åtkomst till lufttrafikföretagets bokningssystem för att hämta en kopia av de PNR-uppgifter som behövs, och sändmetoden (*push*-metoden), som innebär att lufttrafikföretagen överför de begärda PNR-uppgifterna till den myndighet som har begärt dem, vilket således gör det möjligt för lufttrafikföretagen att behålla kontrollen över vilka uppgifter som tillhandahålls. Sändmetoden anses ge en bättre skyddsnivå för uppgifterna och bör vara obligatorisk för alla lufttrafikföretag.

(¹) Rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3).

- (17) Kommissionen stöder Internationella civila luftfartsorganisationens (Icao) riktlinjer om PNR. Dessa riktlinjer bör därför fungera som underlag vid antagandet av understödda dataformat för överföring av PNR-uppgifter från lufttrafikföretag till medlemsstater. För att säkerställa enhetliga villkor för genomförandet av understödda dataformat och av relevanta protokoll som gäller för överföring av uppgifter från lufttrafikföretag bör kommissionen ges genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ⁽¹⁾.
- (18) Medlemsstaterna bör vidta alla nödvändiga åtgärder för att göra det möjligt för lufttrafikföretagen att uppfylla sina skyldigheter enligt detta direktiv. Medlemsstaterna bör fastställa effektiva, proportionella och avskräckande sanktioner, även ekonomiska sanktioner, för de lufttrafikföretag som inte uppfyller sina skyldigheter med avseende på överföring av PNR-uppgifter.
- (19) Varje medlemsstat bör ansvara för att bedöma potentiella hot från terroristbrott och grov brottslighet.
- (20) Med fullt beaktande av rätten till skydd av personuppgifter och rätten till icke-diskriminering, bör inga beslut som har negativa rättsliga verkningar för en person eller som på ett väsentligt sätt påverkar denna person fattas enbart på grund av den automatiska behandlingen av PNR-uppgifter. Med hänsyn till artiklarna 8 och 21 i stadgan bör sådana beslut inte diskriminera på grund av en persons kön, ras, hudfärg, etniska eller sociala ursprung, genetiska särdrag, språk, religion eller övertygelse, politiska eller annan åskådning, tillhörighet till en nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuella läggning. Kommissionen bör även beakta dessa principer när den ser över tillämpningen av detta direktiv.
- (21) Medlemsstaterna bör under inga omständigheter använda resultatet av behandlingen av PNR-uppgifter för att kringgå sina internationella skyldigheter enligt konventionen av den 28 juli 1951 angående flyktingars rättsliga ställning i dess lydelse enligt protokollet av den 31 januari 1967 eller för att förvägra asylsökande säkra, ändamålsenliga och lagliga möjligheter att ta sig till unionens territorium för att utöva sin rätt till internationellt skydd.
- (22) Med fullt beaktande av principerna i aktuell relevant rättspraxis från Europeiska unionens domstol bör tillämpningen av detta direktiv säkerställa full respekt för de grundläggande rättigheterna, rätten till skydd av privatlivet och proportionalitetsprincipen. Den bör även till fullo vara förenlig med vad som är nödvändigt och proportionellt för att de mål av allmänt intresse som erkänts av unionen ska uppnås och med behovet att skydda andras rättigheter och friheter i kampen mot terroristbrott och grov brottslighet. Tillämpningen av detta direktiv bör vara vederbörligen motiverad och nödvändiga skyddsåtgärder bör vidtas för att säkerställa att all lagring, analys, överföring eller användning av PNR-uppgifter sker på laglig grund.
- (23) Medlemsstaterna bör utbyta PNR-uppgifter som de har mottagit med varandra och med Europol, om detta bedöms vara nödvändigt för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Enheterna för passagerarinformation bör om lämpligt och utan dröjsmål översända resultatet av behandlingen av PNR-uppgifter till enheterna för passagerarinformation i andra medlemsstater för ytterligare utredning. Bestämmelserna i detta direktiv bör inte påverka andra unionsinstrument om informationsutbyte mellan polismyndigheter och andra brottsbekämpande myndigheter och rättsliga myndigheter, till exempel rådets beslut 2009/371/RIF ⁽²⁾ och rådets rambeslut 2006/960/RIF ⁽³⁾. Ett sådant utbyte av PNR-uppgifter bör omfattas av bestämmelserna om polissamarbete och rättsligt samarbete och bör inte undergräva den höga skyddsnivå för både privatlivet och personuppgifter som stadgan, konvention nr 108 och Europakonventionen föreskriver.
- (24) Ett säkert informationsutbyte om PNR-uppgifter mellan medlemsstaterna bör säkerställas genom någon av de befintliga kanalerna för samarbete mellan medlemsstaternas behöriga myndigheter och särskilt med Europol genom Europols nätapplikation för säkert informationsutbyte (Siena).

⁽¹⁾ Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

⁽²⁾ Rådets beslut 2009/371/RIF av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol) (EUT L 121, 15.5.2009, s. 37).

⁽³⁾ Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (EUT L 386, 29.12.2006, s. 89).

- (25) Lagringstiden för PNR-uppgifter bör vara tillräckligt lång och stå i proportion till ändamålen, nämligen att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Med tanke på PNR-uppgifternas art och användningsområden bör det vara tillåtet att lagra dem tillräckligt länge för att de ska kunna användas i samband med analyser och utredningar. För att undvika oproportionell användning bör PNR-uppgifterna efter den inledande lagringsperioden avidentifieras genom maskering av uppgifter. För att säkerställa högsta möjliga nivå av dataskydd bör åtkomst till fullständiga PNR-uppgifter, vilka gör det möjligt att direkt identifiera den registrerade, endast beviljas under mycket strikta och begränsade villkor efter den inledande perioden.
- (26) Om specifika PNR-uppgifter har överförts till en behörig myndighet för att användas inom ramen för särskilda brottsutredningar eller lagföringsåtgärder, bör den behöriga myndighetens lagring av dessa uppgifter regleras av nationell rätt, oavsett vilken lagringstid för uppgifter som anges i detta direktiv.
- (27) Den behandling av PNR-uppgifter som i medlemsstaterna utförs av enheten för passagerarinformation och de behöriga myndigheterna bör omfattas av en standard för skydd av personuppgifter enligt nationell rätt i linje med rådets rambeslut 2008/977/RIF⁽¹⁾ och de särskilda krav på dataskydd som fastställs i detta direktiv. Hänvisningar till rambeslut 2008/977/RIF bör ses som hänvisningar till gällande lagstiftning och till lagstiftning som kommer att ersätta denna.
- (28) Med hänsyn till rätten till skydd för personuppgifter är det viktigt att de registrerades rättigheter vid behandling av PNR-uppgifter som rör dem, till exempel rätt till åtkomst, rättelse, radering och begränsning samt rätt till ersättning och tillgång till rättsmedel överensstämmer med både rambeslut 2008/977/RIF och den höga skyddsnivå som stadgan och Europakonventionen föreskriver.
- (29) Med hänsyn till passagerares rätt att bli informerade om behandlingen av personuppgifter bör medlemsstaterna se till att passagerare förses med korrekt, lättåtkomlig och lättbegriplig information om insamlingen av PNR-uppgifter och överföringen av dessa uppgifter till enheten för passagerarinformation samt om sina rättigheter i egenskap av registrerade.
- (30) Detta direktiv påverkar inte tillämpningen av unionsrätt och nationell rätt om principen om allmänhetens tillgång till officiella handlingar.
- (31) Överföring av PNR-uppgifter från medlemsstater till tredjeländer bör endast vara tillåten i enskilda fall och i full överensstämmelse med de bestämmelser som medlemsstaterna fastställt i enlighet med rambeslut 2008/977/RIF. För att säkerställa skyddet av personuppgifter bör sådana överföringar omfattas av kompletterande krav knutna till syftet med överföringen. De bör också omfattas av principerna om nödvändighet och proportionalitet och av den höga skyddsnivå som stadgan och Europakonventionen föreskriver.
- (32) Den nationella tillsynsmyndighet som har inrättats enligt rådets rambeslut 2008/977/RIF bör även ansvara för att meddela riktlinjer för och utöva tillsyn över tillämpningen av de bestämmelser som medlemsstaterna antar i enlighet med detta direktiv.
- (33) Detta direktiv påverkar inte medlemsstaternas möjligheter att i enlighet med nationell rätt tillhandahålla ett system för insamling och behandling av PNR-uppgifter från ekonomiska aktörer som inte är transportörer, t.ex. resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, för vilka de samlar in och behandlar PNR-uppgifter, eller från andra transportföretag än de som anges i detta direktiv, förutsatt att sådan nationell rätt är förenlig med unionsrätten.
- (34) Detta direktiv påverkar inte gällande unionsbestämmelser om formerna för utförande av gränskontroller eller unionsbestämmelser om in- och utresa från unionens territorium.
- (35) På grund av rättsliga och tekniska skillnader mellan olika nationella bestämmelser om behandling av personuppgifter, däribland PNR-uppgifter, möts lufttrafikföretagen av olika krav på vilken typ av information som ska översändas och vilka villkor som gäller för översändandet av denna information till de behöriga nationella

⁽¹⁾ Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60).

myndigheterna. Dessa skillnader kan vara till skada för ett effektivt samarbete mellan de behöriga nationella myndigheterna för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Det är därför nödvändigt att på unionsnivå inrätta en gemensam rättslig ram för överföring och behandling av PNR-uppgifter.

- (36) Detta direktiv står i överensstämmelse med de grundläggande rättigheterna och principerna i stadgan, särskilt rätten till skydd av personuppgifter, rätten till respekt för privatlivet och rätten till icke-diskriminering, som skyddas genom artiklarna 8, 7 och 21 i stadgan, och bör därför genomföras i enlighet med dessa. Detta direktiv överensstämmer med principerna om dataskydd och dess bestämmelser är förenliga med rambeslut 2008/977/RIF. För att detta direktiv inte ska inkräkta på proportionalitetsprincipen kommer dess bestämmelser om dataskydd i vissa fall att vara strängare än motsvarande bestämmelser i rambeslut 2008/977/RIF.
- (37) Tillämpningsområdet för detta direktiv är så begränsat som möjligt eftersom det föreskriver att PNR-uppgifter får lagras i enheter för passagerarinformation i högst fem år, varefter de bör raderas, det föreskriver att uppgifterna bör avidentifieras genom maskering av uppgifter efter en inledande period av sex månader, och det förbjuder insamling och användning av känsliga uppgifter. För att säkerställa effektivitet och en hög nivå av dataskydd, bör medlemsstaterna se till att en oberoende nationell tillsynsmyndighet och särskilt ett dataskyddsbud ges ansvaret för att meddela riktlinjer för och övervaka på vilket sätt PNR-uppgifter behandlas. All behandling av PNR-uppgifter bör loggas eller dokumenteras i syfte att kontrollera att den är laglig, att möjliggöra självövervakning och att säkerställa uppgifternas integritet och en säker behandling. Medlemsstaterna bör också se till att passagerarna klart och tydligt informeras om insamlingen av PNR-uppgifter och om sina rättigheter.
- (38) Eftersom målen för detta direktiv, nämligen lufttrafikföretags överföring av PNR-uppgifter och behandling av dessa uppgifter för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (39) I enlighet med artikel 3 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, har Förenade kungariket och Irland meddelat att de önskar delta i antagandet och tillämpningen av detta direktiv.
- (40) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, deltar Danmark inte i antagandet av detta direktiv, som inte är bindande för eller tillämpligt på Danmark.
- (41) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ⁽¹⁾ och avgav ett yttrande den 25 mars 2011.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte och tillämpningsområde

1. Detta direktiv innehåller bestämmelser om
 - a) lufttrafikföretags överföring av passageraruppgiftssamlingar (PNR-uppgifter) om passagerare på flygningar utanför EU,
 - b) behandlingen av de uppgifter som avses i led a, inbegripet medlemsstaternas insamling, användning, lagring och inbördes utbyte av dessa uppgifter.

⁽¹⁾ Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

2. PNR-uppgifter som samlas in i enlighet med detta direktiv får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet i enlighet med artikel 6.2 a, b och c.

Artikel 2

Detta direktivs tillämpning på flygningar inom EU

1. Om en medlemsstat beslutar att tillämpa detta direktiv på flygningar inom EU, ska denna medlemsstat skriftligen meddela kommissionen detta. En medlemsstat får när som helst lämna eller återkalla ett sådant meddelande. Kommissionen ska offentliggöra detta meddelande, och en eventuell återkallelse av det, i *Europeiska unionens officiella tidning*.
2. När ett meddelande som avses i punkt 1 lämnas, ska alla bestämmelser i detta direktiv gälla för flygningar inom EU som om de vore flygningar utanför EU och för PNR-uppgifter från flygningar inom EU som om de vore PNR-uppgifter från flygningar utanför EU.
3. En medlemsstat får besluta att endast tillämpa detta direktiv på valda flygningar inom EU. När medlemsstaten fattar ett sådant beslut, ska den välja de flygningar som den anser vara nödvändiga för att efterfölja målen för detta direktiv. Medlemsstaten får när som helst besluta att ändra urvalet av flygningar inom EU.

Artikel 3

Definitioner

I detta direktiv avses med

1. *lufttrafikföretag*: ett lufttrafikföretag med giltig operativ licens eller motsvarande som ger rätt att bedriva passagerarflygtrafik,
2. *flygning utanför EU*: varje reguljär eller icke-reguljär flygning som utförs av ett lufttrafikföretag, med avgång från ett tredjeland och planerad landning på en medlemsstats territorium eller flygning från en medlemsstats territorium med planerad landning i ett tredjeland, i båda fallen inklusive eventuella mellanlandningar på territorier i medlemsstater eller tredjeländer,
3. *flygning inom EU*: varje reguljär eller icke-reguljär flygning som utförs av ett lufttrafikföretag, med avgång från en medlemsstats territorium och planerad landning på en eller flera andra medlemsstaters territorium, utan eventuella mellanlandningar på tredjeländers territorier,
4. *passagerare*: alla personer, inbegripet personer i transfer eller transit förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan med lufttrafikföretagets godkännande, vilket godkännande framgår av att denna person står med på passagerarförteckningen,
5. *passageraruppgiftssamling* eller *PNR-uppgifter*: en sammanställning av för resan nödvändiga uppgifter om varje enskild passagerare som gör det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen för varje resa som bokas av en person eller för en persons räkning, oavsett om uppgifterna finns i reservationssystemet, det avgångskontrollsystem som används för att checka in passagerare på flygningar eller likvärdiga system med motsvarande uppgift,
6. *reservationssystem*: lufttrafikföretagets interna system, där PNR-uppgifter samlas för hantering av reservationer,
7. *sändmetod*: den metod varigenom lufttrafikföretagen överför de PNR-uppgifter som förtecknas i bilaga I till databasen vid den myndighet som begärt dem,

8. *terroristbrott*: de brott enligt nationell rätt som avses i artiklarna 1–4 i rambeslut 2002/475/RIF,
9. *grov brottslighet*: brott som förtecknas i bilaga II vilka bestraffas med fängelse eller annan frihetsberövande åtgärd i minst tre år enligt en medlemsstats nationella rätt,
10. *avidentifiering genom maskering av uppgifter*: att göra de uppgifter som kan användas för att omedelbart identifiera den registrerade osynliga för en användare.

KAPITEL II

Medlemsstaternas skyldigheter

Artikel 4

Enhet för passagerarinformation

1. Varje medlemsstat ska inrätta eller utse en myndighet med behörighet att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet eller en avdelning inom en sådan myndighet, vilken ska fungera som medlemsstatens enhet för passagerarinformation.
2. Enheten för passagerarinformation ska ansvara för att
 - a) samla in PNR-uppgifter från lufttrafikföretagen, lagra och behandla dessa uppgifter och överföra dessa uppgifter eller resultatet av behandlingen av dem till de behöriga myndigheter som avses i artikel 7,
 - b) utbyta både PNR-uppgifter och resultatet av behandlingen av dessa uppgifter med andra medlemsstaters enheter för passagerarinformation och med Europol i enlighet med artiklarna 9 och 10.
3. Personal vid enheten för passagerarinformation kan utgöras av tjänstemän som avdelats från behöriga myndigheter. Medlemsstaterna ska ge enheterna för passagerarinformation tillräckliga resurser för att de ska kunna utföra sina uppgifter.
4. Två eller flera medlemsstater (nedan kallade *de deltagande medlemsstaterna*) får inrätta eller utse en och samma myndighet till sin gemensamma enhet för passagerarinformation. En sådan enhet för passagerarinformation ska inrättas i en av de deltagande medlemsstaterna och fungera som nationell enhet för passagerarinformation för alla deltagande medlemsstater. De deltagande medlemsstaterna ska tillsammans enas om närmare bestämmelser för driften av enheten för passagerarinformation utan att avvika från kraven i detta direktiv.
5. Varje medlemsstat ska inom en månad från inrättandet eller utseendet av sin enhet för passagerarinformation meddela kommissionen detta och får när som helst ändra detta meddelande. Kommissionen ska offentliggöra meddelandet och eventuella ändringar därav i *Europeiska unionens officiella tidning*.

Artikel 5

Dataskyddsombud vid enheten för passagerarinformation

1. Enheten för passagerarinformation ska utse ett dataskyddsombud, som ska ansvara för övervakningen av behandlingen av PNR-uppgifter och för genomförandet av relevanta skyddsåtgärder.
2. Medlemsstaterna ska förse dataskyddsombuden med de resurser som de behöver för att utföra sina uppgifter i enlighet med denna artikel på ett effektivt och oberoende sätt.
3. Medlemsstaterna ska se till att en registrerad har rätt att kontakta dataskyddsombudet, i egenskap av enda kontaktpunkt, i alla frågor som rör behandlingen av den registrerades PNR-uppgifter.

Artikel 6

Behandling av PNR-uppgifter

1. PNR-uppgifter som överförs av lufttrafikföretag ska samlas in av den berörda medlemsstatens enhet för passagerarinformation i enlighet med artikel 8. Om PNR-uppgifter som överförs av lufttrafikföretag omfattar andra uppgifter än dem som anges i bilaga I, ska enheten för passagerarinformation omedelbart och slutgiltigt radera dessa vid mottagandet.
2. Enheten för passagerarinformation ska enbart behandla PNR-uppgifterna för följande ändamål:
 - a) Göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från den berörda medlemsstaten, för att identifiera personer som de behöriga myndigheterna enligt artikel 7 och i förekommande fall Europol enligt artikel 10 behöver utreda ytterligare, på grund av att dessa personer kan vara inblandade i terroristbrott eller grov brottslighet.
 - b) I enskilda fall, besvara en vederbörligen motiverad förfrågan som bygger på tillräckliga skäl från de behöriga myndigheterna om att tillhandahålla och behandla PNR-uppgifter i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet och tillhandahålla de behöriga myndigheterna eller, när så är lämpligt, Europol resultaten av sådan behandling.
 - c) Analysera PNR-uppgifter för att uppdatera och skapa nya kriterier som ska användas vid de bedömningar som genomförs enligt punkt 3 b, i syfte att identifiera personer som kan vara delaktiga i terroristbrott eller grov brottslighet.
3. När enheten för passagerarinformation utför den bedömning som avses i punkt 2 a får den:
 - a) Jämföra PNR-uppgifter med uppgifter i databaser som är relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, inklusive databaser över personer eller föremål som är eftersökta eller finns uppförda på spärlista, i enlighet med unionsbestämmelser eller internationella eller nationella bestämmelser som är tillämpliga på sådana databaser, eller
 - b) behandla PNR-uppgifter i enlighet med på förhand fastställda kriterier.
4. En bedömning av passagerare före planerad ankomst till eller avresa från medlemsstaten som görs enligt punkt 3 b i enlighet med på förhand fastställda kriterier ska utföras på ett icke-diskriminerande sätt. Dessa på förhand fastställda kriterier måste vara riktade, proportionella och specifika. Medlemsstaterna ska se till att kriterierna fastställs och regelbundet ses över av enheterna för passagerarinformation i samarbete med de behöriga myndigheter som avses i artikel 7. Dessa på förhand fastställda kriterier får under inga omständigheter vara baserade på en persons ras, etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning.
5. Medlemsstaterna ska se till att eventuella träffar i samband med automatisk behandling av PNR-uppgifter enligt punkt 2 a granskas individuellt med icke-automatiska metoder, för att verifiera huruvida den behöriga myndighet som avses i artikel 7 behöver vidta åtgärder enligt nationell rätt.
6. Enheten för passagerarinformation i en medlemsstat ska översända PNR-uppgifterna beträffande personer som har identifierats i enlighet med punkt 2 a eller resultaten av behandlingen av dessa uppgifter till de behöriga myndigheter som avses i artikel 7 i samma medlemsstat för vidare granskning. Sådana överföringar får endast göras i enskilda fall och, vid automatisk behandling av PNR-uppgifter, efter individuell icke-automatisk granskning.
7. Medlemsstaterna ska se till att dataskyddsombudet har åtkomst till alla uppgifter som enheten för passagerarinformation behandlar. Om dataskyddsombudet anser att behandlingen av vissa uppgifter inte har varit lagenlig, ska dataskyddsombudet hänskjuta ärendet till den nationella tillsynsmyndigheten.
8. Lagring, behandling och analys av PNR-uppgifter vid enheten för passagerarinformation ska uteslutande utföras på en eller flera säkra platser på en medlemsstats territorium.

9. Konsekvenserna av de bedömningar av passagerare som avses i punkt 2 a i denna artikel får inte äventyra rätten för personer som åtnjuter fri rörlighet enligt unionsrätten att resa in på den berörda medlemsstatens territorium i enlighet med Europaparlamentets och rådets direktiv 2004/38/EG⁽¹⁾. När bedömningarna sker i samband med flygningar inom EU mellan medlemsstater för vilka Europaparlamentets och rådets förordning (EG) nr 562/2006⁽²⁾ är tillämplig, ska konsekvenserna av sådana bedömningar vara förenliga med den förordningen.

Artikel 7

Behöriga myndigheter

1. Varje medlemsstat ska fastställa en förteckning över de behöriga myndigheter som har befogenhet att begära eller motta PNR-uppgifter eller resultat av behandlingen av dessa uppgifter från enheten för passagerarinformation för vidare granskning av informationen eller för att vidta lämpliga åtgärder för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet.
2. De myndigheter som avses i punkt 1 ska vara myndigheter som är behöriga att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet.
3. Med avseende på tillämpningen av artikel 9.3 ska varje medlemsstat senast den 25 maj 2017 meddela kommissionen förteckningen över sina behöriga myndigheter och får när som helst ändra sitt meddelande. Kommissionen ska offentliggöra meddelandet och eventuella ändringar därav i *Europeiska unionens officiella tidning*.
4. PNR-uppgifter och resultaten av behandling av dessa uppgifter som mottas av enheten för passagerarinformation får endast vidarebehandlas av de behöriga myndigheterna i medlemsstaterna, om det specifika syftet är att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet.
5. Punkt 4 ska inte påverka de brottsbekämpande eller rättsliga myndigheternas befogenheter på nationell nivå, om andra brott eller indikationer på sådana upptäcks i samband med brottsbekämpande insatser som görs till följd av sådan behandling av PNR-uppgifter.
6. De behöriga myndigheterna får inte fatta några beslut som har negativa rättsliga konsekvenser för en person eller på annat sätt allvarligt påverkar en person endast på grund av den automatiska behandlingen av PNR-uppgifter. Besluten får inte grunda sig på en persons ras eller etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning.

Artikel 8

Luftrafikföretagens skyldigheter vad gäller överföring av uppgifter

1. Medlemsstaterna ska anta de åtgärder som är nödvändiga för att se till att luftrafikföretag genom sändmetoden överför de PNR-uppgifter som förtecknas i bilaga I, förutsatt att de redan samlar in sådana uppgifter som en del av sin normala affärsverksamhet, till databasen hos enheten för passagerarinformation i den medlemsstat på vars territorium flygningen kommer att ankomma eller från det territorium varifrån flygningen kommer att avgå. Om flygningens linjebeteckning delas med ett eller flera andra luftrafikföretag, ska det företag som utför flygningen ha skyldighet att överföra PNR-uppgifter om samtliga passagerare ombord. Om en flygning utanför EU omfattar en eller flera mellanlandningar på medlemsstaternas flygplatser, ska luftrafikföretagen överföra PNR-uppgifterna för alla passagerare till enheterna för passagerarinformation i alla berörda medlemsstater. Detta gäller även om en flygning inom EU innebär en eller flera mellanlandningar på olika medlemsstaters flygplatser, men endast i fråga om medlemsstater som samlar in PNR-uppgifter från flygningar inom EU.

⁽¹⁾ Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier och om ändring av förordning (EEG) nr 1612/68 och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG (EUT L 158, 30.4.2004, s. 77).

⁽²⁾ Europaparlamentets och rådets förordning (EG) nr 562/2006 av den 15 mars 2006 om en gemenskapskodex om gränspassage för personer (kodex om Schengengränserna) (EUT L 105, 13.4.2006, s. 1).

2. Om lufttrafikföretagen har samlat in sådan förhandsinformation om passagerare (API-uppgifter) som förtecknas i punkt 18 i bilaga I men inte lagrar denna information med hjälp av samma tekniska metoder som för andra PNR-uppgifter, ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att lufttrafikföretagen genom sändmetoden även överför dessa uppgifter till enheten för passagerarinformation i de medlemsstater som avses i punkt 1. Vid sådan överföring ska alla bestämmelser i detta direktiv vara tillämpliga på dessa API-uppgifter.
3. Lufttrafikföretagen ska överföra PNR-uppgifter elektroniskt med användning av de gemensamma protokoll och understödda dataformat som ska antas i enlighet med det granskningsförfarande som avses i artikel 17.2 eller, vid eventuella tekniska problem, på något annat sätt som säkerställer ett lämpligt dataskydd
 - a) 24–48 timmar före flygningens planerade avgång, och
 - b) omedelbart efter det att gatens dörrar stängts, det vill säga när passagerarna har stigit ombord på planet inför avgång och passagerare inte längre tillåts stiga ombord eller stiga av.
4. Medlemsstaterna ska tillåta lufttrafikföretag att begränsa den överföring som avses i punkt 3 b till uppdateringar av sådana överföringar som avses i punkt 3 a.
5. I situationer där åtkomst till PNR-uppgifter är nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet, ska lufttrafikföretag efter en bedömning i det enskilda fallet på begäran av en enhet för passagerarinformation, i enlighet med nationell rätt, överföra PNR-uppgifter vid andra tidpunkter än de som anges i punkt 3.

Artikel 9

Utbyte av information mellan medlemsstaterna

1. När personer identifieras av en enhet för passagerarinformation i enlighet med artikel 6.2, ska medlemsstaterna se till att enheten översänder alla relevanta och nödvändiga PNR-uppgifter eller resultaten av en eventuell behandling av dessa uppgifter till motsvarande enheter i de andra medlemsstaterna. Enheterna för passagerarinformation i de mottagande medlemsstaterna ska översända den mottagna informationen till sina behöriga myndigheter i enlighet med artikel 6.6.
2. Enheten för passagerarinformation i en medlemsstat ska ha rätt att vid behov begära att en enhet för passagerarinformation i en annan medlemsstat tillhandahåller PNR-uppgifter som lagras i den senares databas och ännu inte har avidentifierats genom maskering av uppgifter i enlighet med artikel 12.2 och vid behov även resultaten av en eventuell behandling av dessa uppgifter, om en sådan redan har utförts i enlighet med artikel 6.2 a. En sådan begäran ska vederbörligen motiveras. Den får avse en viss uppgift eller en kombination av sådana uppgifter, beroende på vilken information den begärande enheten för passagerarinformation anser vara nödvändig i ett särskilt fall för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet. Enheterna för passagerarinformation ska tillhandahålla den begärda informationen så snart som möjligt. Om de begärda uppgifterna har avidentifierats genom maskering av uppgifter i enlighet med artikel 12.2, ska enheten för passagerarinformation endast tillhandahålla fullständiga PNR-uppgifter, om det rimligen kan antas vara nödvändigt för de ändamål som anges i artikel 6.2 b och detta endast efter tillstånd från en behörig myndighet som avses i artikel 12.3 b.
3. Endast i nödfall och enligt de villkor som fastställts i punkt 2 får en medlemsstats behöriga myndigheter vända sig direkt till enheten för passagerarinformation i en annan medlemsstat med en begäran om utlämnande av PNR-uppgifter som finns lagrade i den enhetens databas. Begäran från de behöriga myndigheterna ska motiveras. En kopia av begäran ska alltid skickas till enheten för passagerarinformation i den begärande medlemsstaten. I alla andra fall ska de behöriga myndigheterna översända sina framställningar via enheten för passagerarinformation i den egna medlemsstaten.
4. Om åtkomst till PNR-uppgifter är nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet, ska enheten för passagerarinformation i en medlemsstat i undantagsfall ha rätt att begära att enheten för passagerarinformation i en annan medlemsstat införskaffar PNR-uppgifter i enlighet med artikel 8.5 och vidarebefordrar dessa till den begärande enheten för passagerarinformation.
5. Informationsutbyte enligt denna artikel får göras via alla befintliga kanaler för samarbete mellan medlemsstaternas behöriga myndigheter. Det språk som används i samband med begäran och informationsutbytet ska vara det som gäller

för den kanal som används. Medlemsstaterna ska i samband med att de lämnar meddelanden i enlighet med artikel 4.5 även meddela kommissionen uppgifter om de kontaktpunkter till vilka framställningar kan sändas i nödfall. Kommissionen ska underrätta medlemsstaterna om dessa uppgifter.

Artikel 10

Villkor för Europols åtkomst till PNR-uppgifter

1. Europol ska inom ramen för sina befogenheter och för fullgörandet av sina arbetsuppgifter ha rätt att begära PNR-uppgifter eller resultatet av behandlingen av dessa uppgifter från enheterna för passagerarinformation i medlemsstaterna.
2. Europol får från fall till fall via Europols nationella enhet lämna in en elektronisk, vederbörligen motiverad begäran till enheten för passagerarinformation i en medlemsstat om översändande av specifika PNR-uppgifter eller resultaten av behandlingen av dessa uppgifter. Europol får lämna in en sådan begäran när detta är absolut nödvändigt för att stödja och stärka medlemsstaternas åtgärder för att förebygga, förhindra, upptäcka eller utreda ett specifikt terroristbrott eller grovt brott i den mån brottet i fråga omfattas av Europols behörighet enligt beslut 2009/371/RIF. I den motiverade begäran ska rimliga skäl anges till varför Europol anser att översändandet av PNR-uppgifterna eller resultaten av behandlingen av PNR-uppgifter väsentligt kommer att bidra till att brottet i fråga förebyggs, upptäcks eller utreds.
3. Europol ska informera det dataskyddsombud som utsetts i enlighet med artikel 28 i beslut 2009/371/RIF om varje informationsutbyte enligt den här artikeln.
4. Informationsutbyte enligt denna artikel ska äga rum via Siena och i enlighet med beslut 2009/371/RIF. Det språk som används för framställningen och informationsutbytet ska vara det som gäller för Siena.

Artikel 11

Överföring av uppgifter till tredjeländer

1. En medlemsstat får överföra PNR-uppgifter och resultaten av behandling av sådana uppgifter som lagras av enheten för passagerarinformation i enlighet med artikel 12 till ett tredjeland efter bedömning i det enskilda fallet, endast under förutsättning att
 - a) de villkor som fastställs i artikel 13 i rambeslut 2008/977/RIF är uppfyllda,
 - b) överföringen är nödvändig för detta direktivs syften enligt artikel 1.2,
 - c) det berörda tredjelandet godtar att överföra uppgifterna till ett annat tredjeland endast om det är strikt nödvändigt för detta direktivs ändamål enligt artikel 1.2 och endast efter uttryckligt samtycke av medlemsstaten, och
 - d) samma villkor som de som fastställs i artikel 9.2 är uppfyllda.
2. Trots vad som sägs i artikel 13.2 i rambeslut 2008/977/RIF ska överföring av PNR-uppgifter utan förhandssamtycke av den medlemsstat från vilken uppgifterna hämtades tillåtas i undantagsfall och endast om
 - a) överföringen är absolut nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet i en medlemsstat eller ett tredjeland, och
 - b) förhandssamtycke inte kan erhållas i tid.

Den myndighet som ansvarar för att ge samtycke ska informeras utan dröjsmål och överföringen ska vederbörligen registreras samt genomgå efterhandskontroll.

3. Medlemsstaterna ska överföra PNR-uppgifter till behöriga myndigheter i tredjeländer på villkor som är förenliga med detta direktiv endast efter att ha förvässat sig om att mottagarnas planerade användning av uppgifterna är förenlig med dessa villkor och skyddsåtgärder.
4. Dataskyddsombudet vid enheten för passagerarinformation i den medlemsstat som har överfört PNR-uppgifterna ska informeras varje gång medlemsstaten överför PNR-uppgifter enligt denna artikel.

Artikel 12

Lagringstid för uppgifter och avidentifiering

1. Medlemsstaterna ska se till att PNR-uppgifter som lämnas av lufttrafikföretag till enheten för passagerarinformation lagras i en databas vid enheten under en period på fem år efter överföringen till enheten för passagerarinformation i den medlemsstat på vars territorium flygningen ankom eller avgick.
2. Vid utgången av en period på sex månader efter överföringen av de PNR-uppgifter som avses i punkt 1 ska alla PNR-uppgifter avidentifieras genom maskering av följande uppgifter, som kan användas för att omedelbart identifiera de passagerare som PNR-uppgifterna avser:
 - a) Namn, inklusive namn på andra passagerare i PNR samt antal passagerare i PNR som reser tillsammans.
 - b) Adress och kontaktuppgifter.
 - c) Alla former av betalningsinformation, inbegripet faktureringsadress, om denna innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som passageraruppgiftssamlingar avser eller andra personer.
 - d) Uppgifter om bonusprogram.
 - e) Allmänna anmärkningar, om dessa innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som passageraruppgiftssamlingar avser.
 - f) Alla API-uppgifter som samlats in.
3. Vid utgången av den sexmånadersperiod som avses i punkt 2 ska utlämnande av de fullständiga PNR-uppgifterna tillåtas endast
 - a) om det rimligen kan antas vara nödvändigt för de ändamål som avses i artikel 6.2 b, och
 - b) efter tillstånd från
 - i) en rättslig myndighet, eller
 - ii) en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda, under förutsättning att dataskyddsbudet vid enheten för passagerarinformation informeras och att denne genomför en efterhandsutvärdering.
4. Medlemsstaterna ska se till att PNR-uppgifterna slutgiltigt raderas vid utgången av den period som avses i punkt 1. Denna skyldighet gäller dock inte om specifika PNR-uppgifter har överförts till en behörig myndighet och används i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet, varvid den behöriga myndighetens lagring av uppgifterna i stället ska regleras av nationell rätt.
5. Resultaten av den behandling som avses i artikel 6.2 a ska bevaras endast av enheten för passagerarinformation så länge som krävs för att informera de behöriga myndigheterna och, i enlighet med artikel 9.1, för att informera enheterna för passagerarinformation i andra medlemsstater om en träff. Även om automatisk behandling som utförs efter en sådan individuell icke-automatisk granskning som avses i artikel 6.5 inte ger någon träff, får resultatet bevaras för att undvika framtida "falska" träffar, så länge de bakomliggande uppgifterna inte har raderats enligt punkt 4 i den här artikeln.

Artikel 13

Skydd av personuppgifter

1. Medlemsstaterna ska föreskriva att alla passagerare vid all behandling av personuppgifter i enlighet med detta direktiv har samma rätt till skydd av sina personuppgifter, rätt till åtkomst, rättelse, radering och begränsning samt rätt till ersättning och tillgång till rättsmedel som fastställs i unionsrätten och nationell rätt och för genomförande av artiklarna 17, 18, 19 och 20 i rambeslut 2008/977/RIF. Dessa artiklar ska därför tillämpas.

2. Medlemsstaterna ska föreskriva att de nationella bestämmelser om konfidentiell behandling och datasäkerhet som har antagits för genomförande av artiklarna 21 och 22 i rambeslut 2008/977/RIF även är tillämpliga på all behandling av personuppgifter i enlighet med detta direktiv.

3. Detta direktiv påverkar inte tillämpligheten av Europaparlamentets och rådets direktiv 95/46/EG⁽¹⁾ på lufttrafikföretags behandling av personuppgifter, i synnerhet deras skyldigheter att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifters säkerhet och konfidentialitet.

4. Medlemsstaterna ska förbjuda behandling av PNR-uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religion eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning. Om enheten för passagerarinformation mottar PNR-uppgifter som avslöjar sådana uppgifter, ska dessa uppgifter omedelbart raderas.

5. Medlemsstaterna ska se till att enheten för passagerarinformation bevarar dokumentation om alla system och förfaranden för uppgiftsbehandling inom deras ansvarsområde. Dokumentationen ska minst innehålla

- a) namn och kontaktuppgifter för den organisatoriska enhet och den personal vid enheten för passagerarinformation som anförtrots behandlingen av PNR-uppgifter och de olika nivåerna av åtkomstbehörighet,
- b) begäran från behöriga myndigheter och enheter för passagerarinformation i andra medlemsstater,
- c) begäran om och överföring av PNR-uppgifter till ett tredjeland.

Enheten för passagerarinformation ska på begäran göra all dokumentation tillgänglig för den nationella tillsynsmyndigheten.

6. Medlemsstaterna ska se till att enheten för passagerarinformation för loggar över åtminstone följande typer av behandling: insamling, läsning, utlämning och radering. Loggarna över läsning och utlämning ska särskilt visa ändamål, datum och tidpunkt för sådan behandling och i möjligaste mån identitetsuppgifter för den person som har läst eller lämnat ut PNR-uppgifterna samt identitetsuppgifter för de personer som mottagit uppgifterna. Loggarna ska uteslutande användas för kontroll och självövervakning, för att säkerställa dataintegritet och datasäkerhet och för revision. Enheten för passagerarinformation ska på begäran göra loggarna tillgängliga för den nationella tillsynsmyndigheten.

Loggarna ska bevaras i fem år.

7. Medlemsstaterna ska se till att deras enhet för passagerarinformation genomför lämpliga tekniska och organisatoriska åtgärder och förfaranden för att säkerställa en så hög säkerhetsnivå som är lämplig med tanke på de risker som är förknippade med behandlingen och arten av PNR-uppgifterna.

8. Om ett en personuppgiftsincident kan antas medföra ett avsevärt hot mot skyddet av den registrerades personuppgifter eller negativt påverka dennes integritet, ska medlemsstaterna se till att enheten för passagerarinformation utan onödigt dröjsmål informerar den registrerade och den nationella tillsynsmyndigheten för dataskydd om incidenten.

Artikel 14

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att se till att de genomförs.

Medlemsstaterna ska särskilt fastställa bestämmelser om sanktioner, inklusive ekonomiska sanktioner, mot lufttrafikföretag som inte översänder uppgifter i enlighet med artikel 8 eller som inte översänder uppgifterna i det fastställda formatet.

Sanktionerna ska vara effektiva, proportionella och avskräckande.

⁽¹⁾ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

*Artikel 15***Nationell tillsynsmyndighet**

1. Varje medlemsstat ska föreskriva att den nationella tillsynsmyndighet som avses i artikel 25 i rambeslut 2008/977/RIF ska ansvara för att inom sitt territorium ge riktlinjer för och övervaka tillämpningen av de bestämmelser som medlemsstaterna antar i enlighet med detta direktiv. Artikel 25 i rambeslut 2008/977/RIF ska tillämpas.
2. De nationella tillsynsmyndigheterna ska utföra sina uppgifter enligt punkt 1 i syfte att skydda grundläggande rättigheter i samband med behandling av personuppgifter.
3. Varje nationell tillsynsmyndighet ska
 - a) hantera klagomål från en registrerad, undersöka ärendet och inom rimlig tid informera de registrerade om förloppet för och resultatet av dennes klagomål,
 - b) kontrollera att uppgiftsbehandlingen är laglig, genomföra utredningar, inspektioner och revision i enlighet med nationell rätt, antingen på eget initiativ eller på grundval av ett klagomål som avses i led a.
4. Varje nationell tillsynsmyndighet ska på begäran ge registrerade råd om hur de kan utöva de rättigheter som fastställs i de bestämmelser som antas i enlighet med detta direktiv.

*KAPITEL III***Genomförandeåtgärder***Artikel 16***Gemensamma protokoll och understödda dataformat**

1. All överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation inom ramen för detta direktiv ska göras med elektroniska medel som tillhandahåller tillräckliga garantier med avseende på de tekniska säkerhetsåtgärder och de organisatoriska åtgärder som styr den behandling som ska utföras. I händelse av tekniska problem får PNR-uppgifterna överföras på annat lämpligt sätt under förutsättning att samma säkerhetsnivå upprätthålls och att unionsrätten om dataskydd respekteras fullt ut.
2. Ett år från den dag då kommissionen för första gången antar gemensamma protokoll och understödda dataformat i enlighet med punkt 3, ska all överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation inom ramen för detta direktiv göras på elektronisk väg med användning av säkra metoder i överensstämmelse med dessa godkända gemensamma protokoll. Dessa protokoll ska vara gemensamma för alla överföringar, så att PNR-uppgifternas säkerhet under överföringen tryggas. PNR-uppgifterna ska överföras i ett understött dataformat, för att säkerställa att de kan läsas av alla berörda parter. Alla lufttrafikföretag ska bestämma vilket gemensamt protokoll och vilket dataformat de avser att använda för sina överföringar och underrätta enheten för passagerarinformation om detta.
3. En förteckning över gemensamma protokoll och understödda dataformat ska upprättas och vid behov anpassas av kommissionen genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 17.2.
4. Punkt 1 ska tillämpas så länge som de gemensamma protokoll och understödda dataformat som avses i punkterna 2 och 3 inte finns tillgängliga.
5. Inom ett år från den dag då de gemensamma protokoll och understödda dataformat som avses i punkt 2 antas, ska medlemsstaterna vidta de tekniska åtgärder som krävs för att dessa gemensamma protokoll och dataformat ska kunna börja användas.

*Artikel 17***Kommittéförfarande**

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Om kommittén inte avger något yttrande, ska kommissionen inte anta utkastet till genomförandeakt och artikel 5.4 tredje stycket i förordning (EU) nr 182/2011 ska tillämpas.

*KAPITEL IV***Slutbestämmelser***Artikel 18***Införlivande**

1. Medlemsstaterna ska sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa detta direktiv senast den 25 maj 2018. De ska genast underrätta kommissionen om detta.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska till kommissionen överlämna texterna till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

*Artikel 19***Översyn**

1. På grundval av information som medlemsstaterna tillhandahållit, inbegripet de statistiska uppgifter som avses i artikel 20.2, ska kommissionen senast den 25 maj 2020 göra en översyn av samtliga delar av detta direktiv och överlämna till och lägga fram en rapport för Europaparlamentet och rådet.
2. Kommissionen ska, när den utför sin översyn, lägga särskild vikt vid
 - a) efterlevnaden av de tillämpliga standarderna för skydd av personuppgifter,
 - b) nödvändigheten och proportionaliteten i insamlingen och behandlingen av PNR-uppgifter för vart och ett av de syften som fastställs i detta direktiv,
 - c) längden på den period som uppgifterna lagras,
 - d) ändamålsenligheten i informationsutbytet mellan medlemsstaterna, och
 - e) kvaliteten på bedömningarna, även med hänsyn till den statistik som samlats in i enlighet med artikel 20.
3. Den rapport som avses i punkt 1 ska också innefatta en översyn av nödvändigheten, proportionaliteten och ändamålsenligheten i att i detta direktivs tillämpningsområde inbegripa obligatorisk insamling och överföring av PNR-uppgifter avseende samtliga eller utvalda flygningar inom EU. Kommissionen ska beakta medlemsstaternas erfarenheter, särskilt de medlemsstater som tillämpar detta direktiv på flygningar inom EU i enlighet med artikel 2. Rapporten ska också beakta huruvida det är nödvändigt att låta ekonomiska aktörer som inte är trafikföretag, t.ex. resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, omfattas av detta direktivs tillämpningsområde.

4. Mot bakgrund av den översyn som genomförs i enlighet med denna artikel, ska kommissionen om lämpligt lägga fram ett lagstiftningsförslag för Europaparlamentet och rådet i syfte att ändra detta direktiv.

Artikel 20

Statistik

1. Medlemsstaterna ska årligen tillhandahålla kommissionen statistik om PNR-uppgifter som lämnats till enheterna för passagerarinformation. Sådan statistik får inte innehålla några personuppgifter.
2. Statistiken ska åtminstone omfatta följande:
 - a) Det totala antalet passagerare vars PNR-uppgifter samlats in och utbyts.
 - b) Antalet passagerare som identifierats för ytterligare undersökning.

Artikel 21

Förhållande till andra instrument

1. Medlemsstaterna får fortsätta att sinsemellan tillämpa de bilaterala eller multilaterala avtal eller ordningar som är i kraft den 24 maj 2016 på utbyte av uppgifter mellan behöriga myndigheter, förutsatt att dessa avtal eller ordningar är förenliga med detta direktiv.
2. Detta direktiv påverkar inte tillämpligheten av direktiv 95/46/EG på lufttrafikföretags behandling av personuppgifter.
3. Detta direktiv påverkar inte medlemsstaternas eller unionens eventuella skyldigheter och åtaganden enligt bilaterala eller multilaterala avtal med tredjeländer.

Artikel 22

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Detta direktiv riktar sig till medlemsstaterna i enlighet med fördragen.

Utfärdat i Bryssel den 27 april 2016.

På Europaparlamentets vägnar
M. SCHULZ
Ordförande

På rådets vägnar
J.A. HENNIS-PLASSCHAERT
Ordförande

BILAGA I

PNR-uppgifter som samlas in av lufttrafikföretag

1. PNR-uppgifternas lokaliseringskod.
 2. Datum för bokning/utfärdande av biljett.
 3. Planerat/planerade resdatum.
 4. Namn.
 5. Adress och kontaktuppgifter (telefonnummer och e-postadress).
 6. Alla former av betalningsinformation, inbegripet faktureringsadress.
 7. Hela resrutten för aktuell passageraruppgiftssamling.
 8. Uppgifter om bonusprogram.
 9. Resebyrå/resebyråtjänsteman.
 10. Passagerarens resestatus, inbegripet resebekräftelser, incheckningsstatus, no show (passagerare som inte infinns) eller go show (passagerare utan bokning).
 11. Delade PNR-uppgifter.
 12. Allmänna anmärkningar (inklusive alla tillgängliga uppgifter om ensamkommande barn under 18 år, såsom namn och kön, ålder, språkkunskaper, namn och kontaktuppgifter för den person som följer barnet till incheckning för avresan och denna persons förhållande till barnet, namn och kontaktuppgifter för den person som hämtar barnet vid ankomsten och denna persons förhållande till barnet, flygplatsanställd som ledsagar barnet vid avresan respektive ankomsten).
 13. Biljettinformation, inbegripet biljettnummer, datum för utfärdande av biljetten, enkelbiljetter och automatisk biljettprisuppgift.
 14. Platsnummer och annan platsinformation.
 15. Information om gemensam linjebeteckning.
 16. All bagageinformation.
 17. Antal medresenärer i PNR-uppgifterna samt deras namn.
 18. Eventuell förhandsinformation (API) som samlats in (inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland och sista giltighetsdag, efternamn, förnamn, kön, födelsedatum, lufttrafikföretag, flygnummer, utresedatum, ankomstdatum, avresehamn, ankomsthavn, avresetid och ankomsttid).
 19. Alla ändringar som gjorts av de PNR-uppgifter som anges i punkterna 1–18.
-

BILAGA II

Förteckning över brott enligt artikel 3.9

1. Deltagande i en kriminell organisation.
 2. Människohandel.
 3. Sexuellt utnyttjande av barn samt barnpornografi.
 4. Olaglig handel med narkotika och psykotropa ämnen.
 5. Olaglig handel med vapen, ammunition och sprängämnen.
 6. Korruption.
 7. Bedrägeri, inbegripet riktat mot unionens finansiella intressen.
 8. Penningtvätt och penningförfalskning, inklusive förfalskning av euron.
 9. It-brottslighet/cyberbrottslighet.
 10. Miljöbrott, inbegripet olaglig handel med hotade djurarter och hotade växtarter och växtsorter.
 11. Hjälptill olovlig inresa och olovlig vistelse.
 12. Mord, grov misshandel.
 13. Olaglig handel med mänskliga organ och vävnader.
 14. Människorov, olaga frihetsberövande och tagande av gisslan.
 15. Organiserad stöld och väpnat rån.
 16. Olaglig handel med kulturföremål, inbegripet antikviteter och konstverk.
 17. Varumärkesförfalskning och piratkopiering.
 18. Förfalskning av administrativa dokument och handel med sådana förfalskningar.
 19. Olaglig handel med hormonsubstanser och andra tillväxsubstanser.
 20. Olaglig handel med nukleära och radioaktiva ämnen.
 21. Våldtäkt.
 22. Brott som omfattas av den internationella brottmålsdomstolens behörighet.
 23. Kapning av flygplan eller fartyg.
 24. Sabotage.
 25. Handel med stulna fordon.
 26. Industrispionage.
-

RÄTTELSER**Rättelse till Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet**

(Europeiska unionens officiella tidning L 119 av den 4 maj 2016)

1. Sidan 138, artikel 3.9

I stället för: "9. *grov brottslighet*: brott som förtecknas i bilaga II vilka bestraffas med fängelse eller annan frihetsberövande åtgärd i minst tre år enligt en medlemsstats nationella rätt,"

ska det stå: "9. *grov brottslighet*: brott som förtecknas i bilaga II som kan leda till fängelse eller annan frihetsberövande åtgärd i minst tre år enligt en medlemsstats nationella rätt,".

2. Sidan 148, bilaga I, punkt 18

I stället för: "18. ... (inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland och sista giltighetsdag, efternamn, förnamn, ..."

ska det stå: "18. ... (inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland och sista giltighetsdag, nationalitet, efternamn, förnamn, ...".

Bryssel den 18 april 2016
(OR. en)

Interinstitutionellt ärende:
2011/0023 (COD)

7829/16
ADD 1

CODEC 422
GENVAL 47
AVIATION 63
DATAPROTECT 29
ENFOPOL 104

I/A-PUNKTSNOT

från: Rådets generalsekretariat
till: Ständiga representanternas kommitté (Coreper)/rådet

Ärende: Utkast till Europaparlamentets och rådets direktiv om användning av passageraruppgiftssamlingar (PNR) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (**första behandlingen**)
- Antagande av lagstiftningsakten (**L + U**)
= Uttalande

Uttalande från rådet

Enligt artikel 2 i PNR-direktivet får de medlemsstater som så önskar på frivillig grund tillämpa direktivet på flygningar inom EU, efter att ha meddelat kommissionen detta.

Mot bakgrund av det aktuella säkerhetsläget i Europa förklarar medlemsstaterna att de senast det datum för införlivande som anges i artikel 18 fullt ut kommer att utnyttja den möjlighet som föreskrivs i artikel 2, enligt de villkor som anges i direktivet.

Medlemsstaterna förklarar att de i enlighet med parlamentets önskemål åtar sig¹ att i enlighet med sin nationella lagstiftning utvidga insamlingen av PNR-uppgifter till att omfatta aktörer som inte är lufttrafikföretag, t.ex. resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, för vilka de samlar in och behandlar PNR-uppgifter.

¹ Med förbehåll för parlamentsbehandling i vissa medlemsstater.

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder
– en sammanhållen politik för
arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare.
Fi.
4. För en god och jämlik hälsa.
En utveckling av det
folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en
globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och
domstolens beslutsunderlag
i brottmål – en bättre hantering av
stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017.
Kärnavfallet – en fråga i ständig
förändring. M.
9. Det handlar om oss.
– unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed
och hantera oredlighet i forskning. U.
11. Vägs katt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt.
Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med
privat kapital? Fi.
14. Migrationsärenden
vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet
på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att
närvara vid rättegången. Genomförande
av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen
mot fördjupad lokal samverkan
för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare
och enklare system för tillträde till
högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för
vård och omsorg om äldre personer.
Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får
Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur
påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt
handläggning. S.
26. Delningsekonomi. På användarnas
villkor. Fi.
27. Vissa frågor inom fastighets- och
stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap
om och utvärdering av arbetsmiljö. A.
29. Brottstatalag. Ju
30. En omreglerad spelmarknad.
Del 1 och 2. Fi.
31. Stärkt konsumentskydd
på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum
– stärkt konkurrenskraft med
kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder
för att motverka nettoförluster av
biologisk mångfald och ekosystem-
tjänster, samtidigt som behovet av
markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi
för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhälls-
viktiga och digitala tjänster. Ju.
37. Kvalificerad välfärdsbrottslighet
– förebygga, förhindra, upptäcka och
beivra. Ju.

38. Kvalitet i välfärden – bättre upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Ju.
40. För dig och för alla. S.
41. Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. Ju.
42. Vem har ansvaret? M.
43. På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. S.
44. Entreprenad, fjärrundervisning och distansundervisning. U.
45. Ny lag om företagshemligheter. Ju.
46. Stärkt ordning och säkerhet i domstol. Ju.
47. Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. S.
48. Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. S.
49. EU:s dataskyddsförordning och utbildningsområdet. U.
50. Personuppgiftsbehandling för forskningsändamål. U.
51. Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. U.
52. Så stärker vi den personliga integriteten. Ju.
53. God och nära vård. En gemensam färdplan och målbild. S.
54. Fler nyanlända elever ska uppnå behörighet till gymnasiet. U.
55. En ny kamerabevakningslag. Ju.
56. Jakten på den perfekta ersättningsmodellen. Vad händer med medarbetarnas handlingsutrymme? Fi.
57. Lag om flygpassageraruppgifter i brottsbekämpningen. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Arbetsmarknadsdepartementet

- Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. [19]
- Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? [24]
- Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. [28]

Finansdepartementet

- Karens för statsråd och statssekreterare. [3]
- Vägs katt. Volym 1 och 2. [11]
- Finansiering av infrastruktur med privat kapital? [13]
- digitalforvaltning.nu. [23]
- Delningsekonomi. På användarnas villkor. [26]
- Vissa frågor inom fastighets- och stämpel-skatteområdet. [27]
- En omreglerad spelmarknad. Del 1 och 2. [30]
- Kvalitet i välfärden – bättre upphandling och uppföljning. [38]
- Jakten på den perfekta ersättningsmodellen. Vad händer med medarbetarnas handlingsutrymme? [56]

Justitiedepartementet

- Se barnet! [6]
- Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. [7]
- Att ta emot människor på flykt. Sverige hösten 2015. [12]
- Migrationsärenden vid utlandsmyndigheterna. [14]
- Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. [17]

- Brottsdatalog. [29]
- Stärkt konsumentskydd på bostadsrättsmarknaden. [31]
- Stärkt ställning för hyresgäster. [33]
- Informationssäkerhet för samhällsviktiga och digitala tjänster. [36]
- Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. [37]
- Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. [39]
- Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. [41]
- Ny lag om företagshemligheter. [45]
- Stärkt ordning och säkerhet i domstol. [46]
- Så stärker vi den personliga integriteten. [52]
- En ny kamerabevakningslag. [55]
- Lag om flygpasageraruppgifter i brottsbekämpningen. [57]

Miljö- och energidepartementet

- Kraftsamling för framtidens energi. [2]
- Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. [8]
- Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. [22]
- Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. [32]
- Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. [34]
- Vem har ansvaret? [42]

Näringsdepartementet

För Sveriges landsbygder
– en sammanhållen politik för
arbete, hållbar tillväxt och välfärd. [1]

Socialdepartementet

För en god och jämlik hälsa.
En utveckling av det
folkhälsopolitiska ramverket. [4]
Svensk social trygghet i en globaliserad
värld. Del 1 och 2. [5]
Kvalitet och säkerhet
på apoteksmarknaden. [15]
Läs mig! Nationell kvalitetsplan
för vård och omsorg om äldre personer.
Del 1 och 2. [21]
Samlad kunskap – starkt handläggning. [25]
För dig och för alla. [40]
På lika villkor! Delaktighet, jämlikhet och
effektivitet i hjälpmedelsförsörjningen.
[43]
Nästa steg på vägen mot en mer jämlik hälsa.
Förslag för ett långsiktigt arbete för en
god och jämlik hälsa. [47]
Kunskapsbaserad och jämlik vård.
Förutsättningar för en lärande hälso-
och sjukvård. [48]
God och nära vård. En gemensam färdplan
och målbild. [53]

Utbildningsdepartementet

Det handlar om oss.
– unga som varken arbetar eller studerar. [9]
Ny ordning för att främja god sed
och hantera oredlighet i forskning. [10]
En nationell strategi för validering [18]
Tillträde för nybörjare – ett öppnare och
enklare system för tillträde till hög-
skoleutbildning. [20]
Samling för skolan.
Nationell strategi för kunskap och
likvärdighet. [35]
Entreprenad, fjärrundervisning
och distansundervisning. [44]
EU:s dataskyddsförordning och
utbildningsområdet. [49]

Personuppgiftsbehandling
för forskningsändamål. [50]

Utbildning, undervisning och ledning
– reformvård till stöd för en bättre
skola. [51]

Fler nyanlända elever ska uppnå behörighet
till gymnasiet. [54]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]