

# Lagrådsremiss

## Kompletterande bestämmelser till EU:s dataförvaltningsförordning

---

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 1 februari 2024

*Erik Slottnér*

*Johan Ndure*  
(Finansdepartementet)

## Lagrådsremissens huvudsakliga innehåll

I lagrådsremissen lämnas förslag till en ny lag som kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).

Lagen innehåller bl.a. bestämmelser om tillsyn av företag som förmedlar data och av fysiska och juridiska personer som vidareutnyttjar skyddade data enligt EU:s dataförvaltningsförordning.

Vidare föreslås kompletterande bestämmelser om tillgängliggörande av skyddade data för vidareutnyttjande enligt EU:s dataförvaltningsförordning i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data. Genom lagändringarna införs bl.a. bestämmelser om handläggningstiden i ärenden om tillgängliggörande av skyddade data för vidareutnyttjande och bemyndiganden för regeringen att utse behöriga organ och meddela föreskrifter om avgifter vid tillgängliggörande av skyddade data för vidareutnyttjande.

Den nya lagen och övriga ändringar föreslås träda i kraft den 2 augusti 2024.

# Innehållsförteckning

1	Beslut .....	4
2	Lagtext .....	5
2.1	Förslag till lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning.....	5
2.2	Förslag till lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data.....	8
3	Ärendet och dess beredning .....	13
4	EU-lagstiftning på digitaliseringsområdet .....	13
4.1	EU:s datastrategi .....	13
4.2	Öppna datadirektivet och öppna datalagen.....	14
4.3	Dataförvaltningsförordningen .....	15
5	Öppna datalagen bör komplettera EU:s dataförvaltningsförordnings regler om vidareutnyttjande av skyddade data.....	16
5.1	Tillämpningsområdet för bestämmelserna om tillgängliggörande av skyddade data för vidareutnyttjande.....	18
5.2	En definition av skyddade data.....	20
5.3	Vidareutnyttjande av skyddade data förutsätter att informationen kan lämnas ut .....	22
5.4	Exklusiva avtal och villkor för vidareutnyttjande av skyddade data .....	25
5.5	Anmälan av överträdelser som en vidareutnyttjare gör sig skyldig till vid tredjelandsöverföringar .....	26
5.6	En avgift ska kunna tas ut för vidareutnyttjande av skyddade data .....	27
5.7	Handläggningstiden för ärenden om vidareutnyttjande.....	29
5.8	Behöriga organ .....	31
5.9	Den gemensamma informationspunkten .....	32
6	Dataförmedling och dataaltruism.....	34
6.1	Bestämmelser om dataförmedlingstjänster och dataaltruismorganisationer .....	34
6.2	Behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer .....	36
6.3	Tillsyn och sanktionsavgift .....	38
6.3.1	Tillsyn.....	38
6.3.2	Tillsynsmyndigheten ska besluta om sanktionsavgift.....	41
6.3.3	Sanktionsavgiftens storlek.....	44
6.3.4	Bestämmelser om förfarandet vid beslut om sanktionsavgifter .....	46
6.3.5	Informationsutbyte och sekretess .....	47
6.4	Anmälningsförfarandet och tillsynen för leverantörer av dataförmedlingstjänster ska avgiftsbeläggas.....	51
6.5	Överklagande av beslut .....	51

7	Ikraftträdande- och övergångsbestämmelser .....	54
8	Konsekvenser .....	54
9	Författningskommentar .....	59
9.1	Förslaget till lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning .....	59
9.2	Förslaget till lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data .....	68
Bilaga 1	Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten) .....	73
Bilaga 2	Sammanfattning av promemorian Genomförande av EU:s dataförvaltningsförordning (Ds 2023:24) .....	117
Bilaga 3	Promemorians lagförslag .....	118
Bilaga 4	Förteckning över remissinstanserna .....	126

# 1 Beslut

- Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till
1. lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning,
  2. lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data.

## 2 Lagtext

Regeringen har följande förslag till lagtext.

### 2.1 Förslag till lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning

Härigenom föreskrivs följande.

**1 §** Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), i denna lag benämnd EU:s dataförvaltningsförordning.

Ord och uttryck i lagen har samma betydelse som i EU:s dataförvaltningsförordning.

#### **Tillsynsmyndighet**

**2 §** Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet enligt denna lag.

Tillsynsmyndigheten ska vara behörig myndighet för dataförmedlingstjänster enligt artikel 13 i EU:s dataförvaltningsförordning och för registrering av dataaltruismorganisationer enligt artikel 23 i EU:s dataförvaltningsförordning.

#### **Uppgiftsskyldighet**

**3 §** De myndigheter som regeringen bestämmer ska på begäran lämna tillsynsmyndigheten de uppgifter som den behöver i sin tillsynsverksamhet.

**4 §** Tillsynsmyndigheten ska på begäran lämna de uppgifter som en annan myndighet behöver i sin tillsynsverksamhet.

Regeringen bestämmer vilka myndigheter som ska ha rätt att få uppgifter enligt första stycket.

#### **Varning**

**5 §** Tillsynsmyndigheten får meddela en varning till en leverantör av dataförmedlingstjänster som bryter mot anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 eller villkoren för överföring av andra data än personuppgifter till tredjeland enligt artikel 31 i EU:s dataförvaltningsförordning.

**6 §** Tillsynsmyndigheten får meddela en varning till en fysisk eller juridisk person som har beviljats rätten att vidareutnyttja andra data än personuppgifter för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.

**7 §** Tillsynsmyndigheten får meddela en varning till en erkänd dataaltruismorganisation som bryter mot

1. villkoren för registrering som erkänd dataaltruismorganisation enligt artiklarna 18, 20, 21 eller 22, eller
2. villkoren för överföring av andra data än personuppgifter till tredjeland enligt artikel 31 i EU:s dataförvaltningsförordning.

### **Föreläggande och vite**

**8 §** Tillsynsmyndigheten får besluta de förelägganden som behövs för att EU:s dataförvaltningsförordning, denna lag eller föreskrifter som har meddelats i anslutning till lagen ska följas.

Tillsynsmyndigheten får förena ett föreläggande enligt artikel 14 i EU:s dataförvaltningsförordning med vite.

### **Sanktionsavgift**

**9 §** Tillsynsmyndigheten ska ta ut en sanktionsavgift från en leverantör av dataförmedlingstjänster vid överträdelser av

- anmälningsskyldigheten enligt artikel 11,
- villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12, eller
- villkoren för överföring av andra data än personuppgifter till tredje land enligt artikel 31 i EU:s dataförvaltningsförordning.

Om det kan anses tillräckligt får tillsynsmyndigheten, i stället för att ta ut en sanktionsavgift vid överträdelser enligt första stycket, meddela en varning enligt 5 §.

**10 §** Tillsynsmyndigheten ska ta ut en sanktionsavgift av en fysisk eller juridisk person som har beviljats rätten att vidareutnyttja andra data än personuppgifter för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.

Om det kan anses tillräckligt får tillsynsmyndigheten, i stället för att ta ut en sanktionsavgift vid överträdelser enligt första stycket, meddela en varning enligt 6 §.

**11 §** En sanktionsavgift enligt 9 eller 10 § ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

När avgiftens storlek bestäms ska hänsyn tas till

1. överträdelsens art, allvar, omfattning och varaktighet,
2. åtgärder som har vidtagits för att begränsa eller avhjälpa den skada som överträdelsen har orsakat,
3. tidigare överträdelser,
4. de ekonomiska vinster som har gjorts eller de förluster som har undvikits till följd av överträdelsen, och
5. försvarande eller förmildrande omständigheter utöver dem i 1–4.

Tillsynsmyndigheten får avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

**12 §** En sanktionsavgift får inte tas ut om överträdelsen omfattas av ett föreläggande som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

**13 §** En sanktionsavgift får tas ut endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från den dag då överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

**14 §** En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i tid, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

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

### **Avgifter**

**16 §** Tillsynsmyndigheten får ta ut avgifter från leverantörer av dataförmedlingstjänster för anmälan, registerhållning och tillsyn av leverantörer av dataförmedlingstjänster enligt EU:s dataförvaltningsförordning och denna lag.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om avgifterna.

### **Överklagande**

**17 §** Tillsynsmyndighetens beslut enligt artiklarna 14, 19 och 24 i EU:s dataförvaltningsförordning eller enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

Denna lag träder i kraft den 2 augusti 2024.

## 2.2 Förslag till lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data

Härigenom föreskrivs i fråga om lagen (2022:818) om den offentliga sektorns tillgängliggörande av data

*dels* att 1 kap. 2–4 och 8 §§ och 5 kap. 1 § ska ha följande lydelse,

*dels* att det ska införas sju nya paragrafer, 1 kap. 1 a och 7 a §§, 2 kap. 5 a, 6 a och 7 §§, 3 kap. 1 a § och 4 kap. 2 a §, och närmast före 2 kap. 6 a och 7 §§ nya rubriker av följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

### 1 kap.

#### 1 a §

*Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), i denna lag benämnd EU:s dataförvaltningsförordning.*

#### 2 §

Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data eller som begränsar en sådan rätt.

Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data *eller skyddade data* eller som begränsar en sådan rätt.

Lagen påverkar inte heller tillämpningen av bestämmelser i någon annan lag eller förordning om skyddet av personuppgifter.

#### 3 §

Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data än i denna lag, ska de kraven tillämpas.

Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data *eller skyddade data* än i denna lag, ska de kraven tillämpas.

#### 4 §

I lagen avses med

*begäran om tillgängliggörande av data för vidareutnyttjande*: en begäran om att data ska göras tillgängliga för vidareutnyttjande i enlighet med denna lag,

*begäran om tillgängliggörande av data för vidareutnyttjande*: en begäran om att data *eller skyddade data* ska göras tillgängliga för vidareutnyttjande i enlighet med



denna lag eller kapitel II i EU:s dataförvaltningsförordning,

*bulknedladdning*: nedladdning av en avgränsad datamängd,

*data*: information i digitalt format oberoende av medium,

*dynamiska data*: data som uppdateras ofta eller i realtid för att vara aktuella och relevanta att vidareutnyttja,

*forskningsdata*: data som till någon del är offentligt finansierade, som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet och som görs direkt tillgängliga för vidareutnyttjande genom en dataplattform som är allmänt åtkomlig,

*gränssnitt*: en regeluppsättning för dynamiskt datautbyte mellan programvaror,

*maskinläsbart format*: ett filformat som är strukturerat på ett sådant sätt att det enkelt kan läsas av ett datorprogram,

*offentligt företag*: ett företag som en eller flera myndigheter har ett bestämmande inflytande över och som är verksamt

– inom de sektorer som framgår av 2 kap. 1 § och 5–8 §§ lagen (2016:1146) om upphandling inom försörjningssektorerna,

– som ett kollektivtrafikföretag enligt Europaparlamentets och rådets förordning (EG) nr 1370/2007 av den 23 oktober 2007 om kollektivtrafik på järnväg och väg och om upphävande av rådets förordning (EEG) nr 1191/69 och (EEG) nr 1107/70,

– som ett lufttrafikföretag som har allmän trafikplikt enligt artikel 16 i Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen, eller

– som ett rederi inom gemenskapen som uppfyller förpliktelser vid allmän trafik enligt artikel 4 i rådets förordning (EEG) nr 3577/92 av den 7 december 1992 om tillämpning av principen om frihet att tillhandahålla tjänster på sjötransportområdet inom medlemsstaterna (cabotage),

*offentligt styrt organ*: ett sådant organ som avses i 1 kap. 18 § lagen (2016:1145) om offentlig upphandling eller en sammanslutning av sådana organ,

*skyddade data*: sådana kategorier av data som avses i artikel 3.1 i EU:s dataförvaltningsförordning,

*vidareutnyttjande*: bearbetning av data från den offentliga sektorn för valfritt ändamål,

*värdefull datamängd*: data som förtecknas i en genomförandeakt som har meddelats med stöd av artikel 14.1 i öppna data-direktivet,

*öppna data-direktivet*: Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

#### 7 a §

*Bestämmelserna om vidareutnyttjande av skyddade data ska endast tillämpas av myndigheter, dock inte av kultur- eller utbildningsinstitutioner.*

Lagen ska tillämpas

1. när någon som har rätt att få tillgång till data enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,

2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, *eller*

3. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.

Trots första stycket ska lagen inte tillämpas

1. när data, i andra fall än som avses i första stycket 3, lämnas

a) mellan statliga och kommunala myndigheter,

b) från ett organ som enligt 1 kap. 5 § andra stycket jämställs med en myndighet eller ett offentligt företag till en statlig eller kommunal myndighet, eller

2. när en statlig eller kommunal myndighet tillhandahåller data i en konkurrensutsatt verksamhet.

1. när någon som har rätt att få tillgång till data *eller skyddade data* enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,

2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas,

3. när en myndighet på eget initiativ tillgängliggör *skyddade data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, eller*

4. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.

1. när data, i andra fall än som avses i första stycket 4, lämnas

## 2 kap.

### 5 a §

*En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska ställa upp villkor för vidareutnyttjandet i enlighet med artikel 5 i EU:s dataförvaltningsförordning.*

*En myndighet som tillgängliggör skyddade data till en vidareutnyttjare som avser att överföra dem till tredjeland i enlighet med artikel 5.10 i EU:s dataförvaltningsförordning är skyldig att anmäla de överträdelser av artikel 5.14 som myndigheten får kännedom om till tillsynsmyndigheten enligt lagen (2024:000) med*

*kompletterande bestämmelser till EU:s dataförvaltningsförordning.*

### **En gemensam informationspunkt**

#### **6 a §**

*Den myndighet som regeringen bestämmer ska tillhandahålla en gemensam informationspunkt enligt artikel 8 i EU:s dataförvaltningsförordning.*

*En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska informera den myndighet som tillhandahåller den gemensamma informationspunkten om sådana data och villkoren för vidareutnyttjande av dessa.*

### **Behöriga organ enligt EU:s dataförvaltningsförordning**

#### **7 §**

*Den eller de myndigheter som regeringen bestämmer ska vara behöriga organ enligt artikel 7 i EU:s dataförvaltningsförordning.*

### **3 kap.**

#### **1 a §**

*En myndighet som innehar skyddade data får ge någon en exklusiv rätt att vidareutnyttja dessa data endast om det är tillåtet enligt artikel 4 i EU:s dataförvaltningsförordning.*

### **4 kap.**

#### **2 a §**

*En myndighet som tillgängliggör skyddade data för vidareutnyttjande får ta ut en avgift för tillgängliggörandet.*

*Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om avgiften.*

## 5 kap.

### 1 §

En myndighet ska inom fyra veckor avgöra ett ärende till följd av en begäran om tillgängliggörande av data för vidareutnyttjande.

*Om en sådan begäran avser skyddade data ska ärendet avgöras inom åtta veckor.*

Tidsfristen får förlängas med ytterligare fyra veckor, om en begäran är omfattande eller komplicerad. Myndigheten ska underätta sökanden om förlängningen och redovisa skälen för den senast tre veckor från den dag då begäran kom in.

Tidsfristen enligt första eller andra stycket får förlängas med ytterligare fyra veckor, om en begäran är omfattande eller komplicerad. Myndigheten ska underätta sökanden om förlängningen och redovisa skälen för den senast tre veckor från den dag då begäran kom in.

---

Denna lag träder i kraft den 2 augusti 2024.

### 3 Ärendet och dess beredning

Europaparlamentet och rådet har antagit förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), förkortad EU:s dataförvaltningsförordning. Förordningen finns i *bilaga 1*.

I oktober 2022 beslutades att ge en ämnessakkunnig i uppdrag att biträda Infrastrukturdepartementet med att ta fram ett förslag på hur EU:s dataförvaltningsförordning kan kompletteras i nationell rätt.

Resultatet av utredningen redovisades i juli 2023 i departementspromemorian Genomförande av EU:s dataförvaltningsförordning (Ds 2023:24). En sammanfattning av promemorian finns i *bilaga 2*. Promemorians lagförslag finns i *bilaga 3*. Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissyttrandena finns tillgängliga i Finansdepartementet (Fi2023/01601).

I denna lagrådsremiss behandlas promemorians förslag.

## 4 EU-lagstiftning på digitaliseringsområdet

### 4.1 EU:s datastrategi

I februari 2020 meddelade Europeiska kommissionen en datastrategi för EU (COM (2020) 66, Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – En EU-strategi för data). Datastrategin innehåller förslag till åtgärder som syftar till att göra EU till den mest attraktiva, säkraste, mest dynamiska och mest snabbväxande datadrivna ekonomin i världen. Tanken är att Europa genom bättre användning av data som resurs ska förbättra beslutsfattande och livskvalitet för samtliga medborgare.

Kommissionen anser att EU:s teknologiska framtid är avhängig förmågan att hantera värdet av data genom en europeisk modell, samt genom strukturer och politik för data under kommande år. Kommissionen lyfter bl.a. fram 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), Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) och inrättandet av en kodex för elektronisk kommunikation som betydelsefulla rättsliga grunder för en säker, trygg och snabbväxande dataekonomi. Likaså betonas investeringar i digital infrastruktur och lagstiftning inom vissa sektorer och domäner, bl.a. för intelligenta transportsystem, som angelägna för bättre tillgång till data inom EU. Kommissionens vision går bl.a. ut på att, med beaktande av klimatutmaningarna och grundläggande värden för medborgarna, skapa

europiska datautrymmen som ska kunna stödja utvecklingen inom vissa samhällssektorer, såsom tillverkning, hälsa och mobilitet.

EU:s datastrategi tar upp ett antal åtgärder och investeringar som behöver genomföras under kommande år för att uppnå de i meddelandet uppsatta målen samt stärka Europas internationella konkurrenskraft inom bl.a. artificiell intelligens och annan digital innovation. Kommissionens mål är att skapa ett gemensamt europeiskt dataområde och en fungerande och säker inre marknad för data. Genom genomförandet av de olika åtgärderna i EU:s datastrategi ska mer data göras tillgänglig för användning i ekonomin och samhället, samtidigt som de som genererar uppgifterna behåller kontrollen. Slutmålet för EU är att dra nytta av fördelarna med bättre dataanvändning, vilket kan vara ökad produktivitet och konkurrenskraftiga marknader, men även förbättringar inom hälsa och välbefinnande, miljö, transparent styrning och bekväma offentliga tjänster.

## 4.2 Öppna datadirektivet och öppna datalagen

Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn, nedan öppna datadirektivet, syftar till att främja användningen av öppna data och stimulera innovation inom produkter och tjänster genom vidareutnyttjande av information som tillgängliggörs av den offentliga sektorn. Direktivet har anpassats till de senaste framstegen inom digital teknik och ska ytterligare främja digital innovation, särskilt beträffande artificiell intelligens (skäl 3). Direktivets reglering strävar mot att hantera kvarstående och nya hinder som motverkar ett brett vidareutnyttjande av information.

Öppna datadirektivet genomfördes i Sverige genom lagen (2022:818) om den offentliga sektorns tillgängliggörande av data, i fortsättningen öppna datalagen. Lagen syftar till att främja den offentliga sektorns tillgängliggörande av data för vidareutnyttjande, särskilt i form av öppna data, under förutsättning att krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och att det inte innebär risker för Sveriges säkerhet. Med öppna data avses data som finns tillgängliga i ett öppet format och som kan vidareutnyttjas fritt för valfritt ändamål (prop. 2021/22:225 s. 71). Vidare reglerar lagen vad som ska gälla i fråga om tilldelning av exklusiv rätt till vidareutnyttjande av data samt uttag av avgifter och utformning av villkor när data görs tillgängliga.

Öppna datadirektivet ger inte någon en rätt att få tillgång till data. En enskild kan alltså inte åberopa öppna datadirektivet, eller lagstiftningen som grundas på direktivet, för att få tillgång till data. Öppna datalagen är tillämplig när någon i ett konkret fall har rätt att få tillgång till data enligt någon annan lag eller förordning, oavsett på vilken rättslig grund det sker (prop. 2021/22:225 s. 29). I första hand finns sådana bestämmelser i 2 kap. tryckfrihetsförordningen, förkortad TF, om utlämnande av allmänna handlingar och i 6 kap. offentlighets- och sekretesslagen (2009:400), förkortad OSL, om utlämnande av uppgifter. Bestämmelser om rätt till data finns också i sektors- eller myndighetsspecifika författningar, bl.a. lagen (2010:1767) om geografisk miljöinformation, lagen (2000:224) om

fastighetsregister och förordningen (1984:692) om det allmänna företagsregistret. En myndighet kan också i sin instruktion ha till uppgift att tillhandahålla vissa data, se exempelvis 2 § förordningen (2008:1233) med instruktion för Sveriges geologiska undersökning. En myndighet eller ett offentligt företag kan också på eget initiativ göra data tillgängliga för vidareutnyttjande i syfte att data ska kunna vidareutnyttjas. Öppna datalagen är tillämplig i båda situationerna, dvs. när någon har rätt att få tillgång till data med stöd i annan lag eller förordning eller när en myndighet eller ett offentligt företag på eget initiativ ger tillgång till data i syfte att dessa ska kunna vidareutnyttjas. Att data tillgängliggörs i syfte att kunna vidareutnyttjas innebär att lagen inte ska tillämpas vid varje tillfälle som en myndighet eller ett offentligt företag publicerar data på eget initiativ. Om data publiceras i ett annat syfte, exempelvis för att sprida information om myndighetens eller företagets verksamhet, ska lagen inte tillämpas (prop. 2021/22:225. s. 29 och 30).

### 4.3 Dataförvaltningsförordningen

Europaparlamentet och rådet har antagit förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), i fortsättningen EU:s dataförvaltningsförordning. Bestämmelserna i förordningen tillämpas fr.o.m. den 24 september 2023. EU:s dataförvaltningsförordning är den första EU-förordningen som har sin grund i EU:s datastrategi.

EU:s dataförvaltningsförordning syftar till att förbättra villkoren för datadelning på den inre marknaden genom att skapa en harmoniserad ram för utbyte av data och föreskriva vissa grundläggande krav på dataförvaltning, med särskild omsorg om att underlätta samarbetet mellan medlemsstaterna (skäl 3).

I kapitel II i EU:s dataförvaltningsförordning finns villkor och ramar för vidareutnyttjande av skyddade data som innehas av offentliga myndigheter. Kapitlet kan ses som en komplettering till öppna datadirektivet och en vidareutveckling gällande det rättsliga ramverket för att kunna tillgängliggöra offentligt producerade data för vidareutnyttjande. Med skyddade data avses olika kategorier av data som är skyddade på grund av insynsskydd för kommersiella uppgifter, statistiska uppgifter, immateriella rättigheter eller personuppgifter (artikel 3.1). EU:s dataförvaltningsförordnings bestämmelser om tillgängliggörande av skyddade data för vidareutnyttjande ger inte någon rätt till tillgång till sådan data, utan regelverket handlar om hur information kan och ska tillhandahållas när data görs tillgänglig. Tanken är sedan att nya kompletterande regleringar ska utvecklas genom sektorsspecifik unionsrätt, t.ex. den planerade unionsrätten inom hälsodataområdet (se skäl 3).

Genom EU:s dataförvaltningsförordning inrättas vidare en ram för anmälan av och tillsyn över tillhandahållandet av dataförmedlingstjänster (kapitel III), en ram för frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål (kapitel IV) och en ram för inrättandet av en europeisk datainnovationsstyrelse (kapitel VI).

EU:s dataförvaltningsförordning ställer bl.a. krav på att medlemsstaterna utser behöriga organ (artikel 7.1) och myndigheter (artiklarna 13 och 23), en s.k. gemensam informationspunkt (artikel 8), tillhandahåller en förteckning över tillgängliga datakällor (artikel 8.2) samt inför bestämmelser om sanktioner (artikel 34) och en rätt till överprövning av vissa beslut (artiklarna 9.2 och 28). Vidare föreskriver EU:s dataförvaltningsförordning att medlemsstaterna får besluta om avgifter (artikel 6) och om handläggningstiden för ärenden om vidareutnyttjande av skyddade data (artikel 9.1). Mot denna bakgrund behövs det kompletterande nationella bestämmelser om bl.a. handläggningen av ärenden om vidareutnyttjande av skyddade data, rättsmedel och bemyndiganden för regeringen att utse behöriga organ och myndigheter.

## 5 Öppna datalagen bör komplettera EU:s dataförvaltningsförordnings regler om vidareutnyttjande av skyddade data

**Regeringens bedömning:** De bestämmelser som behövs för att komplettera EU:s dataförvaltningsförordnings reglering om vidareutnyttjande av skyddade data bör införas i lagen om den offentliga sektorns tillgängliggörande av data.

**Promemorians förslag** överensstämmer med regeringens bedömning.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget. *Sveriges kommuner och regioner (SKR)* och *Stockholms kommun* ser positivt på att införa kompletterande bestämmelser om vidareutnyttjande av skyddade data i öppna datalagen. De anser att lagstiftningen blir mer överskådlig om bestämmelserna integreras i öppna datalagen. SKR menar dock att det är viktigt att det tydligt framgår hur de olika regelverken ska tillämpas. *Nacka kommun* är positiv till att tillgängliggöra skyddade data för vidareutnyttjande. Enligt kommunen ligger lagstiftningen i linje med kommunens digitaliseringsstrategi.

*Lantmäteriet* ser en risk med att ha kompletterande bestämmelser om skyddade data i öppna datalagen när det inte tydligt framgår vilka bestämmelser i lagen som är avsedda att användas i respektive ärendetyp. Enligt *Myndigheten för digital förvaltning* bör myndigheterna ha mer långtgående skyldigheter att dela data än vad EU:s dataförvaltningsförordning föreskriver. *TechSverige* anser att regeringen, mot bakgrund av att det finns flera utredningar och initiativ på området, bör vidta åtgärder för att samla och samordna politiken för data, vidareutnyttjande av data och närliggande frågor.



Endast ett fåtal remissinstanser, bl.a. *Försvarsmakten*, avstyrker förslaget. *Bolagsverket* menar att de kompletterande bestämmelserna om vidareutnyttjande av skyddade data i stället bör införas i den föreslagna nya lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning (i fortsättningen benämnd kompletteringslagen).

**Skälen för regeringens bedömning:** EU:s dataförvaltningsförordning, öppna datadirektivet och öppna datalagen har gemensamt att de bl.a. reglerar vidareutnyttjande av data som tillhandahålls av den offentliga sektorn. Det befintliga nationella regelverket med bestämmelser om vidareutnyttjande av data i öppna datalagen skulle därför vara ett alternativ för införande av kompletterande bestämmelser till dataförvaltningsförordningen om vidareutnyttjande av skyddade data. De olika regelverken avser dock olika typer av data. Vilka subjekt som träffas av regelverken skiljer sig också delvis åt. EU:s dataförvaltningsförordnings bestämmelser om vidareutnyttjande av data omfattar t.ex. bara myndigheter medan öppna datadirektivet även omfattar offentliga företag.

Trots de skillnader som finns mellan regelverken finns det flera skäl som talar för att samla bestämmelser om vidareutnyttjande av data i en lag. Som flera remissinstanser påpekar, däribland *SKR* och *Stockholms kommun*, skulle det t.ex. göra det enklare för såväl myndigheter som vidareutnyttjare att få en samlad bild av regelverket gällande vidareutnyttjande av data. Vidare anser regeringen, till skillnad från *Lantmäteriet*, att det är en fördel att ha ett gemensamt regelverk för vidareutnyttjande av data när flera av bestämmelserna kommer att vara likartade, t.ex. bestämmelser om handläggningstid, skyddsåtgärder och rättsmedel. I de fall det behövs olika bestämmelser är det förstås av vikt att se till att det tydligt framgår av lagstiftningen vilka bestämmelser som är tillämpliga i respektive ärendetyp. Detta kan dock säkerställas genom att det av respektive bestämmelse framgår om den endast avser data, skyddade data eller båda kategorier av data.

Ett alternativ till att införa kompletterande bestämmelser om vidareutnyttjande av skyddade data i öppna datalagen är att, som *Bolagsverket* förespråkar, införa dessa i en ny lag. Flera av bestämmelserna skulle dock i ett sådant regelverk motsvara eller vara likartade de som redan finns i öppna datalagen. För att göra så att öppna datalagen även gäller för skyddade data krävs det däremot endast att det görs mindre justeringar och tillägg i lagen. Det finns således fördelar med att använda sig av befintligt regelverk.

Sammantaget bedömer regeringen att de kompletterande bestämmelserna om vidareutnyttjande av skyddade data som behöver införas i den nationella lagstiftningen bör införas i öppna datalagen.

Det ligger utanför detta lagstiftningsärende att, som *TechSverige* efterfrågar, vidta åtgärder för att samla och samordna politiken för data. Det ligger också utanför detta lagstiftningsärende att, som *Myndigheten för digital förvaltning* efterfrågar, besluta om mer långtgående skyldigheter för myndigheterna att dela data än vad EU:s dataförvaltningsförordning föreskriver.

## 5.1 Tillämpningsområdet för bestämmelserna om tillgängliggörande av skyddade data för vidareutnyttjande

**Regeringens förslag:** Bestämmelserna om vidareutnyttjande av skyddade data ska endast tillämpas av myndigheter, dock inte av kultur- eller utbildningsinstitutioner.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Luleå, Gagnefs kommun, Integritetsskyddsmyndigheten, Justitiekanslern, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Kungliga tekniska högskolan* anser att det inte är tillräckligt klart om undantaget för utbildningsinstitutioner även omfattar utbildningsinstitutioner för högre utbildning, som t.ex. Sveriges universitet och högskolor. Enligt myndigheten är det också oklart om hela eller delar av universitetens verksamhet inryms i ordet hybridorganisation i EU:s dataförvaltningsförordning. *Försvarmakten* och *Försvarets radioanstalt* anser att deras verksamhet inte ska omfattas av EU:s dataförvaltningsförordning, eftersom försvars- och säkerhetsområdet ligger utanför EU:s kompetens. Myndigheternas verksamhet bör därför enligt myndigheterna uttryckligen undantas från öppna datalagens tillämpningsområde. Enligt *Försvarmakten* är öppna datalagens bestämmelser för skyddet av information, och därmed skyddet av den nationella säkerheten, inte tillräckliga.

**Skälen för regeringens förslag:** Öppna datadirektivet och öppna datalagen omfattar inte bara data som innehas av offentliga myndigheter utan också vissa data som innehas av offentliga företag och vissa kulturinstitutioner (artikel 1.1 i öppna datadirektivet och 1 kap. 5–7 §§ öppna datalagen). Bestämmelserna om vidareutnyttjande av skyddade data i kapitel II i EU:s dataförvaltningsförordning omfattar däremot endast offentliga myndigheter (artikel 3.1). Med offentliga myndigheter avses statliga, regionala eller lokala myndigheter och offentligrättsliga organ, eller sammanslutningar av en eller flera sådana myndigheter eller av ett eller flera sådana offentligrättsliga organ (artikel 2.17). Från EU:s dataförvaltningsförordnings tillämpningsområde görs också uttryckligen undantag för offentliga företag, public service-bolag, kulturinstitutioner och utbildningsinstitutioner (artikel 3.2). Med offentligt företag avses varje företag över vilket de offentliga myndigheterna har ett direkt eller indirekt bestämmande inflytande (artikel 2.19). Definitionen av offentligt företag skiljer sig från motsvarande uttryck i öppna datadirektivet (jfr artikel 1.1 b i öppna datadirektivet).

Public service-bolag omfattas inte heller av öppna datadirektivet eller öppna datalagen (jfr artikel 2 i öppna datadirektivet och 1 kap. 7 § öppna datalagen). I de engelska versionerna av öppna datadirektivet och EU:s

dataförvaltningsförordning används samma uttryck, nämligen public service broadcasters. I de svenska översättningarna används dock uttrycket offentliga radio- och tv-företag i öppna datadirektivet respektive public service-bolag i EU:s dataförvaltningsförordning. I öppna datalagen används uttrycket radio- och tv-företag vars sändningsverksamhet finansieras med public service-avgift enligt lagen (2018:1893) om finansiering av radio och tv i allmänhetens tjänst.

Tillämpningsområdet för bestämmelserna om vidareutnyttjande av skyddade data i EU:s dataförvaltningsförordning är sammanfattningsvis snävare än öppna datadirektivet avseende vilka innehavare av data som omfattas. Om öppna datalagen ska komplettera EU:s dataförvaltningsförordning bör det därför enligt regeringens mening införas en bestämmelse i öppna datalagen som förtydligar vilka subjekt som träffas av de kompletterande bestämmelserna om vidareutnyttjande av skyddade data enligt EU:s dataförvaltningsförordning. Bestämmelserna om vidareutnyttjande av skyddade data i EU:s dataförvaltningsförordning ska endast tillämpas av myndigheter, inte av offentliga företag, public service-bolag eller kultur- och utbildningsinstitutioner. Public service-bolag och offentliga företag betraktas inte som myndigheter enligt svensk rätt (prop. 1979/80:2 Del A s. 125). Det behövs därför enligt regeringen inte ett särskilt undantag för dessa. Bestämmelsen bör således endast omfatta myndigheter, och uttryckligen undanta kultur- och utbildningsinstitutioner.

*Kungliga tekniska högskolan* efterfrågar ett förtydligande av vilka utbildningsinstitutioner som undantas från tillämpningsområdet. I EU:s dataförvaltningsförordning preciseras inte vad som avses med utbildningsinstitutioner. Av skälen till EU:s dataförvaltningsförordning framgår att organisationer som bedriver forskning och organisationer som finansierar forskning omfattas av tillämpningsområdet. Även hybridorganisationer, i den del dessa organisationer bedriver forskning, omfattas av tillämpningsområdet (skäl 12). Av artikel 3.2 framgår dock endast att kultur- och utbildningsinstitutioner undantas från tillämpningsområdet. Det anges inte i den artikeln att sådana organisationer ska omfattas om de bedriver forskning. Det bör därför enligt regeringen vara upp till rättstillämparen, och ytterst EU-domstolen, att förtydliga hur bestämmelserna i artikel 3.2 ska tolkas i förhållande till skälen. De nationella bestämmelserna om vidareutnyttjande av skyddade data bör således endast tillämpas av myndigheter, dock inte av kultur- eller utbildningsinstitutioner.

I artikel 3.2.d i EU:s dataförvaltningsförordning undantas data som innehas av offentliga myndigheter som är skyddade av skäl som rör allmän säkerhet, försvar eller nationell säkerhet. Enligt regeringen finns det därför inte anledning att, som *Försvarmakten* och *Försvarets radioanstalt* efterfrågar, undanta dessa myndigheters verksamheter från tillämpningsområdet för de föreslagna bestämmelserna om vidareutnyttjande av skyddade data. EU:s dataförvaltningsförordning medför dessutom inte några skyldigheter för myndigheter att tillgängliggöra skyddade data (se avsnitt 5.3).

## 5.2 En definition av skyddade data

**Regeringens förslag:** En begäran om tillgängliggörande av data för vidareutnyttjande enligt öppna datalagen ska även omfatta skyddade data enligt EU:s dataförvaltningsförordning.

Med skyddade data ska data avses som innehas av myndigheter och som är skyddade på grund av

- insynsskydd för kommersiella uppgifter, inklusive affärs-, yrkes- och företagshemligheter,
- insynsskydd för statistiska uppgifter,
- skydd av tredje parts immateriella rättigheter, eller
- skydd av personuppgifter, i den mån sådana uppgifter faller utanför tillämpningsområdet för öppna datadirektivet.

De kompletterande bestämmelserna om vidareutnyttjande av skyddade data ska inte påverka tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till skyddade data eller som begränsar en sådan rätt eller som innebär mer långtgående krav i fråga om tillgängliggörande av skyddade data.

**Promemorians förslag** överensstämmer delvis med regeringens. I promemorian föreslås att undantaget i öppna datalagen för data som omfattas av immateriella rättigheter inte ska gälla för sådana kategorier av skyddade data som omfattas av EU:s dataförvaltningsförordning.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

Enligt *Försäkringskassan* bör det förtydligas vilka datamängder med personuppgifter som omfattas av uttrycket skyddade data. *Lantmäteriet* anser att det bör tydliggöras om en och samma datamängd kan omfattas av tillämpningsområdet för den nuvarande öppna datalagen och de föreslagna kompletterande bestämmelserna i samma lag.

### Skälen för regeringens förslag

#### *Uttrycken data och skyddade data*

EU:s dataförvaltningsförordnings bestämmelser om vidareutnyttjande tar sikte på särskilda typer av data, nämligen vissa kategorier av skyddade data som innehas av myndigheter (artikel 3.1). Det är data som är skyddade på grund av insynsskydd för kommersiella uppgifter, statistiska uppgifter, tredje parts immateriella rättigheter och personuppgifter. Öppna datalagen omfattar däremot data i en bredare bemärkelse. Om det ska införas kompletterande bestämmelser för skyddade data i öppna datalagen behövs det en definition av sådan data i den lagen. Enligt regeringen bör det därför i öppna datalagen införas en hänvisning till definitionen av skyddade data i EU:s dataförvaltningsförordning. På så sätt säkerställs att definitionen överensstämmer med den i EU:s dataförvaltningsförordning.

Hänvisningen bör vara utformad så att den avser förordningen i den vid varje tidpunkt gällande lydelsen, s.k. dynamisk hänvisning. Förordningen kan då ändras utan att de kompletterande bestämmelserna behöver justeras.

Till skillnad från vad *Försäkringskassan* framför bör det vara upp till rättstillämparen, ytterst EU-domstolen, att bestämma den närmare innebörden av uttrycket skyddade data. Det saknas vidare skäl att, som *Lantmäteriet* efterfrågar, förtydliga om samma datamängd kan omfattas av såväl öppna datalagens nuvarande bestämmelser som de föreslagna bestämmelserna om skyddade data. En datamängd bör i vissa fall kunna omfattas av både öppna datalagen och de föreslagna bestämmelserna. I en sådan situation bör de bestämmelser som föreskriver de mer långtgående kraven gälla, t.ex. i form av skyddsåtgärder, vilket i de flesta av fallen torde vara EU:s dataförvaltningsförordning (jfr skäl 3, 10 och artikel 3.1 d).

Data som skyddas på grund av tredje parts immateriella rättigheter omfattas av kapitel II i EU:s dataförvaltningsförordning, men inte av öppna datalagen (jfr 1 kap. 10 § öppna datalagen). I promemorian föreslås därför att skyddade data ska undantas från bestämmelserna i 1 kap. 10 § öppna datalagen för skyddade data. Eftersom bestämmelserna i 1 kap. 10 § öppna datalagen dock endast omfattar data anser regeringen att det inte behövs ett sådant undantag för skyddade data.

Bestämmelserna i öppna datalagen om att lagen inte påverkar tillämpningen av bestämmelser i någon annan lag eller förordning bör även gälla för skyddade data. Av de bestämmelserna följer också att lagen inte påverkar tillämpningen av bestämmelser i någon annan lag eller förordning om skyddet av personuppgifter (1 kap. 2 §). Även bestämmelserna om att mer långtgående krav i annan lag eller förordning i fråga om tillgängliggörande av data har företräde framför öppna datalagen bör gälla för skyddade data (1 kap. 3 §).

#### *Vidareutnyttjande i öppna datalagen, öppna datadirektivet och EU:s dataförvaltningsförordning*

Vidareutnyttjande definieras i 1 kap. 4 § öppna datalagen som bearbetning av data från den offentliga sektorn för valfritt ändamål. Definitionen av vidareutnyttjande i EU:s dataförvaltningsförordning ställer, till skillnad från definitionen i öppna datalagen, inte något krav på bearbetning (artikel 2.2). I öppna datadirektivet definieras vidareutnyttjande däremot som användning av handlingar för andra ändamål än det ursprungliga ändamål för vilket handlingarna framställdes (artikel 2.11). Den definitionen stämmer bättre överens med den i EU:s dataförvaltningsförordning. Eftersom 1 kap. 4 § öppna datalagen bl.a. införlivar artikel 2.2 i öppna datadirektivet bedömer regeringen att ordet vidareutnyttjande i öppna datalagen är likvärdigt med motsvarande ord i EU:s dataförvaltningsförordning (prop. 2021/22:225 s. 73).

#### *Vidareutnyttjande enligt öppna datalagen strider inte mot efterforskningsförbudet i tryckfrihetsförordningen*

Den som har fått del av en allmän handling får som huvudregel använda den fritt för valfritt ändamål. Det innebär att en myndighet i allmänhet inte får förena ett utlämnande av en allmän handling med villkor om hur hand-

lingen får vidareutnyttjas. En myndighet får inte heller på grund av att någon begär att få ta del av en allmän handling efterforska vem denne är eller vilket syfte han eller hon har med sin begäran i större utsträckning än vad som behövs för att myndigheten ska kunna pröva om det finns hinder mot att handlingen lämnas ut (2 kap. 18 § TF), det s.k. efterforskningsförbudet.

Av 1 kap. 8 § första stycket 1 öppna datalagen, som föreslås gälla även för skyddade data, framgår att lagen bl.a. ska tillämpas när någon som har rätt att få tillgång till data enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande. Det förutsätter dels att vidareutnyttjaren begär att få tillgång till data enligt någon annan författning, dels att de ska tillgängliggöras för vidareutnyttjande enligt öppna datalagen. Öppna datalagen ska alltså tillämpas först när det har konstaterats att det finns en författningsreglerad rätt till tillgång och att det inte finns några hinder mot att ge tillgång till de data som efterfrågas. Efterforskningsförbudet gäller vid en prövning av om en allmän handling får lämnas ut eller inte. En sådan prövning föregår den prövning som görs av om handlingen i fråga kan tillgängliggöras som data för vidareutnyttjande. Regeringen har därför gjort bedömningen att ordet vidareutnyttjande inte strider mot efterforskningsförbudet i tryckfrihetsförordningen (jfr prop. 2021/22:225 s. 20).

Regeringen bedömer alltså att ordet vidareutnyttjande inte strider mot efterforskningsförbudet i tryckfrihetsförordningen. Definitionen av begäran om tillgängliggörande av data för vidareutnyttjande i öppna datalagen bör därför även omfatta skyddade data. För att en prövning enligt bestämmelserna i öppna datalagen ska aktualiseras bör det dessutom krävas att det tydligt framgår att det handlar om en begäran om tillgängliggörande för vidareutnyttjande av skyddade data. Myndigheten ska i sådana fall inte behöva efterforska syftet med begäran.

### 5.3 Vidareutnyttjande av skyddade data förutsätter att informationen kan lämnas ut

**Regeringens förslag:** Bestämmelserna om tillgängliggörande av skyddade data för vidareutnyttjande ska tillämpas när någon som har rätt att få tillgång till skyddade data enligt någon annan lag eller förordning begär att dessa data ska tillgängliggöras för vidareutnyttjande. Bestämmelserna ska också tillämpas när en myndighet på eget initiativ tillgängliggör skyddade data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för inno-*

vationssystem, Växjö kommun och Åklagarmyndigheten tillstyrker eller har inga synpunkter på förslaget.

*Myndigheten för digital förvaltning* anser att det bör klargöras hur rätten att få tillgång till data enligt öppna datalagen förhåller sig till Högsta domstolens avgörande NJA 2023 s. 498. Det bör enligt myndigheten även klargöras hur bestämmelserna i 2 kap. 1 § öppna datalagen om att göra data tillgänglig för vidareutnyttjande efter en begäran förhåller sig till EU:s dataförvaltningsförordning, som inte medför någon motsvarande skyldighet för myndigheter att tillgängliggöra data. Myndigheten anser vidare att det saknas en analys av om rätten att få tillgång till skyddade data även omfattar offentliga myndigheters skyldigheter att försörja med information enligt t.ex. vissa registerförfattningar.

*Bolagsverket* ifrågasätter bedömningen att vidareutnyttjande av skyddade data förutsätter att informationen kan lämnas ut enligt annan lagstiftning. Uppgifter som maskerats på grund av sekretess kan enligt myndigheten inte anses utlämnade. Om den som begärt ut uppgifterna samtidigt framställer en begäran om tillgängliggörande för vidareutnyttjande riskerar de nya föreslagna bestämmelserna enligt myndigheten att tolkas så att uppgifterna ska lämnas ut med hjälp av de metoder som räknas upp i artikel 5.3 i EU:s dataförvaltningsförordning, vilket inte är avsikten med förordningen.

### **Skälen för regeringens förslag**

*I vilka situationer ska öppna datalagen tillämpas för skyddade data?*

Bestämmelserna i kapitel II i EU:s dataförvaltningsförordning ger inte en rätt att få tillgång till skyddade data för vidareutnyttjande, utan de syftar till att ge en uppsättning harmoniserade regler om under vilka förutsättningar vidareutnyttjande av sådan data kan tillåtas. Rätten att vidareutnyttja data, och begränsningar i denna rätt, följer i stället av medlemsstaternas nationella rätt. EU:s dataförvaltningsförordning påverkar, till skillnad från vad *Bolagsverket* anför, inte dessa regler (se artikel 1.2). Innan frågan om tillgängliggörande av skyddade data för vidareutnyttjande kan behandlas måste alltså först frågan om rätten till tillgång till informationen hanteras, bl.a. enligt bestämmelserna i tryckfrihetsförordningen, offentlighets- och sekretesslagen och andra författningar som reglerar tillgången till information. På samma sätt är regelverket om vidareutnyttjande av data enligt öppna datalagen uppbyggt. Av 1 kap. 8 § öppna datalagen framgår bl.a. att lagen ska tillämpas när någon som har rätt att få tillgång till data enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande. Öppna datalagen ska alltså tillämpas först när det har konstaterats att det finns en författningsreglerad rätt till tillgång och att det inte finns några hinder mot att ge tillgång till de data som efterfrågas (prop. 2021/22:225 s. 29 och 78).

Bestämmelserna i tryckfrihetsförordningen ger dock inte någon rätt att ta del av information i något visst format. En myndighet är nämligen inte skyldig att i större utsträckning än vad som följer av lag lämna ut en upptagning för automatiserad behandling i annan form än utskrift, det s.k. utskriftsundantaget (2 kap. 16 § TF). Högsta domstolen har uttalat att öppna datalagen inte påverkar den begränsning av rätten till tillgång till uppgifter

i digital form som följer av utskriftsundantaget (se NJA 2023 s. 498). Som *Myndigheten för digital förvaltning* efterfrågar innebär det i praktiken att tryckfrihetsförordningen inte kommer att grunda någon rätt för enskilda att få tillgång till data för vidareutnyttjande. Den rätten behöver i stället grunda sig på någon annan lag för att aktualisera bestämmelserna i 1 kap. 8 § första stycket öppna datalagen. Sådan unionslagstiftning planeras nu inom t.ex. hälsodataområdet (se COM (2022) 66). Bestämmelserna i 1 kap. 8 § första stycket 1 öppna datalagen kommer således fortfarande att vara aktuella i olika situationer. Eftersom EU:s dataförvaltningsförordning, på samma sätt som öppna datalagen, förutsätter att det finns en rätt att få tillgång till data enligt annan lagstiftning bör samma princip gälla vid en begäran om tillgängliggörande av skyddade data för vidareutnyttjande.

Även om tryckfrihetsförordningen inte innebär någon skyldighet för myndigheter att lämna ut information i ett visst format innebär utskriftsundantaget inte något hinder för myndigheter att göra det. En myndighet eller ett offentligt företag kan också på eget initiativ göra data tillgängliga för vidareutnyttjande. Öppna datalagen innehåller därför en bestämmelse i 1 kap. 8 § 2 om att lagen ska tillämpas när en myndighet eller ett offentligt företag på eget initiativ ger tillgång till data som omfattas av lagen, i syfte att de ska kunna vidareutnyttjas (prop. 2021/22:225 s. 30 och 78). En sådan möjlighet bör även finnas för skyddade data.

Sammanfattningsvis bör öppna datalagen tillämpas antingen om myndigheter gör skyddade data tillgängliga för vidareutnyttjande på frivillig väg eller om det finns en rätt att få tillgång till skyddade data enligt annan lagstiftning. Det senare gäller all lagstiftning som grundar en sådan rätt. I likhet med vad *Myndigheten för digital förvaltning* påpekar gäller det alltså även sådana lagstadgade skyldigheter för myndigheter att försörja med information. Eftersom öppna datalagen ska tillämpas först när det har konstaterats att det finns en författningsreglerad rätt till tillgång och det inte finns några hinder mot att ge tillgång till de data som efterfrågas bör det inte, som Bolagsverket befarar, finnas någon risk för att data lämnas ut i strid med t.ex. tryckfrihetsförordningen eller offentlighets- och sekretesslagen.

Bestämmelserna i 1 kap. 8 § första stycket 2 öppna datalagen innebär att lagen är tillämplig när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data. Motsvarande bestämmelser bör införas även för skyddade data. Bestämmelserna bör dock inte gälla offentliga företag, eftersom de föreslagna bestämmelserna om tillgängliggörande av skyddade data för vidareutnyttjande endast ska gälla för myndigheter (se avsnitt 5.1).

*Myndigheten för digital förvaltning* framför att det bör klargöras om 2 kap. 1 § öppna datalagen är tänkt att gälla för skyddade data. I promemorian föreslås inte att 2 kap. 1 § öppna datalagen ska gälla för skyddade data. Eftersom det inte bör införas en skyldighet för myndigheter att tillgängliggöra skyddade data anser regeringen inte heller att det finns skäl att lämna något sådant förslag.



## 5.4 Exklusiva avtal och villkor för vidareutnyttjande av skyddade data

**Regeringens förslag:** Exklusiva avtal om vidareutnyttjande av skyddade data ska vara förbjudna om det inte är tillåtet enligt EU:s dataförvaltningsförordning.

En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska ställa upp villkor för vidareutnyttjandet i enlighet med artikel 5 i EU:s dataförvaltningsförordning.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Luleå, Förvaltningsrätten i Stockholm, Konsumentverket, Kungliga biblioteket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Bolagsverket* anför att den föreslagna bestämmelsen är obehövlig eftersom det redan följer av EU:s dataförvaltningsförordning vad som gäller för exklusiva avtal. Enligt myndigheten bör det däremot införas en bestämmelse som anger under vilka förutsättningar en myndighet får eller ska ändra skyddade data i syfte att med bibehållet skydd kunna tillgängliggöra data för vidareutnyttjande. Bestämmelsen bör utformas med artikel 5.1 i öppna datadirektivet som förebild.

**Skälen för regeringens förslag:** Både öppna datalagen och EU:s dataförvaltningsförordning innehåller bestämmelser om begränsningar avseende exklusiva avtal om vidareutnyttjande av data. Bestämmelserna i de olika rättsakterna är mycket snarlika. Utgångspunkten är att exklusiva avtal inte är tillåtna, utom när det är nödvändigt för att en tjänst av allmänt intresse ska kunna tillhandahållas (jfr artikel 12.2 i öppna datadirektivet, 3 kap. 1 § öppna datalagen och artikel 4.1 och 4.2 i EU:s dataförvaltningsförordning).

En EU-förordning är direkt tillämplig i varje medlemsstat. Det innebär att en sådan rättsakt som utgångspunkt inte bör inkorporeras i eller transformerar till nationell rätt. Gränserna för vad som är tillåtet när det kommer till exklusiva avtal för kategorier av data som omfattas av artikel 3.1 i EU:s dataförvaltningsförordning följer direkt av artikel 4 i samma förordning. Det behövs därför inte någon kompletterande nationell reglering för exklusiva avtal avseende skyddade data motsvarande den som finns i öppna datalagen. Däremot bör det, som det föreslås i promemorian, införas en bestämmelse av upplysningskaraktär som hänvisar till artikel 4 i EU:s dataförvaltningsförordning. En sådan bestämmelse är enligt regeringens mening, till skillnad från vad *Bolagsverket* anför, inte obehövlig. Detta för att det ska vara tydligt att det finns särskilda bestämmelser avseende exklusiva avtal för skyddade data.

Det bör också införas en bestämmelse av upplysningskaraktär som hänvisar till artikel 5 i EU:s dataförvaltningsförordning om att en myndighet som tillgängliggör skyddade data för vidareutnyttjande ska

ställa upp villkor för vidareutnyttjandet i enlighet med den artikeln. Av artikel 5 följer bl.a. att tillgängliggörande myndigheter ska säkerställa att uppgifternas skyddade karaktär bevaras och att myndigheten för att göra det kan föreskriva vissa krav enligt artikeln. Villkoren för vidareutnyttjande ska vara icke-diskriminerande, transparenta, proportionerliga och objektivt motiverade med hänsyn till kategorierna av data, vidareutnyttjandets syfte och typerna av data för vilka vidareutnyttjande tillåts. Villkoren får inte användas för att begränsa konkurrensen. Eftersom det följer direkt av artikel 5 i EU:s dataförvaltningsförordning under vilka förutsättningar en myndighet får eller ska ändra skyddade data i syfte att med bibehållet skydd kunna tillgängliggöra data för vidareutnyttjande bör en sådan bestämmelse, till skillnad från vad Bolagsverket anför, inte införas i nationell rätt.

## 5.5 Anmälan av överträdelser som en vidareutnyttjare gör sig skyldig till vid tredjelandsoverföringar

**Regeringens förslag:** En myndighet som överfört skyddade data till en vidareutnyttjare som avser att överföra dessa till ett tredjeland ska anmäla överträdelser av EU:s dataförvaltningsförordnings villkor för tredjelandsoverföringar som vidareutnyttjaren har gjort sig skyldig till. Anmälan ska göras till den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen*, *E-hälsomyndigheten*, *Försvarets materielverk*, *Förvaltningsrätten i Stockholm*, *Konsumentverket*, *Läkemedelsverket*, *Malmö kommun*, *Patent- och registreringsverket*, *Pensionsmyndigheten*, *Polismyndigheten*, *Region Östergötland*, *Socialstyrelsen*, *Säkerhetspolisen*, *Verket för innovationssystem*, *Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Stockholms kommun* anser att anmälningsplikten kan vara utmanande att uppfylla. *Post- och telestyrelsen (PTS)* anser att det bör framgå direkt av lag vad en anmälan ska innehålla.

**Skälen för regeringens förslag:** Enligt artikel 5.10 i EU:s dataförvaltningsförordning får en myndighet under vissa förutsättningar överföra skyddade data som inte är personuppgifter (s.k. icke-personuppgifter enligt förordningen) eller immaterialrättsligt skyddat material till en vidareutnyttjare som avser att föra ut dessa till ett tredjeland.

Om en myndighet medger tillgång till skyddade data till en vidareutnyttjare som avser att överföra uppgifterna till ett tredjeland ska myndigheten enligt artikel 5.10 ställa upp vissa villkor för tillgängliggörandet. Den som beviljas rätt att vidareutnyttja sådan data får i sin tur överföra dessa till ett tredjeland bara om vissa krav enligt EU:s dataförvaltningsförordning är uppfyllda (se artikel 5.14 som hänvisar till artiklarna 5.10, 5.12 och 5.13). Om en vidareutnyttjare bryter mot kraven ska vidareutnyttjaren kunna träffas av en sanktion (artikel 34). Sanktionen

bör beslutas av den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer som regeringen utser (se avsnitt 6.2).

För att den behöriga myndigheten ska kunna besluta om sanktioner behöver den få kännedom om överträdelser enligt artikel 5.14. Den myndighet som har störst möjlighet att få kännedom om sådana överträdelser är den som har lämnat ut datan. Utlämnande myndighet bör därför ha en skyldighet att anmäla överträdelser av artikel 5.14 till den behöriga myndigheten.

En anmälan bör innehålla de uppgifter om överträdelserna som den behöriga myndigheten behöver för att kunna besluta om sanktioner. Det kan t.ex. vara uppgifter om vidareutnyttjaren, en beskrivning av de data som lämnats ut, vilka villkor som ställts upp för vidareutnyttjandet och överföringen till tredje land, en redogörelse för den eller de överträdelser som vidareutnyttjaren gjort sig skyldig till samt vilka effekter överträdelserna fått. Även uppgifter om hur överträdelserna upptäcktes, hur allvarlig den bedöms vara, vilken omfattning den har och under hur lång tid den pågått bör anges. Om myndigheten har kännedom om tidigare överträdelser som vidareutnyttjaren gjort sig skyldig till bör det också framgå. Likaså uppgifter om de ekonomiska vinster som överträdelserna inneburit för vidareutnyttjaren. Myndigheten kan därutöver inkludera andra försvårande eller förmildrande omständigheter som kan ha betydelse för bedömningen av en sanktionsavgift. Det går inte att uttömmande ange vilka uppgifter som den behöriga myndigheten kan behöva och som bör framgå av anmälan. Regeringen anser därför, till skillnad från *PTS*, att det inte bör preciseras i lag.

*Stockholms kommun* framför att anmälningsplikten kan vara svår att uppfylla. Anmälningsplikten innebär emellertid inte något tillsynsansvar. Den myndighet som lämnat ut data har endast en skyldighet att anmäla de överträdelser av artikel 5.14 som myndigheten får kännedom om. Uppgiften bör således inte vara särskilt betungande.

## 5.6 En avgift ska kunna tas ut för vidareutnyttjande av skyddade data

**Regeringens förslag:** Myndigheter som tillåter vidareutnyttjande av skyddade data ska få ta ut en avgift av vidareutnyttjaren för tillhandahållande av skyddade data.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om avgiften.

**Regeringens bedömning:** Några undantag från avgiftsskyldigheten för vidareutnyttjande av skyddade data bör inte införas.

**Promemorians förslag och bedömning** överensstämmer delvis med regeringens. I promemorian föreslås att beräkningsgrunderna för avgiften ska framgå av öppna datalagen. I promemorian föreslås inte något bemyndigande för regeringen att meddela föreskrifter om avgiften.

**Remissinstanserna:** Samtliga remissinstanser tillstyrker eller har inga synpunkter på förslaget.

## Skälen för regeringens förslag och bedömning

*Myndigheter ska ha möjlighet att ta ut en avgift för tillgängliggörande av skyddade data för vidareutnyttjande*

Myndigheter som tillåter vidareutnyttjande av skyddade data enligt EU:s dataförvaltningsförordning får ta ut en avgift för det. Avgifter som tas ut ska vara transparenta, icke-diskriminerande, proportionella och objektivt motiverade och får inte begränsa konkurrensen (artikel 6.1 och 6.2).

Den som vill ta del av en allmän handling har enligt 2 kap. 16 § TF rätt att mot avgift få en avskrift eller kopia av handlingen. För statliga myndigheter regleras den avgiften i avgiftsförordningen (1992:191). Avgiftsförordningen innehåller fastställda avgifter som ska tillämpas när allmänna handlingar tillhandahålls i pappersform. Motsvarande reglering saknas när information tillhandahålls i elektronisk form. Det behövs mot denna bakgrund införas särskilda bestämmelser för uttag av avgifter för tillhandahållande av skyddade data för vidareutnyttjande.

### *Avgiftens storlek*

Kriterierna och metoden för beräkning av avgifter för vidareutnyttjande av skyddade data ska fastställas av medlemsstaterna och offentliggöras (artikel 6.6 i EU:s dataförvaltningsförordning). Avgifterna ska enligt artikel 6.5 härledas från kostnaderna för att genomföra förfarandet för begäran om vidareutnyttjande, och de ska vara begränsade till nödvändiga kostnader i samband med

- reproduktion, tillhandahållande och spridning av data,
- klarering av upphovsrätt,
- anonymisering eller andra former av framställning av personuppgifter och affärshemligheter,
- underhåll av den säkra behandlingsmiljön,
- förvärvande av rätten från tredje part att tillåta vidareutnyttjande, och
- visst bistånd till vidareutnyttjare.

I promemorian föreslås att beräkningsgrunden för avgiften dels ska följa bestämmelserna i 4 kap. 2 § öppna datalagen, dels artikel 6.5 i EU:s dataförvaltningsförordning. Några av de kostnader som räknas upp i artikel 6.5 anges nämligen även i 4 kap. 2 § öppna datalagen. Samtliga kostnader som får ligga till grund för avgiften framgår dock av artikel 6.5 i EU:s dataförvaltningsförordning. Regeringen anser mot denna bakgrund att det saknas anledning att, som det föreslås i promemorian, både hänvisa till 4 kap. 2 § öppna datalagen och EU:s dataförvaltningsförordning för att ange beräkningsgrunderna för avgiften för tillgängliggörande av skyddade data. De kostnader som kan läggas till grund för avgiften behöver inte heller framgå direkt av lag, eftersom de redan följer av EU-förordningen. Regeringen eller den myndighet som regeringen bestämmer bör dock få meddela föreskrifter om avgiften, t.ex. om avgiftens storlek utifrån de kostnader som är tillåtna enligt EU:s dataförvaltningsförordning.

### *Det bör inte införas några undantag från avgiftsuttag*

I promemorian görs bedömningen att det inte ska införas något undantag från avgiftsuttag enligt artikel 6.4 i EU:s dataförvaltningsförordning. När

offentliga myndigheter tar ut avgifter ska de vidta åtgärder för att ge incitament till vidareutnyttjande av de kategorier av data som avses i artikel 3.1 för icke-kommersiella ändamål, såsom vetenskaplig forskning, och av små och medelstora företag och uppstarts företag i enlighet med reglerna för statligt stöd. I detta avseende får de offentliga myndigheterna också göra dessa data tillgängliga till en nedsatt avgift eller kostnadsfritt, särskilt för små och medelstora företag och uppstarts företag, det civila samhället och utbildningsanstalter.

Öppna datadirektivet uppställer ett krav på att forskningsdata ska göras tillgänglig avgiftsfritt (artikel 6.6 b). Bestämmelsen har införlivats i öppna datalagen (4 kap. 3 §). Även vissa andra typer av data, en s.k. värdefull datamängd, ska tillgängliggöras avgiftsfritt enligt öppna datalagen (4 kap. 4 §). Syftet med tillhandahållande av data avgiftsfritt är att motverka att avgiftsuttag blir ett betydande hinder för vidareutnyttjande av data, i synnerhet för nystartade eller små och medelstora företag (jfr skäl 36 till öppna datadirektivet). Bestämmelserna i artikel 6.4 i EU:s dataförvaltningsförordning om tillgängliggörande av data till en nedsatt avgift eller kostnadsfritt bygger på en liknande tanke. Detta talar enligt regeringens mening för att det ska vara möjligt att i vissa fall kunna sätta ned avgiften eller låta den utgå helt. Samtidigt är avgifter ett viktigt sätt för myndigheter att täcka kostnader som uppstår i samband med tillgängliggörande av skyddade data. Om möjligheten att ta ut avgifter i vissa fall begränsas skulle det kunna få den effekten att skyddade data inte tillgängliggörs i samma utsträckning som vid full kostnadstäckning. Eftersom det ännu inte finns någon marknad för vidareutnyttjande av skyddade data är det också svårt att bedöma konsekvenserna av att införa en möjlighet att tillgängliggöra skyddade data till en nedsatt avgift eller avgiftsfritt. Regeringen delar därför bedömningen i promemorian att det för närvarande inte bör införas någon sådan möjlighet.

## 5.7 Handläggningstiden för ärenden om vidareutnyttjande

**Regeringens förslag:** Handläggningstiden för ärenden som avser en begäran om tillgängliggörande av skyddade data för vidareutnyttjande ska uppgå till högst åtta veckor. Vid omfattande och komplicerade begäranden om vidareutnyttjande får handläggningstiden förlängas med ytterligare fyra veckor.

**Regeringens bedömning:** Det behöver inte införas några särskilda överklagandebestämmelser för ärenden om tillgängliggörande av skyddade data för vidareutnyttjande.

**Promemorians förslag och bedömning** överensstämmer i sak med regeringens. I promemorian görs dock inget förtydligande om att möjligheten att förlänga handläggningstiden även gäller skyddade data.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läke medelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polis myndigheten,*

Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun och Åklagarmyndigheten tillstyrker eller har inga synpunkter på förslaget.

*Lantmäteriet* anser att den förlängda tidsfristen för handläggning bör stå i proportion till den ursprungliga handläggningstiden och lämpligen uppgå till ca sex veckor. *Bolagsverket* anser att det inte behövs någon bestämmelse om handläggningstiden, eftersom det följer direkt av EU:s dataförvaltningsförordning.

*Försäkringskassan* anser att det är otydligt om överklagandemöjligheten är tänkt att gälla endast de som träffas direkt av ett beslut eller även de som påverkas indirekt. *Göteborgs kommun* lyfter att det finns risker med att ett överklagande av ett beslut om tillgängliggörande av skyddade data kan komma att prövas parallellt i olika instanser samt att kretsen klagoberättigade kan skilja sig åt i de olika förfarandena.

## Skälen för regeringens förslag och bedömning

### *Handläggningstiden för ärenden om vidareutnyttjande*

En EU-förordning är direkt tillämplig i varje medlemsstat (se avsnitt 5.4). En sådan rättsakt bör som utgångspunkt inte inkorporeras i eller transformeras till nationell rätt, eftersom några särskilda åtgärder för att införliva en förordning generellt sett inte får vidtas. Detta gäller dock inte om förordningen föreskriver att medlemsstaterna behöver genomföra den i nationell rätt.

Av artikel 9.1 i EU:s dataförvaltningsförordning framgår att behöriga myndigheter eller organ ska besluta i ett ärende om begäran om vidareutnyttjande av skyddade data inom två månader från dagen för mottagandet av begäran, såvida inte kortare tidsfrister fastställs i nationell rätt. Vid exceptionellt omfattande och komplicerade begäranden om vidareutnyttjande får tvåmånadersperioden förlängas med högst 30 dagar. EU:s dataförvaltningsförordning föreskriver inte att medlemsstaterna behöver införa bestämmelser om handläggningstiden för ärenden om begäran om vidareutnyttjande, om det inte ska införas kortare tidsfrister än de som föreskrivs i förordningen. Det är inte möjligt att, som *Lantmäteriet* efterfrågar, införa längre handläggningstider i nationell rätt än de som EU:s dataförvaltningsförordning föreskriver.

I öppna datalagen finns bestämmelser om handläggningstiden för ärenden om tillgängliggörande av data för vidareutnyttjande (5 kap. 1 §). Ett sådant ärende ska avgöras inom fyra veckor. Vid en begäran om tillgängliggörande av skyddade data för vidareutnyttjande behöver myndigheten bl.a. ta ställning till eventuella villkor för tillgängliggörandet och säkerställa att uppgifternas skyddade karaktär bevaras (artikel 5 i EU:s dataförvaltningsförordning). Eftersom en sådan begäran i många fall kommer att avse känsliga uppgifter kan det antas att ett ärende om tillgängliggörande av skyddade data för vidareutnyttjande kommer att vara mer komplicerat och resurskrävande än ett ärende om tillgängliggörande av data. Handläggningstiden vad gäller skyddade data bör därför tillåtas vara längre än de fyra veckor som gäller enligt öppna datalagen. I promemorian föreslås att handläggningstiden för ärenden om skyddade data ska uppgå till som längst åtta veckor. Det är en något kortare handläggningstid än den längsta tillåtna i EU:s dataförvaltningsförordning

(artikel 9.1). Enligt regeringen är den föreslagna handläggningstiden väl avvägd. Eftersom denna tid understiger den som anges i EU:s dataförvaltningsförordning behöver det, till skillnad från vad *Bolagsverket* anför, införas nationella bestämmelser om handläggningstiden för ärenden om vidareutnyttjande av skyddade data. Regeringen anser vidare att bestämmelserna i 5 kap. 1 § andra stycket öppna datalagen om möjligheten att förlänga handläggningstiden om en begäran är omfattande eller komplicerad även bör gälla i ärenden om tillgängliggörande av skyddade data för vidareutnyttjande. Ett sådant förtydligande bör därför göras i bestämmelserna i 5 kap. 1 § tredje stycket.

### *Öppna datalagens bestämmelser om överklagande tillgodoser EU:s dataförvaltningsförordnings krav på rättsmedel*

Av artikel 9.2 i EU:s dataförvaltningsförordning följer att fysiska eller juridiska personer som direkt påverkas av ett beslut efter en begäran om vidareutnyttjande av skyddade data ska ha en effektiv rätt till överprövning. Beslut enligt öppna datalagen får överklagas enligt bestämmelserna i 5 kap. 4 §. Bestämmelserna om överklagande i 5 kap. 4 § träffar alla beslut enligt öppna datalagen och kommer därmed även att omfatta beslut om skyddade data om sådana ärenden förs in i lagen enligt förslaget. Regeringen bedömer att överklagandebestämmelsen i öppna datalagen tillgodoser de krav på rättsmedel som EU:s dataförvaltningsförordning föreskriver.

Enligt *Försäkringskassan* är det otydligt om överklagandebestämmelsen i öppna datalagen gäller endast för de som träffas direkt av ett beslut eller även de som träffas indirekt. *Göteborgs kommun* framför liknande synpunkter. Kretsen klagoberättigade följer av 42 § förvaltningslagen (2017:900) och av den rättspraxis som utvecklats på området. Det är således upp till rättstillämparen att avgöra vem som får överklaga ett beslut enligt öppna datalagen.

Göteborgs kommun anser också att det finns risk för parallella processer i olika instanser. Problematiken med en prövning i olika instanser vid överklagande av en begäran om tillgång och en begäran om tillgängliggörande av data för vidareutnyttjande i samma ärende behandlades i propositionen till öppna datalagen. Regeringen bedömde då att övervägande skäl talade för att förvaltningsrätten bör vara första överklagandeinstans i en prövning av ett beslut om att avslå en begäran om tillgängliggörande av data för vidareutnyttjande trots att det emellanåt kan vara förenat med viss svårighet för en enskild att hantera två samtidiga men separata prövningar i olika instanser (prop. 2021/22:225 s. 59). Enligt regeringen saknas det skäl att nu göra en annan bedömning.

## 5.8 Behöriga organ

<p><b>Regeringens förslag:</b> Den eller de myndigheter som regeringen bestämmer ska vara behöriga organ enligt EU:s dataförvaltningsförordning.</p>
--

**Promemorians bedömning** överensstämmer i sak med regeringens förslag. I promemorian föreslås inte något uttryckligt bemyndigande för regeringen att utse behöriga organ.

**Remissinstanserna:** Ingen remissinstans yttrar sig särskilt över att regeringen ska få utse behöriga organ. *Statistiska centralbyrån (SCB)* anser att det bör framgå av såväl lag som förordning vilka myndigheter som utses till behöriga organ.

**Skälen för regeringens förslag:** Varje medlemsstat ska enligt artikel 7 i EU:s dataförvaltningsförordning utse ett eller flera behöriga organ. Ett behörigt organ ska bistå de offentliga myndigheter som beviljar eller vägrar tillgång till skyddade data för vidareutnyttjande. Behöriga organ får också ges befogenhet att bevilja tillgång till vidareutnyttjande. Det bistånd som behöriga organ ska ge till de offentliga myndigheterna förtydligas i artikel 7.4. Det avser bl.a. tekniskt stöd, vägledning och rättsligt bistånd. De behöriga organen måste alltså ha juridiska, ekonomiska och tekniska resurser för att kunna uppfylla uppdraget.

I promemorian redovisas att det har undersökts i vilken utsträckning myndigheter innehar data som skulle kunna omfattas av EU:s dataförvaltningsförordnings tillämpningsområde. De tillfrågade myndigheterna bedömer att regelverket endast kommer att bli tillämpligt i enstaka fall. Uppgiften som behörigt organ bedöms därför i ett inledande skede inte bli särskilt omfattande. Detta talar för att det inte behöver inrättas en ny myndighet för uppgiften utan att uppgiften kan fördelas till en eller flera befintliga myndigheter, som utses av regeringen. I promemorian föreslås att Myndigheten för digital förvaltning och SCB ska utses till behöriga organ. Till skillnad från vad *SCB* anför anser regeringen att det är tillräckligt att det anges i lagen att regeringen bestämmer vilka myndigheter som ska vara behöriga organ.

I promemorian görs bedömningen att behöriga organ inte bör ges befogenhet att bevilja tillgång till skyddade data för andra offentliga myndigheters räkning. Regeringen gör för närvarande samma bedömning, men utesluter inte att det i framtiden kan vara aktuellt att överlåta en sådan uppgift till det eller de behöriga organ som utses.

I promemorian görs också bedömningen att behöriga organ inom olika sektorer bör införas på sikt och att frågan behöver utredas. De behöriga organens uppgifter bedöms samtidigt inte bli särskilt omfattande. Detta talar enligt regeringens mening snarare för att det är tillräckligt att utse en eller högst två myndigheter till behöriga organ. Det bedöms därför i nuläget inte vara aktuellt att utreda frågan.

## 5.9 Den gemensamma informationspunkten

**Regeringens förslag:** Den myndighet som regeringen bestämmer ska vara gemensam informationspunkt enligt EU:s dataförvaltningsförordning.

Myndigheter som tillgängliggör skyddade data för vidareutnyttjande ska informera den gemensamma informationspunkten om vilken data som de tillgängliggjort.



**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läke medelsverket, Malmö kommun, Pensionsmyndigheten, Polismyndigheten, Patent- och registreringsverket, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagar myndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Region Skåne* framför att det inte är tydligt vilka krav EU:s dataförvaltningsförordning ställer för den gemensamma informationspunkten beträffande olika dataområden. Regionen anser också att det är oklart vad det är för information som myndigheterna ska informera den gemensamma informationspunkten om.

## **Skälen för regeringens förslag**

### *Gemensamma informationspunkter*

Enligt artikel 8 i EU:s dataförvaltningsförordning ska medlemsstaterna säkerställa att all relevant information om tillämpningen av artiklarna 5 och 6, som avser villkor för vidareutnyttjande och avgifter, finns tillgänglig och lätt åtkomlig via en s.k. gemensam informationspunkt. Medlemsstaterna ska också inrätta ett nytt organ eller utse ett befintligt organ till gemensam informationspunkt. EU:s dataförvaltningsförordning använder alltså uttrycket gemensam informationspunkt dels för att beskriva ett gränssnitt som ska underlätta att vidareutnyttja data, dels om det organ som ska tillhandahålla den gemensamma informationspunkten. Regeringen bör bestämma vilken myndighet som ska vara gemensam informationspunkt.

I den gemensamma informationspunkten ska det finnas en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor tillsammans med relevant information som beskriver tillgängliga data samt villkoren för vidareutnyttjandet av dessa. Den gemensamma informationspunkten ska också kunna ta emot förfrågningar eller ansökningar om vidareutnyttjande av skyddade data och vidareförmedla dessa till de myndigheter som innehar aktuella data (artikel 8.2).

Europeiska kommissionen ska i sin tur inrätta en europeisk gemensam åtkomstpunkt som erbjuder ett sökbart elektroniskt register över tillgängliga data i nationella gemensamma informationspunkter och ytterligare information om hur man begär data via dessa nationella gemensamma informationspunkter (artikel 8.4).

### *Uppgifter som ska finnas i den gemensamma informationspunkten*

I den gemensamma informationspunkten ska en sökbar tillgångsförteckning tillhandahållas på elektronisk väg. I den ska en översikt över alla tillgängliga datakällor finnas tillsammans med relevant information som beskriver alla tillgängliga datakällor, inbegripet åtminstone dataformatet och datastorleken samt villkoren för vidareutnyttjande av dessa (artikel 8.2 i EU:s dataförvaltningsförordning).

För att den myndighet som tillhandahåller den gemensamma informationspunkten ska kunna tillhandahålla en sådan tillgångsförteckning behöver myndigheter som tillgängliggör data för vidareutnyttjande förse den

gemensamma informationspunkten med relevant information. Det bör därför införas en skyldighet för myndigheter att underrätta den gemensamma informationspunkten om de skyddade data som gjorts tillgängliga för vidareutnyttjande. Myndigheten ska också ge annan relevant information om dessa data, i enlighet med artikel 8.2 i EU:s dataförvaltningsförordning. En bestämmelse med en sådan skyldighet, som hänvisar till EU:s dataförvaltningsförordning, bör införas i öppna datalagen. På så sätt bör de eventuella otydligheter som skyldigheten innebär, och som *Region Skåne* befarar, i princip undanröjas. Det är sedan en uppgift för rättstillämparen att närmare förtydliga innebörden av skyldigheten.

## 6 Dataförmedling och dataaltruism

### 6.1 Bestämmelser om dataförmedlingstjänster och dataaltruismorganisationer

**Regeringens förslag:** Det ska införas nationella bestämmelser om dataförmedlingstjänster och dataaltruismorganisationer. Ord och uttryck i den nationella lagstiftningen ska ha samma betydelse som i EU:s dataförvaltningsförordning.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen*, *E-hälsomyndigheten*, *Försvarets materielverk*, *Förvaltningsrätten i Stockholm*, *Konsumentverket*, *Läkemedelsverket*, *Malmö kommun*, *Patent- och registreringsverket*, *Pensionsmyndigheten*, *Polismyndigheten*, *Region Östergötland*, *Socialstyrelsen*, *Säkerhetspolisen*, *Verket för innovationssystem*, *Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Försvarsmakten* anser att myndighetens verksamhet inte ska omfattas av EU:s dataförvaltningsförordning, eftersom försvars- och säkerhetsområdet ligger utanför EU:s kompetens. Myndighetens verksamhet bör därför enligt myndigheten uttryckligen undantas från kompletteringslagens tillämpningsområde. Enligt *Sveriges advokatsamfund* saknas det i den föreslagna kompletteringslagens bestämmelser om att den allmänna dataskyddsförordningen och nationella bestämmelser om dataskydd har företräde framför EU:s dataförvaltningsförordning och kompletteringslagen.

**Skälen för regeringens förslag:** EU:s dataförvaltningsförordnings kapitel III och IV har en delvis annan struktur och innehåll än kapitel II. Även bestämmelserna i dessa kapitel syftar till att öka tillgängligheten och användningen av data, men handlar i stället om att reglera formerna för hur vissa aktörer som tillgängliggör data ska få bedriva sin verksamhet. I kapitel III finns en uppsättning bestämmelser för leverantörer av dataförmedlingstjänster, s.k. dataförmedlare. Syftet med dessa bestämmelser är att öka förtroendet för dataförmedlare, genom att få dem att agera som neutrala parter i förhållanden till den data de tillgängliggör. Detta genom att de inte själva ska få använda den data som de förmedlar för att generera

vinst, t.ex. genom att sälja den till ett annat företag. Bakgrunden till bestämmelserna är att minska de farhågor som finns hos framför allt företag att dela sin data för att det skulle kunna innebära nackdelar i konkurrens-hänseende eller utgöra en risk för missbruk av data.

I kapitel IV i EU:s dataförvaltningsförordning regleras i första hand förutsättningarna för erkännande och registrering av dataaltruismorganisationer. Dataaltruism handlar om att individer och företag på frivillig väg och utan krav på ersättning ger sitt samtycke eller tillåtelse att tillgängliggöra data för att användas i allmänhetens intresse. Dataaltruismorganisationer samlar i sin tur in sådana uppgifter för mål av allmänt intresse, eller för att ge andra fysiska och juridiska personer möjlighet att behandla data för de mål av allmänt intresse för vilka uppgifterna samlades in. Regelverket bygger på att den som delar med sig av sin data kan följa hur uppgifterna används.

EU:s dataförvaltningsförordning ställer krav på att medlemsstaterna inför kompletterande bestämmelser till kapitel III och IV om bl.a. behöriga myndigheter, avgifter, informationsutbyte samt om vissa tillhörande bestämmelser i kapitel V om förfarandet och i kapitel IX om sanktioner. Eftersom regelverket om dataförmedlare och dataaltruismorganisationer skiljer sig åt i struktur och innehåll jämfört med bestämmelserna om vidareutnyttjande av data är det inte lämpligt att införa de kompletterande nationella bestämmelserna om dataförmedlare och dataaltruismorganisationer i öppna datalagen. Det bör i stället regleras i en ny lag. Den nya lagen bör endast utgöra ett komplement till EU:s dataförvaltningsförordning, eftersom förordningen gäller direkt (se t.ex. avsnitt 5.4). Det stora flertalet bestämmelser som ska tillämpas för dataförmedlare och dataaltruismorganisationer finns i EU:s dataförvaltningsförordning.

Den föreslagna kompletteringslagen innehåller bestämmelser om bl.a. behörig myndighet, tillsyn och avgifter. Regeringen bedömer att Försvarsmakten inte omfattas av de föreslagna bestämmelserna. Det saknas därför skäl att, till skillnad från vad *Försvarsmakten* anför, undanta myndigheten från kompletteringslagens tillämpningsområde.

Av artikel 1.3 i EU:s dataförvaltningsförordning framgår bl.a. att förordningen inte påverkar tillämpningen av den allmänna dataskyddsförordningen eller nationell rätt som har antagits i enlighet med unionsrätt om skydd av personuppgifter. Eftersom kompletteringslagen bygger på EU:s dataförvaltningsförordning anser regeringen, till skillnad från *Sveriges advokatsamfund*, att det inte behövs några särskilda bestämmelser i kompletteringslagen om att den allmänna dataskyddsförordningen, eller kompletterande nationella bestämmelser till skydd av personuppgifter, har företräde framför EU:s dataförvaltningsförordning eller kompletteringslagen. Den allmänna dataskyddsförordningen gäller vidare direkt i svensk rätt och ska tillämpas av myndigheter vid behandling av personuppgifter.

Hänvisningar till EU:s dataförvaltningsförordning i kompletteringslagen bör vara utformade på så sätt att de avser förordningen i den vid varje tidpunkt gällande lydelsen, s.k. dynamisk hänvisning. Förordningen kan då ändras utan att de kompletterande nationella bestämmelserna behöver justeras.

## 6.2 Behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer

**Regeringens förslag:** Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet. Tillsynsmyndigheten ska vara behörig myndighet för leverantörer av dataförmedlingstjänster och dataaltruismorganisationer.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

### Skälen för regeringens förslag

#### *Behörig myndighet för leverantörer av dataförmedlingstjänster*

Varje medlemsstat ska utse en eller flera behöriga myndigheter för att utföra uppgifter i samband med anmälningsförfarandet för dataförmedlingstjänster (artikel 13). Den behöriga myndigheten ska på begäran av leverantören av dataförmedlingstjänster inom en vecka från det att en komplett anmälan inkom utfärda en standardiserad förklaring som bekräftar att leverantören inkommit med en anmälan (artikel 11.8). Den behöriga myndigheten ska vidare underrätta kommissionen på elektronisk väg om varje ny anmälan (artikel 11.10). Myndigheten ska utöva tillsyn och inom ramen för den ha befogenheter att besluta om ekonomiska sanktioner (artikel 14). Myndighetens jurisdiktion, dvs. vilka leverantörer av dataförmedlingstjänster som myndigheten ska registrera och därmed utöva tillsyn över, följer av EU:s dataförvaltningsförordning (artikel 11.2 och 11.3).

De huvudsakliga uppgifterna för den behöriga myndigheten är att ta emot och bedöma anmälningar samt att utöva tillsyn över leverantörer av dataförmedlingstjänster. Av effektivitetsskäl är det lämpligt att utse en myndighet som redan utför sådana uppgifter så att befintliga system, processer och rutiner kan nyttjas. Den eller de behöriga myndigheterna bör utses av regeringen.

Det följer av EU:s dataförvaltningsförordning att den behöriga myndigheten ska ha ett nära samarbete med Integritetsskyddsmyndigheten, Konkurrensverket och myndigheterna som ansvarar för cybersäkerhet för att utbyta information (artikel 13). Samverkan behöver i det här fallet inte regleras särskilt eftersom det redan följer av bl.a. bestämmelserna i 8 § förvaltningslagen att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter. Däremot kan det finnas fördelar med att utse en myndighet som redan samverkar med dessa myndigheter. Det bör inte krävas en sekretessbrytande bestämmelse i nationell rätt för att myndigheterna inom ramen för ett sådant samarbete ska kunna utbyta sekretessbelagda uppgifter, eftersom grunden för samarbetet följer direkt av EU:s dataförvaltningsförordning (se avsnitt 6.3.5).

Företrädare för den behöriga myndigheten ska vidare ingå i den Europeiska datainnovationsstyrelse som den Europeiska kommissionen ska inrätta (artikel 29). Datainnovationsstyrelsen ska bl.a. rådgöra och bistå kommissionen i utarbetandet av praxis för myndigheter och behöriga organ som ska tillämpa EU:s dataförvaltningsförordning (artikel 30 a).

#### *Behörig myndighet för dataaltruismorganisationer*

Varje medlemsstat ska också utse en eller flera behöriga myndigheter för registrering av dataaltruismorganisationer (artikel 23). Den behöriga myndigheten ska bl.a. hantera ansökningar om registrering från dataaltruismorganisationer, hålla registret uppdaterat (artiklarna 17 och 19) och utöva tillsyn över sådana organisationer (artikel 24). Den behöriga myndigheten ska också ta emot de årliga verksamhetsrapporterna som de erkända dataaltruismorganisationerna ska lämna (artikel 20.2) och underrätta kommissionen om alla registreringar (artikel 19.5). Myndighetens jurisdiktion, dvs. vilka dataaltruismorganisationer som myndigheten ska registrera och därmed utöva tillsyn över, följer av EU:s dataförvaltningsförordning (artikel 19).

#### *Tillsynsmyndigheten bör även vara behörig myndighet för dataförmedlingstjänster och dataaltruismorganisationer*

Uppgifterna för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer får utföras av samma myndighet. Medlemsstaterna får antingen inrätta en eller flera myndigheter eller förlita sig på befintliga myndigheter (artikel 26). Behöriga myndigheter för dataförmedlingstjänster och dataaltruismorganisationer ska båda hantera ansökningar och anmälningar samt utöva tillsyn. Flera av bestämmelserna i EU:s dataförvaltningsförordning som avser de behöriga myndigheterna är dessutom gemensamma (se artiklarna 26, 27 och 28) och båda förfarandena omfattas av Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (artikel 36). Vidare ska den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer representeras i den Europeiska datainnovationsstyrelsen. Mot bakgrund av att uppgifterna för behörig myndighet för leverantörer av dataförmedlingstjänster och för dataaltruismorganisationer är mycket likartade finns det skäl att överväga att inrätta en gemensam behörig myndighet för dessa aktörer. Enligt regeringen bör den myndighet som utses till tillsynsmyndighet enligt kompletteringslagen även vara behörig myndighet enligt EU:s dataförvaltningsförordning. Tillsynsmyndigheten bör utses av regeringen.

## 6.3 Tillsyn och sanktionsavgift

### 6.3.1 Tillsyn

**Regeringens förslag:** Tillsynsmyndigheten ska få meddela de förelägganden som behövs för att EU:s dataförvaltningsförordning, lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning eller de föreskrifter som har meddelats i anslutning till lagen ska följas. Förelägganden enligt artikel 14 i EU:s dataförvaltningsförordning, som riktar sig mot leverantörer av dataförmedlingstjänster, ska få förenas med vite.

Tillsynsmyndigheten ska kunna utfärda en varning till leverantörer av dataförmedlingstjänster för överträdelser av

- anmälningsskyldigheten,
- villkoren för tillhandahållande av dataförmedlingstjänster, och
- villkoren för överföring av andra data än personuppgifter till tredjeland.

Tillsynsmyndigheten ska vidare kunna utfärda en varning till en fysisk eller juridisk person för överträdelser av villkoren för överföring av andra data än personuppgifter till tredjeland.

Tillsynsmyndigheten ska också kunna utfärda en varning till en erkänd dataaltruismorganisation för överträdelser mot villkoren för registrering samt villkoren för överföring av andra data än personuppgifter till tredjeland.

**Promemorians förslag** överensstämmer delvis med regeringens. I promemorian förslås ordet erinran i stället för varning. I promemorian förslås inte att tillsynsmyndigheten ska kunna utfärda en varning till en fysisk eller juridisk person för överträdelser av villkoren för överföring av andra data än personuppgifter till tredjeland.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Sveriges advokatsamfund* anser att möjligheten att besluta om förelägganden och att förena dessa med vite även bör omfatta brott mot artiklarna 5.14 och 31 i EU:s dataförvaltningsförordning. Advokatsamfundet menar vidare att ordet erinran bör ersättas med reprimand för att använda samma definition som i den allmänna dataskyddsförordningen. Den behöriga myndigheten bör också enligt advokatsamfundet ges möjlighet att meddela en reprimand vid brott mot artikel 5.14 i EU:s dataförvaltningsförordning. På så sätt ges den behöriga myndigheten fler verktyg samtidigt som den enskilde kan undgå utfärdande av mer ingripande sanktioner.

Enligt *PTS* bör det övervägas att införa upplysningsbestämmelser för samtliga tillsynsbestämmelser i EU:s dataförvaltningsförordning. Myndigheten anser att tillsynsmyndigheten också bör ges möjlighet att vid vite

förelägga vidareutnyttjare att komma in med uppgifter samt ha befogenhet att vidta fler utredningsåtgärder än vad som följer av förvaltningslagen. Myndigheten anser vidare att det bör förtydligas om ett föreläggande kan beslutas med stöd av artikel 14.4 i EU:s dataförvaltningsförordning och om det i så fall ska föregås av ett meddelande enligt artikel 14.3 eller om det i stället är en begäran enligt artikel 14.2 som får förenas med vite. Artikel 24.5 i EU:s dataförvaltningsförordning bör enligt myndigheten tolkas som att en dataaltruismorganisation ska förlora sin rätt att använda beteckningen så snart villkoren inte längre är uppfyllda, vilket innebär att det inte borde finnas något utrymme att besluta om en erinran i sådana situationer. Slutligen bör det enligt myndigheten förtydligas i vilka situationer en erinran kan bli aktuell och hur sanktionen förhåller sig till den föreslagna möjligheten att avstå från att ta ut en sanktionsavgift.

### **Skälen för regeringens förslag**

*Tillsyn över leverantörer av dataförmedlingstjänster, dataaltruismorganisationer och vidareutnyttjare*

Den behöriga myndigheten ska utöva tillsyn över leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer. Den behöriga myndigheten ska t.ex. enligt artikel 14.2 kunna begära information från leverantörer av dataförmedlingstjänster för att kontrollera uppfyllandet av kraven i EU:s dataförvaltningsförordning. Det finns liknande bestämmelser som tar sikte på dataaltruismorganisationer (artikel 24).

Att ha möjlighet att hämta in uppgifter från leverantörer av dataförmedlingstjänster och dataaltruismorganisationer är ett viktigt redskap i tillsynsarbetet. Regeringen anser att möjligheten att meddela förelägganden bör knyta an till den behöriga myndighetens tillsynsuppdrag. Det handlar bl.a. om att kontrollera uppgifterna som ligger till grund för anmälan respektive registrering, uppgifterna som ska finnas i registren över dataförmedlingstjänster och dataaltruismorganisationer (se t.ex. artiklarna 11.6, 11.10 och 18) samt att villkoren för tillhandahållandet av dataförmedlingstjänster och dataaltruismåtgärder följs (se t.ex. artiklarna 12 och 21).

Möjligheten för myndigheter att utfärda förelägganden för att kunna utföra sitt tillsynsuppdrag följer av bestämmelserna om myndigheters utredningsansvar i förvaltningslagen. Regeringen anser dock att det för tydlighetens skull bör införas en bestämmelse i kompletteringslagen om att den behöriga myndigheten har möjlighet att utfärda förelägganden inom ramen för sin tillsynsverksamhet. Det bedöms däremot inte, som *PTS* föreslår, som lämpligt att ta in upplysningsbestämmelser för samtliga tillsynsuppgifter som följer av EU:s dataförvaltningsförordning. En sådan lösning skulle göra lagstiftningen onödigt komplicerad och svåröverskådlig.

Det är av vikt att tillsynsmyndigheten i så stor utsträckning som möjligt kan bedriva ett effektivt tillsynsarbete. För att underlätta det arbetet bör myndigheten ha tillgång till flera verktyg, t.ex. möjligheten att besluta om förelägganden, med eller utan vite. I promemorian föreslås att tillsynsmyndigheten ska kunna förena förelägganden enligt artikel 14 i EU:s dataförvaltningsförordning med vite. Av artikel 14.4 framgår att den behöriga myndigheten genom administrativa förfaranden får ålägga leverantörer av

dataförmedlingstjänster avskräckande ekonomiska sanktioner. Dessa får inbegripa löpande viten och sanktioner med retroaktiv verkan. Det finns inte någon motsvarande bestämmelse som tar sikte på tillsynen av erkända dataaltruismorganisationer eller regelverket om vidareutnyttjande av skyddade data. Regeringen anser mot bakgrund av detta, till skillnad från *Sveriges advokatsamfund* och PTS, att tillsynsmyndigheten endast bör ha möjlighet att förena förelägganden som riktar sig mot leverantörer av dataförmedlingstjänster med vite.

Sammanfattningsvis anser regeringen att tillsynsmyndigheten ska kunna meddela förelägganden och att den möjligheten ska regleras i den nya kompletteringslagen. Det är dock endast förelägganden som riktar sig mot leverantörer av dataförmedlingstjänster enligt artikel 14 i EU:s dataförvaltningsförordning som ska kunna förenas med vite.

Lagen (1985:206) om viten ska tillämpas när myndigheter beslutar om viten.

### *Tillsynsmyndigheten ska kunna utfärda en varning*

Den behöriga myndigheten har möjlighet att kräva att tillhandahållandet av dataförmedlingstjänsten upphör om allvarliga eller upprepade överträdelser inte åtgärdas. Vidare ska den behöriga myndigheten begära att kommissionen avlägsnar leverantören av dataförmedlingstjänster från registret över leverantörer av dataförmedlingstjänster när den har utfärdat föreläggande om att tillhandahållandet av dataförmedlingstjänsten ska upphöra (artikel 14.4 c). En liknande bestämmelse finns för dataaltruismorganisationer när de inte uppfyller kraven i EU:s dataförvaltningsförordning (artikel 24.3). Vid en sådan situation ska den erkända dataaltruismorganisationen förlora sin rätt att använda beteckningen dataaltruismorganisation som är erkänd i unionen och avlägsnas från det offentliga nationella registret och det offentliga unionsregistret för sådana organisationer. Innan det sker ska organisationen få ett meddelande om att den inte bedöms uppfylla ett eller flera av kraven i förordningen och ges möjlighet att yttra sig. Till skillnad från *PTS* bedömer regeringen att ett meddelande i form av t.ex. en erinran eller varning bör kunna utfärdas inför ett beslut att avlägsna en dataaltruismorganisation från registret över erkända dataaltruismorganisationer (jfr artikel 24.3 och 24.5). Även en leverantör av dataförmedlingstjänster ska få ett meddelande och möjlighet att yttra sig när den behöriga myndigheten bedömer att dataförmedlaren inte uppfyller ett eller flera av kraven i förordningen (artikel 14.3). Det bör, som *Sveriges advokatsamfund* påpekar, även gälla för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.

I promemorian föreslås att den behöriga myndigheten ska kunna utfärda en erinran till leverantörer av dataförmedlingstjänster om de bryter mot anmälningsskyldigheten i artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster i artikel 12 eller villkoren för överföring i artikel 31. Den behöriga myndigheten ska också enligt promemorians förslag kunna meddela en erinran till en erkänd dataaltruismorganisation som bryter mot villkoren i artiklarna 18, 20, 21 och 22 eller villkoren för överföring i artikel 31. Det följer av artikel 34 i EU:s dataförvaltningsförordning att medlemsstaterna ska fastställa regler om sanktioner för dessa överträdelser, men även för överträdelser mot artikel 5.14. Regeringen



anser därför att tillsynsmyndigheten bör ha möjlighet att meddela en varning även vid överträdelse av artikel 5.14 i EU:s dataförvaltningsförordning. Det blir då möjligt för tillsynsmyndigheten att meddela en varning i stället för en sanktionsavgift vid mindre allvarliga överträdelser (se avsnitt 6.3.2).

Sveriges advokatsamfund förespråkar att ordet reprimand används i stället för erinran. Reprimand är dock främmande för svensk rätt. Erinran förekommer däremot i flera författningar, t.ex. i rättegångsbalken, lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, luftfartslagen (2010:500), aktiebolagslagen (2005:551) och fastighetsmäklarlagen (2021:516). Tanken med förslaget om att den behöriga myndigheten ska kunna meddela en erinran mot leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer är bl.a. att de, om de inte rättar sig efter beslutet, ska kunna drabbas av en hårdare sanktion, t.ex. avregistrering. En erinran ses emellertid ofta som en mildare påföljd än en varning. Varning reserveras vanligtvis för mer klandervärda ageranden som, om de upprepas, kan leda till återkallelse av ett tillstånd eller avregistrering (se t.ex. prop. 2010/11:15 s. 40 och Högsta förvaltningsdomstolens avgöranden i HFD 2016 ref. 2 I och II). Eftersom syftet med förslaget bl.a. är att en situation där en överträdelse inte upphör ska kunna leda till avregistrering, bedömer regeringen att det ord som bör användas i lagen är varning.

Regeringen bedömer således att tillsynsmyndigheten bör ha möjlighet att utfärda en varning inom ramen för sin tillsyn över leverantörer av dataförmedlingstjänster, dataaltruismorganisationer och vidareutnyttjare. En varning bör i princip alltid utfärdas som en första åtgärd när det finns risk för att en tillhandahållare av dataförmedlingstjänster eller en dataaltruismorganisation avlägsnas från sina respektive register. En varning bör vidare kunna utfärdas innan en sanktionsavgift beslutas eller när förutsättningarna för att besluta om mer ingripande påföljder, t.ex. en sanktionsavgift, inte är uppfyllda.

### 6.3.2 Tillsynsmyndigheten ska besluta om sanktionsavgift

**Regeringens förslag:** Tillsynsmyndigheten ska ta ut en sanktionsavgift från en leverantör av dataförmedlingstjänster för överträdelser av anmälningsskyldigheten, villkoren för tillhandahållande och villkoren för överföring av andra data än personuppgifter till ett tredjeland.

Tillsynsmyndigheten ska också ta ut en sanktionsavgift från en vidareutnyttjare för överträdelser av villkoren för överföring av andra data än personuppgifter till ett tredjeland.

Om det kan anses tillräckligt får tillsynsmyndigheten i stället för att ta ut en sanktionsavgift meddela en varning.

En sanktionsavgift ska inte få beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömning av vitet.

**Promemorians förslag** överensstämmer i huvudsak med regeringens. I promemorian föreslås att tillsynsmyndigheten ska få ta ut en sanktions-

avgift. I promemorian föreslås emellertid inte en uttrycklig bestämmelse om att varning kan meddelas i stället för sanktionsavgift om det kan anses tillräckligt.

**Remissinstanserna:** Samtliga remissinstanser tillstyrker eller har inga synpunkter på förslaget.

### **Skälen för regeringens förslag**

*Tillsynsmyndigheten bör utfärda sanktionsavgifter till leverantörer av dataförmedlingstjänster och vidareutnyttjare av data*

Medlemsstaterna ska fastställa sanktioner för överträdelse av vissa bestämmelser i EU:s dataförvaltningsförordning (artikel 34). Sanktionerna ska vara effektiva, proportionella och avskräckande. Vilka överträdelse som avses framgår av samma bestämmelse och omfattar vidareutnyttjare av skyddade data, leverantörer av dataförmedlingstjänster och dataaltruismorganisationer. Det finns inte någon definition av vad som avses med sanktion i EU:s dataförvaltningsförordning.

I promemorian föreslås att sanktionsavgifter endast ska kunna riktas mot vidareutnyttjare av data och leverantörer av dataförmedlingstjänster, men däremot inte mot dataaltruismorganisationer eftersom dessa organisationer är icke-vinstdrivande. Allt för hårda sanktioner med stora ekonomiska konsekvenser för dessa organisationer bedöms vara oproportionerligt. För dessa organisationer föreslås i stället andra sanktioner. Det finns t.ex. en skyldighet att avregistrera dataaltruismorganisationen från nationella register och unionsregister om organisationen inte uppfyller kraven i EU:s dataförvaltningsförordning (artikel 24.5). Tillsynsmyndigheten föreslås också kunna utfärda en varning inför ett sådant beslut (se avsnitt 6.3). Regeringen bedömer att dessa åtgärder är tillräckliga för att tillförsäkra att dataaltruismorganisationer följer bestämmelserna i EU:s dataförvaltningsförordning.

Leverantörer av dataförmedlingstjänster och vissa vidareutnyttjare av data är däremot vinstdrivande företag som verkar i konkurrens med varandra. EU:s dataförvaltningsförordning syftar bl.a. till att säkerställa att konkurrensen på den inre marknaden inte snedvrids. Det behövs därför effektiva ekonomiska sanktioner som avhåller leverantörer av dataförmedlingstjänster från att tillskansa sig oproportionerliga fördelar samtidigt som ett fritt dataflöde främjas. I promemorian konstateras att straffbestämmelser endast bör införas i undantagsfall och att en sanktionsavgift i stället är ett väl avvägt alternativ. Regeringen instämmer i den bedömningen.

*Vilka överträdelse bör leda till en sanktionsavgift?*

Enligt artikel 34 i EU:s dataförvaltningsförordning ska medlemsstaterna införa sanktioner för överträdelse av skyldigheter om överföring av andra data än personuppgifter (s.k. icke-personuppgifter enligt förordningen) till tredjeländer enligt artiklarna 5.14 och 31. I artikel 5.14 regleras ramarna för tredjelandsöverföringar för den som vidareutnyttjar vissa kategorier av skyddade data från offentliga myndigheter enligt kapitel II i EU:s dataförvaltningsförordning. I artikel 31 regleras internationell tillgång till och överföring av andra data än personuppgifter och den träffar såväl offentliga myndigheter, vidareutnyttjare av skyddade data enligt kapitel II som

leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer. Sanktioner ska också kunna utgå vid överträdelse mot anmälningskyldigheten för vidareutnyttjare av dataförmedlingstjänster enligt artiklarna 11 och 12.

Regeringen anser att tillsynsmyndigheten ska kunna besluta om sanktionsavgifter för överträdelse av artiklarna 5.14, 11, 12 och 31 i EU:s dataförvaltningsförordning, med undantag för dataaltruismorganisationer. Om det kan anses tillräckligt bör tillsynsmyndigheten i stället för att ta ut en sanktionsavgift kunna meddela en varning. Det bör t.ex. kunna ske i fall av mindre allvarliga överträdelse (se avsnitt 6.3.1).

### *Hinder mot dubbelbestraffning*

Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och några av dess tilläggsprotokoll, däribland det sjunde tilläggsprotokollet, gäller som svensk lag enligt lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. I 2 kap. 19 § regeringsformen finns ett förbud mot att meddela lag eller forskrift som står i strid med Sveriges åtaganden enligt Europakonventionen. I artikel 4.1 i sjunde tilläggsprotokollet till Europakonventionen finns ett förbud mot dubbel lagföring eller dubbla straff.

Tillsynsmyndigheten ska enligt förslaget få meddela de förelägganden som behövs för att EU:s dataförvaltningsförordning, den kompletterande nationella lagstiftningen till EU:s dataförvaltningsförordning eller de föreskrifter som har meddelats i anslutning till lagen ska följas (se avsnitt 6.3.1). I vissa fall ska tillsynsmyndigheten kunna förena förelägganden med vite. Syftet med möjligheten till vitesföreläggande är att tillsynsmyndigheten med effektivt medel ska kunna utöva sin tillsynsverk-samhet och bevaka att bestämmelserna i EU:s dataförvaltningsförordning och den kompletterande lagstiftningen efterlevs. Ett vite har karaktär av straff och aktualiserar tillämpningen av förbudet mot dubbel lagföring och dubbla straff i sjunde tilläggsprotokollet till Europakonventionen. Högsta domstolen har i sin praxis fastslagit att det inte enbart är ett slutligt avgörande som utgör ett hinder mot andra förfaranden, utan att även en pågående prövning utgör ett sådant hinder enligt svenska grundläggande processuella principer (se bl.a. avgörandet NJA 2013 s. 502). I regelverk där det är möjligt att utfärda ett vitesföreläggande och ta ut en sanktionsavgift för samma överträdelse införs därför bestämmelser som syftar till att hindra dubbelbestraffning. Dessa brukar utformas på så sätt att sanktionsavgift inte får beslutas om överträdelsen även omfattas av ett vitesföreläggande och överträdelsen ligger till grund för en ansökan om utdömning av vite, se t.ex. 3 kap. 6 § lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden och 12 kap. 3 § lagen (2022:482) om elektronisk kommunikation (jfr prop. 2016/17:22 s. 228 och prop. 2021/22:136 s. 525). Följaktligen bör möjligheten att besluta om en sanktionsavgift förutsätta att samma omständigheter som ligger till grund för avgiften inte omfattas av ett föreläggande om vite, om omständigheterna ligger till grund för en ansökan om utdömning av vite, vilket också bör framgå av kompletteringslagen.

Eftersom en ansökan om utdömande av vite utgör hinder mot ett beslut om sanktionsavgift avseende samma omständigheter bör tillsynsmyndigheten noga överväga om en sådan ansökan är nödvändig när det samtidigt kan vara aktuellt att besluta om en sanktionsavgift.

Regeringen bedömer att det inte är särskilt troligt att den omvända situationen skulle uppstå, dvs. att en beslutad sanktionsavgift skulle utgöra hinder mot ett föreläggande eller utdömande av vite. Ett vitesföreläggande syftar till att få enskilda att vidta en åtgärd eller underlåta att göra något, dvs. att påverka ett framtida handlande. En sanktionsavgift däremot syftar till att straffa ett tidigare agerande. Ett vitesföreläggande som beslutas efter en sanktionsavgift kan därför inte omfatta samma händelse. Regeringen bedömer vidare att det inte är sannolikt att tillsynsmyndigheten skulle använda sig av ett vitesföreläggande eller ansöka om utdömande av vite för en överträdelse för vilken en sanktionsavgift har beslutats (jfr prop. 2021/22:136 s. 363 och 364). Regeringen konstaterar därför att risken för dubbelbestraffning i den beskrivna situationen är mycket osannolik och därför inte motiverar en bestämmelse om förbud mot dubbelprövning.

### 6.3.3 Sanktionsavgiftens storlek

**Regeringens förslag:** Sanktionsavgiften ska uppgå till lägst 5 000 kronor och högst 10 000 000 kronor.

När avgiftens storlek bestäms ska hänsyn tas till

- överträdelsens art, allvar, omfattning och varaktighet,
- åtgärder som har vidtagits för att begränsa eller avhjälpa den skada som överträdelsen har orsakat,
- tidigare överträdelser,
- de ekonomiska vinster som har gjorts eller de förluster som har undvikits till följd av överträdelsen, och
- andra försvårande eller förmildrande omständigheter.

Tillsynsmyndigheten ska kunna avstå från att ta ut avgiften helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Samtliga remissinstanser tillstyrker eller har inga synpunkter på förslaget.

#### Skälen för regeringens förslag

*Sanktionsavgiften bör bygga på strikt ansvar, men bör kunna sättas ned i vissa fall*

Huvudregeln är att sanktionsavgifter bygger på strikt ansvar, dvs. att avgiften tas ut oberoende av om överträdelsen har skett med uppsåt eller på grund av oaktsamhet (prop. 1981/82:142 s. 95). Syftet med avgiften är ofta att uppnå en vinsteliminierande och handlingsdirigerande effekt, vilket innebär att avgiften inte sällan sätts något högre än den beräknade vinsten eller minskade förlusten till följd av överträdelsen. När det gäller de nu

aktuella överträdelserna är det av vikt att det upprätthålls ett starkt skydd för de uppgifter som kan bli föremål för vidareutnyttjande eller som tillhandahålls av leverantörer av dataförmedlingstjänster. Avgiften bör därför bygga på strikt ansvar.

Det bör dock finnas ett utrymme för tillsynsmyndigheten att sätta ned avgiften eller avstå från att helt eller delvis ta ut avgiften om överträdelserna är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften. Det kan t.ex. vara fråga om en bagatellartad överträdelse som inte har varit till men för något allmänt eller enskilt intresse. Det skulle kunna röra sig om att leverantören av dataförmedlingstjänster inte anmält en uppgift enligt artikel 11 och att det rör sig om en uppgift som t.ex. inte har haft någon större betydelse för bedömningen av leverantörens rätt att tillhandahålla dataförmedlingstjänster eller som inte inverkat på möjligheten att utöva tillsyn. En överträdelse kan vidare vara ursäktlig om det varit närmast omöjligt för den avgiftsskyldige att upptäcka överträdelserna eller om den på annat sätt varit utanför den avgiftsskyldiges kontroll. Avsikten är dock inte att sanktionsavgiften ska sättas ned på grund av bristande kännedom om reglerna, dålig ekonomi, tidsbrist, bristande rutiner eller liknande.

### *Sanktionsavgiftens storlek*

Sanktionsavgifter kan vara utformade på olika sätt. De kan avse på förhand bestämda belopp, ett beloppsintervall eller vara kopplade till omsättningen i näringsverksamheten.

De överträdelser som nu är aktuella för sanktionsavgift rör bl.a. anmälningsskyldigheten för leverantörer av dataförmedlingstjänster enligt artiklarna 11 och 12 eller att vidareutnyttjare och leverantörer av dataförmedlingstjänster inte lyckats upprätthålla ett fullgott skydd för data.

Eftersom det inte finns någon befintlig marknad för vidareutnyttjande av data och dataförmedlingstjänster är det svårt att uppskatta vilken nivå som krävs för att sanktionsavgiften ska ha en tillräckligt handlingsdirigerande och avskräckande effekt. Beloppsintervallet för sanktionsavgifter varierar mellan olika rättsområden, från 1 000 kronor som lägsta nivå, upp till 20 000 000 kronor för de allvarligaste överträdelserna, se t.ex. resegarantilagen (2018:1218) och lagen (2016:1145) om offentlig upphandling.

Den aktuella lagstiftningen innebär att dataförmedlingstjänster kommer att kunna erbjudas av såväl mindre företag som stora globala företag. Intervallet behöver därför vara förhållandevis stort med möjlighet att besluta om högre avgifter för allvarliga överträdelser. Regeringen bedömer mot bakgrund av detta att en sanktionsavgift bör kunna beslutas med lägst 5 000 kronor och högst 10 000 000 kronor.

I artikel 34.2 anges ett antal vägledande kriterier som kan beaktas vid utdömning av sanktioner. De omständigheter som räknas upp är bl.a. överträdelsens art och omfattning, eventuella åtgärder som vidtagits för att begränsa eller avgränsa den skada som överträdelserna orsakat, andra tidigare överträdelser, de ekonomiska vinster som gjorts eller förluster som undvikits till följd av överträdelserna och andra försvårande eller förmildrande omständigheter. Regeringen anser att dessa omständigheter är relevanta för bedömningen av sanktionsavgiftens storlek och att de bör ligga till

grund för tillsynsmyndighetens bedömning av sanktionsavgiftens storlek. De omständigheter som kan beaktas bör dock inte vara uttömmande, utan hänsyn ska kunna tas till samtliga relevanta omständigheter i det enskilda fallet.

### 6.3.4 Bestämmelser om förfarandet vid beslut om sanktionsavgifter

**Regeringens förslag:** En sanktionsavgift ska endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Ett beslut om sanktionsavgift ska delges.

Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften fick laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas i tid, ska den lämnas in för indrivning.

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

Sanktionsavgiften ska tillfalla staten.

**Promemorians förslag** överensstämmer i huvudsak med regeringens. I promemorian föreslås en uttrycklig bestämmelse om att verkställighet får ske enligt utsökningsbalken.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Bolagsverket* anför att bestämmelsen om att verkställighet får ske enligt utsökningsbalken är överflödig eftersom en förvaltningsmyndighets beslut som innefattar betalningsskyldighet numera utgör en exekutionstitel enligt utsökningsbalken.

**Skälen för regeringens förslag:** Det är vanligt att bestämmelser om sanktionsavgifter åtföljs av särskilda förfarandebestämmelser om bl.a. delgivning, preskription och verkställighet, se t.ex. 15 kap. 9 d § och 11–14 §§ lagen (2004:297) om bank- och finansieringsrörelse och 7 kap. 20–23 §§ lagen om åtgärder mot penningtvätt och finansiering av terrorism. Eftersom en sanktionsavgift är en ingripande åtgärd bör det t.ex. finnas en bortre tidsgräns för när avgiften får beslutas. En sanktionsavgift bör endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Bevisbördan för att kommunikation har skett bör ligga på tillsynsmyndigheten. Tidsfristen bör räknas från när överträdelsen ägde rum. I fråga om en överträdelse som skett löpande under viss tid är det tillräckligt att kommunikation sker inom två år från det att överträdelsen upphörde för att en sanktionsavgift ska kunna åläggas.

En sanktionsavgift bör betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om avgiften inte betalas i tid bör

tillsynsmyndigheten vara skyldig att lämna den obetalda avgiften för indrivning. Av 3 kap. 1 § 6 utsökningsbalken följer att en förvaltningsmyndighets beslut som innefattar betalningsskyldighet och som får överklagas som t.ex. förvaltningsbesvär utgör en exekutionstitel (prop. 2021/22:206 s. 36). Det saknas därför, som *Bolagsverket* anför, behov av en särskild bestämmelse om att verkställighet får ske enligt utsökningsbalken.

I likhet med vad som i allmänhet gäller för sanktionsavgifter bör avgiften preskriberas till den del verkställighet inte har skett inom fem år. Slutligen bör sanktionsavgiften tillfalla staten.

### 6.3.5 Informationsutbyte och sekretess

**Regeringens förslag:** Tillsynsmyndigheten ska, när den bedriver tillsyn, kunna utbyta information med andra myndigheter. Även andra myndigheter, som regeringen ska få bestämma, ska kunna utbyta information med tillsynsmyndigheten i syfte att myndigheterna ska kunna bedriva tillsyn.

**Regeringens bedömning:** Det behövs inte några sekretessbestämmelser för att skydda uppgifter i den behöriga myndighetens tillsynsverksamhet.

**Promemorians förslag och bedömning** överensstämmer i sak med regeringens. Promemorians förslag har dock en något annorlunda redaktionell utformning.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen*, *E-hälsomyndigheten*, *Försvarets materielverk*, *Förvaltningsrätten i Stockholm*, *Konsumentverket*, *Läkemedelsverket*, *Malmö kommun*, *Patent- och registreringsverket*, *Pensionsmyndigheten*, *Polismyndigheten*, *Region Östergötland*, *Socialstyrelsen*, *Säkerhetspolisen*, *Verket för innovationssystem*, *Växjö kommun* och *Åklagarmyndigheten* tillstyrker eller har inga synpunkter på förslaget.

*Konkurrensverket* anser att det behöver klargöras vilka sekretessregler som ska gälla i tillsynsmyndighetens verksamhet för uppgifter som omfattas av sekretess hos den utlämnande myndigheten. Enligt myndigheten är det angeläget att säkerställa att det finns ett motsvarande skydd för uppgifterna hos tillsynsmyndigheten.

#### Skälen för regeringens förslag och bedömning

##### *Sekretess för uppgifter i tillsynsmyndighetens tillsynsverksamhet*

Generellt gäller att uppgifter i allmänna handlingar är offentliga hos alla myndigheter. För att göra undantag från den principen krävs stöd i lag. Bestämmelser om sekretess finns huvudsakligen i offentlighets- och sekretesslagen. Sekretess innebär att det är förbjudet att röja uppgifter, vare sig det sker muntligen, genom att en handling lämnas ut eller på annat sätt (3 kap. 1 § OSL).

För att tillsynsmyndigheten ska kunna utföra den tillsyn som krävs enligt EU:s dataförvaltningsförordning och som föreslås i den föreslagna kompletteringslagen kommer myndigheten att behöva få tillgång till ett

stort antal uppgifter för att kontrollera att bl.a. leverantörer av dataförmedlingstjänster och dataaltruismorganisationer uppfyller kraven i EU:s dataförvaltningsförordning, t.ex. uppgifter om hur data används, kommersiella villkor, uppbyggnaden av tjänster, säkerhetsåtgärder och loggar (se artiklarna 12, 20 och 21). Flera av dessa uppgifter kan tänkas utgöra känsliga affärsuppgifter.

Sekretess innebär en inskränkning i den grundlagsfästa rätten till att ta del av allmänna handlingar och avvägningen mellan allmänhetens intresse av insyn måste vägas noga mot sekretessintresset. Regeringen anser emellertid att det är av vikt att de uppgifter som lämnas till tillsynsmyndigheten inom ramen för myndighetens tillsyn, t.ex. om sådant som kan betraktas som affärshemligheter, ska kunna omfattas av sekretess.

I 30 kap. 23 § OSL finns en bestämmelse som gör det möjligt för regeringen att meddela föreskrifter om sekretess för en statlig myndighets verksamhet om den bl.a. innefattar tillsyn. I 9 § och bilagan till offentlighets- och sekretessförordningen (2009:641) finns sådana föreskrifter. Beroende på vilken myndighet som regeringen beslutar att utse till behörig myndighet kan det finnas behov av att komplettera den aktuella bilagan.

Enligt 30 kap. 23 § OSL gäller sekretess bl.a. för uppgift om en enskilds affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgifterna röjs, och för uppgift om andra ekonomiska eller personliga förhållanden för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet. De aktuella bestämmelserna i 30 kap. 23 § OSL bedöms innebära att uppgifter i den behöriga myndighetens tillsynsverksamhet i tillräcklig utsträckning kommer att omfattas av sekretess.

#### *Tillsynsmyndigheten och andra myndigheter bör kunna utbyta information när de bedriver tillsyn*

Tillsynen över dataförmedlingstjänster angränsar mot flera andra områden och tillsynsverksamheter, t.ex. dataskydd, konkurrensrätt och cybersäkerhet. Tillsynsmyndigheten behöver därför kunna samverka och utbyta information med andra tillsynsmyndigheter inom framför allt dessa områden. Samverkan bör i första hand avse samordning av tillsyn och utbyte av information inom ramen för respektive verksamhets tillsynsområde. På samma sätt som när tillsynen bedrivs direkt mot t.ex. leverantörer av dataförmedlingstjänster kommer de uppgifter som kan behöva lämnas mellan myndigheterna att röra känsliga uppgifter av olika slag, främst affärsuppgifter. Mot bakgrund av att granskningen inte kommer att avse själva datan gör regeringen bedömningen att det inte finns behov av att utbyta information som utgör personuppgifter.

I offentlighets- och sekretesslagen finns inte någon generell bestämmelse som innebär att myndigheter kan utbyta information som skyddas av sekretess. Det finns en bestämmelse som innebär att en uppgift kan lämnas till en annan myndighet, trots att den skyddas av sekretess, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet (10 kap. 2 § OSL). Den bestämmelsen tar dock sikte på den utlämnande myndighetens verksamhet och gör det inte möjligt för tillsynsmyndigheten att, inom ramen för sin tillsynsverksamhet, ta emot uppgifter från andra myndigheter. Regeringen bedömer därför att det behövs en sär-



skild bestämmelse som innebär att den behöriga myndigheten och andra myndigheter kan utbyta information inom ramen för respektive myndighets tillsynsverksamhet (jfr 10 kap. 28 § OSL). Regeringen bör bestämma mellan vilka myndigheter information ska kunna utbytas mot bakgrund av att myndigheternas verksamhet kan komma att ändras.

*Konkurrensverket* anser att det bör säkerställas att det finns sekretessregler som gäller i tillsynsmyndighetens verksamhet för uppgifter som omfattas av sekretess hos den utlämnande myndigheten. Av 11 kap. 1 § OSL följer att om en myndighet får en sekretessreglerad uppgift från en annan myndighet, så blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten. Bestämmelsen omfattar den mottagande myndighetens verksamhet som avser tillsyn eller revision. Eftersom det föreslagna informationsutbytet mellan tillsynsmyndigheten och andra myndigheter ska omfatta dessa myndigheters tillsynsverksamhet kommer sekretessbelagda uppgifter fortsätta att skyddas av sekretess vid ett överlämnande.

#### *Sekretess för uppgifter som utbyts mellan myndigheter enligt EU:s dataförvaltningsförordning*

Den behöriga myndigheten ska samarbeta med och bistå motsvarande myndigheter i andra medlemsstater (artikel 14.7 i EU:s dataförvaltningsförordning). Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna för utförande av deras uppgifter enligt förordningen och i vissa fall finns en skyldighet att lämna ut information (artikel 26.4). Den behöriga myndigheten ska också i vissa fall samarbeta med de nationella konkurrensmyndigheterna, de myndigheter som ansvarar för cybersäkerhet och andra relevanta sektorsmyndigheter (artikel 13.3), se avsnitt 6.2.

Uppgifter i den behöriga myndighetens tillsynsverksamhet kan sannolikt komma att omfattas av sekretess. Det innebär att det måste finnas stöd i offentlighets- och sekretesslagen, eller i annan lag eller förordning som den lagen hänvisar till, för att uppgifter som omfattas av sekretess ska kunna lämnas ut till andra myndigheter (8 kap. 1 § OSL). Av 10 kap. 28 § OSL följer att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldigheten följer av lag eller förordning. En uppgift för vilken sekretess gäller får inte heller röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning (8 kap. 3 § 1 OSL).

EU-förordningar bör anses likställda med svensk lag (se t.ex. prop. 1999/2000:126 s. 272). Detta innebär att en uppgiftsskyldighet som följer av en EU-förordning får anses bryta sekretessen enligt 10 kap. 28 § och 8 kap. 3 § OSL (jfr samma prop. s. 283). För att den behöriga myndigheten ska kunna utbyta uppgifter med behöriga myndigheter i andra medlemsstater behövs det enligt regeringens mening därför inte en sekretessbrytande bestämmelse i nationell lagstiftning, eftersom skyldigheten att samarbeta följer direkt av EU-förordningen (se t.ex. artiklarna 14.7 och 26.6 i EU:s dataförvaltningsförordning). Detsamma gäller för samarbete mellan nationella myndigheter som följer direkt av EU:s dataförvaltningsförordning.

Om en myndighet får en sekretessreglerad uppgift från en annan myndighet fortsätter sekretessen att gälla hos den mottagande myndigheten, om myndigheten får uppgiften i sin verksamhet som avser tillsyn eller revision (11 kap. 1 § OSL). Sekretesskyddet fortsätter alltså att gälla med stöd av 11 kap. 1 § OSL för uppgifter som lämnas mellan myndigheter i Sverige i deras tillsynsverksamhet enligt EU:s dataförvaltningsförordning. Sekretess gäller vidare för vissa uppgifter som en svensk myndighet får som ett led i ett förfarande enligt t.ex. en EU-förordning (30 kap. 24 § OSL).

Det finns också bestämmelser i EU:s dataförvaltningsförordning som innebär att den behöriga myndigheten, om den anser att begärd information från behöriga myndigheter i andra medlemsstater eller från kommissionen är konfidentiell, kan påkalla att skyddet för uppgifterna upprätthålls. De behöriga myndigheterna och kommissionen ska i sådana fall säkerställa konfidentiell behandling (artikel 26.6). Dessa bestämmelser bör enligt regeringens mening säkerställa sekretesskyddet för uppgifter som lämnas över till kommissionen och till behöriga myndigheter i andra medlemsstater. Det innebär att svenska myndigheter kan påkalla att sekretess fortsatt ska gälla för uppgifter som lämnas till utländska myndigheter och EU:s institutioner enligt EU:s dataförvaltningsförordning. I sådana fall bör myndigheten göra en sekretessmarkering på handlingen enligt 5 kap. 5 § OSL.

För uppgifter som myndigheter i andra medlemsstater lämnar till tillsynsmyndigheten i Sverige med stöd av EU:s dataförvaltningsförordning aktualiseras bestämmelserna i 15 kap. 1 och 1 a §§ OSL. Av 15 kap. 1 § följer bl.a. att sekretess gäller för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör en annan stat, myndighet, medborgare eller juridisk person i annan stat, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Enligt 15 kap. 1 a § OSL gäller sekretess för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EUrättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation, om det kan antas att Sveriges möjlighet att delta i det internationella samarbetet som avses i rättsakten eller i avtalet försämras om uppgiften röjs. Dessa bestämmelser har bedömts tillgodose behovet av utrikessekretess med anledning av Sveriges inträde i EU (se prop. 1994/95:112 s. 26–29). Regeringen bedömer mot denna bakgrund att bestämmelserna i 15 kap. 1 och 1 a §§ är tillräckliga för att uppfylla kraven i artikel 26.4 i EU:s dataförvaltningsförordning.

Möjligheten att i övrigt bevara sekretesskyddet för uppgifter som lämnas till EU:s institutioner regleras i Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar.

## 6.4 Anmälningförfarandet och tillsynen för leverantörer av dataförmedlingstjänster ska avgiftsbeläggas

**Regeringens förslag:** Tillsynsmyndigheten ska få ta ut avgifter för anmälan, registerhållning och tillsyn av leverantörer av dataförmedlingstjänster.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om avgifterna för anmälningförfarandet, registerhållningen och tillsynen av leverantörer av dataförmedlingstjänster.

**Promemorians förslag** överensstämmer i sak med regeringens. Promemorians förslag har dock en något annorlunda redaktionell utformning.

**Remissinstanserna:** Samtliga remissinstanser tillstyrker eller har inga synpunkter på förslaget.

**Skälen för regeringens förslag:** Anmälningförfarandet för dataförmedlingstjänster får enligt EU:s dataförvaltningsförordning avgiftsbeläggas i medlemsstaterna (artikel 11.11). Leverantörer av dataförmedlingstjänster ska sedan de anmält sig stå under tillsyn av den behöriga myndigheten (artikel 14). Avgiften får omfatta administrativa kostnader för de behöriga myndigheternas övervakning av efterlevnaden, och andra marknadskontrollåtgärder, avseende anmälningar av leverantörer av dataförmedlingstjänster. Avgiften får därmed omfatta både anmälningförfarandet och den efterföljande tillsynen.

Ansvar för att registrera och utöva tillsyn över leverantörer av dataförmedlingstjänster bör läggas på en statlig myndighet (avsnitt 6.2). Regeringen bedömer att registret och tillsynen bör avgiftsfinansieras. Regeringen eller den myndighet som regeringen bestämmer bör få meddela föreskrifter om avgifterna. Det finns många osäkerhetsfaktorer för marknaden av dataförmedlingstjänster och hur den kommer att utvecklas. Oaktat det anser regeringen, till skillnad från den bedömning som görs i promemorian, att storleken på avgiften bör följa huvudregeln i avgiftsförordningen att avgifter ska beräknas så att de helt täcker verksamhetens kostnader (full kostnadstäckning).

## 6.5 Överklagande av beslut

**Regeringens förslag:** Den behöriga myndighetens beslut enligt EU:s dataförvaltningsförordning och kompletteringslagen ska kunna överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätt.

**Promemorians förslag** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läkemedelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för inno-*

vationssystem, Växjö kommun och Åklagarmyndigheten tillstyrker eller har inga synpunkter på förslaget.

*Bolagsverket* anför att det saknas ett resonemang och analys avseende rätten att lämna in ett klagomål samt att överklaga kollektivt enligt artiklarna 27 och 28 i EU:s dataförvaltningsförordning. Möjligheten att föra talan kollektivt får anses saknas i förvaltningslagen och förvaltningsprocesslagen (1971:291).

### **Skälen för regeringens förslag**

*Beslut enligt kompletteringslagen och EU:s dataförvaltningsförordning ska kunna överklagas*

Rätten till ett effektivt rättsmedel mot myndighetsbeslut tillgodoses normalt sett genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol, dvs. till en förvaltningsrätt som första instans (se t.ex. prop. 1981/82:142 s. 99). När det gäller beslut som fattas enligt en EU-förordning följer rätten att överklaga av allmänna förvaltningsrättsliga principer och förvaltningslagen. Någon särskild överklagandebestämmelse behövs därmed i och för sig inte i nationell lagstiftning när det gäller beslut som tillsynsmyndigheten fattar enligt EU:s dataförvaltningsförordning.

Däremot behövs det särskilda bestämmelser om rätten att överklaga tillsynsmyndighetens beslut enligt den föreslagna kompletteringslagen, dvs. om varning och sanktionsavgift. För att inte skapa otydlighet om hur olika beslut ska kunna överklagas bör regleringen i den nya lagen vara uttömmande. Således bör även rätten att överklaga tillsynsmyndighetens beslut enligt EU:s dataförvaltningsförordning uttryckligen anges i kompletteringslagen.

Regeringen anser att den överklagandefrist om tre veckor som normalt sett gäller vid överklagande av förvaltningsbeslut även bör gälla vid överklagande av tillsynsmyndighetens beslut enligt EU:s dataförvaltningsförordning och kompletteringslagen (44 § förvaltningslagen). Det bör också krävas prövningstillstånd vid överklagande till kammarrätten.

*Särskilt om möjligheten att överklaga beslut enligt EU:s dataförvaltningsförordning*

Enligt artikel 28.1 i EU:s dataförvaltningsförordning ska berörda fysiska och juridiska personer ha rätt till effektiva rättsmedel avseende rättsligt bindande beslut som avses i artiklarna 14, 19 och 24 som fattas av den behöriga myndigheten. Förfaranden enligt artikel 28 ska inledas vid domstolarna i den medlemsstat där den behöriga myndigheten som rättsmedlen avser är belägen, antingen individuellt eller i förekommande fall kollektivt.

*Bolagsverket* efterfrågar en analys av möjligheten att kollektivt överklaga vissa beslut enligt EU:s dataförvaltningsförordning. Det finns dock inte någon uttrycklig skyldighet för medlemsstaterna att införa en möjlighet att överklaga kollektivt och regeringen anser inte heller att det finns skäl att införa någon sådan möjlighet i nationell rätt för överklagande av beslut enligt EU:s dataförvaltningsförordning. Enligt förslaget ska den behöriga myndighetens beslut enligt EU:s dataförvaltningsförordning och

kompletteringslagen överklagas till allmän förvaltningsdomstol. De processuella regler som allmän förvaltningsdomstol ska tillämpa i förvaltningsmål finns huvudsakligen i förvaltningsprocesslagen (1971:291). Enligt lagen (2002:599) om grupprättegång finns en möjlighet att föra grupptalan i allmän domstol. Någon motsvarande möjlighet att föra grupptalan i förvaltningsdomstol finns i princip inte, se dock lagen (2023:730) om grupptalan till skydd för konsumenters kollektiva intressen. Bestämmelserna om grupptalan har motiverats av ett behov av att tillvarata enskildas rättsskydd i situationer där det kan vara svårt att göra gällande anspråk i domstol, t.ex. när varje enskilt anspråk har ett mindre ekonomiskt värde. Till saken hör att det i mål i allmän domstol, enligt reglerna i rättegångsbalken, som utgångspunkt gäller att tappande part ska ersätta vinnande parts kostnader (se 18 och 31 kap. rättegångsbalken). Vidare måste käranden för att väcka talan i allmän domstol som regel betala en ansökningsavgift till tingsrätten. Några motsvarande kostnader eller risker för rättsförluster finns inte för parter som för talan i förvaltningsdomstol. Det finns inte heller några hinder för klaganden att ge in ett gemensamt överklagande av ett beslut. Regeringen bedömer mot bakgrund av detta att det inte aktualiseras något behov av att, på samma sätt som för vissa mål i allmän domstol, införa en möjlighet för enskilda att överklaga beslut enligt EU:s dataförvaltningsförordning kollektivt.

Vidare ska berörda fysiska och juridiska personer ha en rätt till ett effektivt rättsmedel om den behöriga myndigheten underlåter att vidta åtgärder med avseende på ett klagomål enligt artikel 27 i EU:s dataförvaltningsförordning. EU-domstolen har, beträffande en liknande motsvarande bestämmelse i artikel 28.3 i det tidigare dataskyddsdirektivet (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), uttalat att bestämmelsen innebär att den person som har kommit in med en begäran till tillsynsmyndigheten ska ha tillgång till rättsmedel med vilka han eller hon vid nationella domstolar kan angripa det beslut som gått vederbörande emot (se t.ex. dom Schrems, C-362/14, EU:C:2015:650, punkt 64). Detta talar för att EU:s dataförvaltningsförordning skulle kunna förutsätta att personer som ger in klagomål till den behöriga myndigheten enligt artikel 27 har en generell rätt att överklaga den behöriga myndighetens beslut att t.ex. inte vidta någon åtgärd med anledning av ett klagomål.

Det finns dock omständigheter som talar emot en sådan tolkning. Enligt artikel 28.1 i EU:s dataförvaltningsförordning är det berörda fysiska och juridiska personer som ska ha rätt till effektiva rättsmedel. Dessutom ska beslutet vara rättsligt bindande för denne. Ett beslut om att inte vidta några åtgärder med anledning av ett klagomål medför normalt sett inte några rättsligt bindande följder för den som har lämnat in klagomålet (se t.ex. avgörandet HFD 2023 not. 47).

Sammanfattningsvis anser regeringen att det bör överlämnas till rättstillämparen att, genom en tolkning av förvaltningslagens generella bestämmelser om överklagande och bestämmelserna i EU:s dataförvaltningsförordning, bedöma klagorätten (jfr prop. 2017/18:105 s. 163–165).

Av den föreslagna kompletteringslagen bör det framgå att tillsynsmyndighetens beslut enligt lagen och enligt artiklarna 14, 19 och 24 i EU:s dataförvaltningsförordning får överklagas till allmän förvaltningsdomstol.

## 7 Ikraftträdande- och övergångsbestämmelser

**Regeringens förslag:** Den föreslagna lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning och övriga lagändringar ska träda i kraft den 2 augusti 2024.

**Regeringens bedömning:** Några övergångsbestämmelser behövs inte.

**Promemorians förslag och bedömning** överensstämmer delvis med regeringens. I promemorian föreslås att den föreslagna lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning och lagändringarna ska träda i kraft den 1 januari 2024.

**Remissinstanserna:** Ingen av remissinstanserna yttrar sig särskilt över förslaget och bedömningen.

**Skälen för regeringens förslag och bedömning:** Den tidpunkt för ikraftträdande som föreslås i promemorian har passerat och ikraftträdandet behöver därför senareläggas. Eftersom EU:s dataförvaltningsförordning har trätt i kraft bör den föreslagna nya lagen och lagändringarna träda i kraft så snart som möjligt, vilket bedöms vara den 2 augusti 2024.

Det bedöms inte finnas något behov av några övergångsbestämmelser.

## 8 Konsekvenser

**Regeringens bedömning:** Förslagen innebär inte några skyldigheter för myndigheter att tillgängliggöra skyddade data enligt EU:s dataförvaltningsförordning.

Flera myndigheter får med anledning av förslagen nya permanenta uppgifter som kommer att medföra en ökad arbetsbörda. Det handlar om de myndigheter som utses till behöriga organ, tillsynsmyndigheten, som även ska vara behörig myndighet, samt den myndighet som ska tillhandahålla den gemensamma informationspunkten. De nya uppgifterna kommer som huvudregel att finansieras genom ökade anslag. Tillsynsmyndighetens uppgifter att hantera anmälningar, registerhållning och tillsyn över leverantörer av dataförmedlingstjänster kommer dock att avgiftsfinansieras.

Förslagen leder till något ökade kostnader för domstolarna. Kostnadsökningarna bedöms inte vara större än att de kan hanteras inom befintliga ekonomiska ramar.

Förslagen innebär inte några konsekvenser för företagen, eftersom det för närvarande inte finns någon etablerad marknad för vidareut-

nyttjande av skyddade data, dataförmedling eller dataaltruism. Förslagen bedöms inte heller på kort sikt innebära några samhällsekonomiska konsekvenser.

**Promemorians bedömning** överensstämmer med regeringens.

**Remissinstanserna:** Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen, E-hälsomyndigheten, Försvarets materielverk, Förvaltningsrätten i Stockholm, Konsumentverket, Läke-medelsverket, Malmö kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Region Östergötland, Socialstyrelsen, Säkerhetspolisen, Verket för innovationssystem, Växjö kommun* och *Åklagarmyndigheten* delar eller har inga synpunkter på bedömningen.

*Myndigheten för digital förvaltning* och *Region Skåne* anser att den föreslagna finansieringen till de behöriga organen inte är tillräcklig. Enligt Myndigheten för digital förvaltning kommer kostnaderna för att ge det stöd som krävs för att främja användningen av data samt att vara behörigt organ uppgå till 3,6 miljoner kronor det första året och därefter ca 2,3 miljoner kronor per år. Vidare kommer kostnaden för att bygga upp den tekniska funktionaliteten som krävs för att implementera den gemensamma informationspunkten enligt myndigheten att uppgå till 3,8 miljoner kronor det första året och därefter till ca 3 miljoner kronor per år. Region Skåne anser att tillgängliggörande av skyddade data för vidareutnyttjande kommer att få ekonomiska konsekvenser för kommuner och regioner, eftersom de bör arbeta med frågan proaktivt för att främja ökad innovation, konkurrenskraft och transparens, trots att regleringen inte ställer tvingande krav på att tillgängliggöra skyddade data.

*Försäkringskassan* anser att det är svårt att förutse konsekvenserna av förslagen och därmed om de kommer att medföra ökade kostnader och behov av finansiering. *Kammarrätten i Jönköping* menar att förslagen kan leda till ytterligare måltillströmning hos samtliga förvaltningsdomstolar och anser att domstolarnas eventuellt ökade arbetsbörda bör följas upp.

Enligt *Kungliga tekniska högskolan* och *Stockholms kommun* leder förslagen till ekonomiska konsekvenser för de myndigheter som ska hantera begäranden om vidareutnyttjande. Även om myndigheter har rätt att ta ut avgifter för ärenden om vidareutnyttjande, kommer handläggningen av sådana ärenden enligt Stockholms kommun att kräva mer resurser. *Bolagsverket* menar att myndighetens anmälningsskyldighet för överträdelse enligt artikel 5.14 i EU:s dataförvaltningsförordning inte rymmer inom befintliga anslag, eftersom myndigheten inte är anslagsfinansierad.

*Regelrådet* anser att det av konsekvensanalysen bör framgå att det inte bara är dataförmedlingstjänster eller dataaltruismorganisationer som kan tänkas påverkas av regleringen, utan också sådana företag i vilkas intresse det är att använda den offentliga data som kan tillgängliggöras. Enligt myndigheten bör det även framgå vilka och hur många sådana företag som kan komma att påverkas, eventuella effekter för företagets kostnader, tidsåtgång och verksamhet samt hur små företag påverkas av förslagen.

*Kommerskollegium* bedömer att förslagen inte aktualiserar EU:s anmälningsprocedurer för varor och tjänster.

## Skälen för regeringens bedömning

### *Samhällsekonomiska konsekvenser*

EU:s dataförvaltningsförordning kommer enligt Europeiska kommissionens konsekvensanalys till EU:s dataförvaltningsförordning att förbättra den inre marknaden för data, och därmed den inre marknaden som helhet. Säkra produkter och tjänster med tillgång till stora datamängder är enligt kommissionens analys centralt för den ekonomiska utvecklingen inom unionen. En sådan utveckling är svår att genomföra genom nationella regelverk i olika medlemsstater. Genom en EU-förordning som är direkt tillämplig i alla medlemsstater bedömer kommissionen att det blir lättare för företag att anpassa sina produkter eller tjänster som utvecklats i en medlemsstat till marknaden i andra medlemsstater. Regeringen bedömer att de kompletterande nationella bestämmelserna till EU:s dataförvaltningsförordning bidrar till att uppfylla kommissionens mål med förordningen. För närvarande finns det inte någon etablerad marknad för vidareutnyttjande av data, dataförmedling eller dataaltruism, varför förslagen inte bedöms medföra några samhällsekonomiska konsekvenser. De föreslagna bestämmelserna bedöms på sikt kunna bidra till att skapa sådana marknader, dock främst genom tillkommande sektorslagstiftning som t.ex. den planerade unionsrätten inom hälsodataområdet.

### *Konsekvenser för behöriga organ för vidareutnyttjande av skyddade data*

Den eller de myndigheter som regeringen bestämmer ska vara behöriga organ enligt EU:s dataförvaltningsförordning. De behöriga organen ska bistå de myndigheter som beviljar eller vägrar tillgång för vidareutnyttjande av skyddade data. Med detta avses bl.a. tekniskt stöd, vägledning och rättsligt bistånd. Enligt EU:s dataförvaltningsförordning ska behöriga organ ha tillräckliga juridiska, ekonomiska och tekniska resurser för att utföra sina uppgifter (se avsnitt 5.8).

I promemorian redovisas att det har undersökts i vilken utsträckning myndigheter innehar data som skulle kunna omfattas av tillämpningsområdet för EU:s dataförvaltningsförordning. De tillfrågade myndigheterna bedömer att regelverket endast kommer att bli tillämpligt i enstaka fall. Uppgiften som behörigt organ bedöms därför i ett inledande skede inte bli särskilt omfattande. Detta talar enligt regeringen för att det inte behöver inrättas en ny myndighet för uppgiften utan att den kan fördelas till en eller flera befintliga myndigheter, som utses av regeringen.

Uppgifterna för den eller de myndigheter som kommer att utses till behöriga organ bedöms initialt kräva 2 miljoner kronor per år tills vidare för den myndighet som får huvudansvaret för uppgifterna och 1 miljon kronor per år tills vidare för andra myndigheter och kommer att finansieras genom ökade anslag (prop. 2023/24:1 utg.omr. 2 och 22). Till skillnad från *Myndigheten för digital förvaltning* och *Region Skåne* anser regeringen att det för närvarande inte krävs någon ytterligare finansiering, eftersom antalet ärenden om vidareutnyttjande av data bedöms bli mycket begränsat. Det beror på att det föreslagna regelverket inte medför några krav på tillgängliggörande av skyddade data för vidareutnyttjande och att det i princip inte finns några sådana skyldigheter i andra lagar eller förordningar. På sikt kan antalet ärenden dock förväntas öka i omfattning, särskilt om nya skyldigheter att tillgängliggöra skyddade data införs.



### *Konsekvenser för den myndighet som ska tillhandahålla den gemensamma informationspunkten*

Den gemensamma informationspunkten ska tillhandahålla en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor. Europeiska kommissionen ska inrätta en europeisk gemensam åtkomstpunkt som den nationella informationspunkten ska vara ansluten till (se avsnitt 5.9).

Kostnaderna för den myndighet som ska tillhandahålla den gemensamma informationspunkten uppskattas till sammanlagt 3 miljoner kronor per år och kommer att tillgodoses genom ökade anslag (prop. 2023/24:1 utg.omr. 22). Kostnaderna omfattar i huvudsak teknisk utveckling av den gemensamma informationspunkten och förvaltning av systemet. Myndigheten som tillhandahåller den gemensamma informationspunkten kommer också att behöva vägleda myndigheter om vilken data och information som de ska lämna till informationspunkten. Till skillnad från *Myndigheten för digital förvaltning* anser regeringen att det för närvarande inte krävs någon ytterligare finansiering.

### *Konsekvenser för den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer*

För att kunna bedöma konsekvenserna för den behöriga myndigheten för dataförmedlingstjänster och dataaltruismorganisationer behöver en uppskattning göras av hur många leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som kan tänkas anmäla sig respektive registrera sig i Sverige. I promemorian anges att det inte har varit möjligt att göra någon sådan beräkning eller uppskattning, men att det i dagsläget i princip inte finns några aktörer som tillhandahåller sådana tjänster. Flerparten andra medlemsstater har gjort samma bedömning. Företag som är etablerade utanför unionen men som verkar här ska utse en rättslig företrädare i någon av medlemsstaterna. Hur många sådana aktörer som kan tänkas omfattas av regelverket är också svårt att bedöma.

Regeringen konstaterar, i likhet med det som redovisas i promemorian, att det för närvarande inte finns någon etablerad marknad för vare sig dataförmedlingstjänster eller dataaltruismorganisationer. Det innebär att arbetet för den behöriga myndigheten till en början kommer att vara begränsat. Myndigheten behöver dock, oavsett antalet aktörer, ha en teknisk infrastruktur redo och ha kapacitet för att hantera registreringar och anmälningar. Regeringen avser att utse en myndighet som har e-tjänster, verksamhetssystem och rutiner att utgå ifrån, vilket också bedöms begränsa kostnaderna jämfört med om en myndighet utan sådan kompetens skulle utses.

Den behöriga myndighetens arbete kommer i huvudsak att bestå av teknisk utveckling av e-tjänster, hantering av ansökningsförfarandet och tillsynen av dataaltruismorganisationer, representation i europeiska datainnovationsstyrelsen och rapportering av uppgifter till Europeiska kommissionen. Kostnaderna för detta uppskattas till sammanlagt 4 miljoner kronor per år och kommer att finansieras genom ökade anslag (prop. 2023/24:1 utg.omr. 22). Den behöriga myndigheten ska även registrera och utöva tillsyn över leverantörer av dataförmedlingstjänster. Dessa uppgifter föreslås vara helt avgiftsfinansierade.

### *Konsekvenser för myndigheter i övrigt samt domstolar*

De nationella bestämmelserna som föreslås komplettera EU:s dataförvaltningsförordning innebär inte några skyldigheter för statliga eller kommunala myndigheter. Det är först om en myndighet till följd av bestämmelser i annan lag, eller på eget initiativ, tillgängliggör skyddade data som den behöver tillämpa bestämmelserna i förordningen och den kompletterande nationella lagstiftningen (se avsnitt 5.3). De nya bestämmelserna kan visserligen tänkas innebära att antalet ärenden om tillgängliggörande av data ökar, men ökningen bedöms bli mycket liten. En myndighet som tillgängliggör skyddade data för vidareutnyttjande föreslås få ta ut en avgift för tillgängliggörandet. Förslagen bedöms i övrigt inte innebära några kostnader för tillgängliggörande myndigheter som inte kommer att täckas av avgiftsintäkterna. Det innebär, till skillnad från vad bl.a. *Bolagsverket* och *Region Skåne* menar, att det inte behövs någon ytterligare finansiering genom ökade anslag för dessa myndigheter.

Eftersom förslagen inte innebär några skyldigheter att tillgängliggöra skyddade data för vidareutnyttjande påverkar de inte heller den kommunala självstyrelsen.

Möjligheten att överklaga myndigheters beslut om tillgängliggörande av skyddade data kommer att innebära en ökning av antalet mål till de allmänna förvaltningsdomstolarna. Det är svårt att bedöma antalet ärenden om tillgängliggörande av skyddade data för vidareutnyttjande. Regeringen bedömer dock att antalet ärenden kommer att vara förhållandevis få och därmed även att antalet överklaganden till domstol kommer att vara få. Förslagen i denna del bedöms därför inte innebära att antalet mål i de allmänna förvaltningsdomstolarna kommer att öka i någon större omfattning. Eventuella kostnadsökningar anses vara marginella och bedöms rymmas inom domstolarnas befintliga anslag. Om behov uppstår kan det dock, i likhet med vad *Kammarrätten i Jönköping* anför, vara lämpligt att så småningom följa upp domstolarnas eventuellt ökade arbetsbörda till följd av förslagen.

### *Konsekvenser för staten*

Förslagen bedöms medföra ökade kostnader för staten med anledning av flera nya myndighetsuppgifter. En statlig myndighet ska utses till tillsynsmyndighet som i sin tur ska vara behörig myndighet enligt EU:s dataförvaltningsförordning. Vidare ska en eller flera statliga myndigheter utses till behöriga organ och en myndighet ska tillhandahålla den gemensamma informationspunkten. Samtliga dessa uppgifter kommer att anslagsfinansieras och kostnaderna bedöms sammanlagt uppgå till 10 miljoner kronor per år. Förslagen innebär i övrigt inte några konsekvenser för staten.

### *Konsekvenser för företag*

Förslagen bedöms, till skillnad från vad *Regelrådet* påpekar, inte medföra några konsekvenser för företagen, eftersom det för närvarande inte finns någon etablerad marknad för vidareutnyttjande av skyddade data, dataförmedling eller dataaltruism. Förslagen syftar dock till att skapa förutsättningar för att en sådan marknad ska etableras, vilket enligt regeringens mening på sikt kommer att gynna företag.

Anmälningsförfarandet för leverantörer av dataförmedlingstjänster föreslås vara avgiftsfinansierat. Även tillgängliggörandet av skyddade data för vidareutnyttjande föreslås avgiftsbeläggas. Trots att det inte finns någon etablerad marknad för vidareutnyttjande eller dataförmedling kan den föreslagna avgiften komma att inverka på företags benägenhet att utveckla sådana tjänster. Det kan dock antas att priset på tjänsterna kommer att anpassas till de avgifter som företagen kommer att behöva betala. Avgiften bedöms därmed inte inverka i någon större utsträckning på företags möjligheter att bedriva dataförmedling.

Enligt EU:s dataförvaltningsförordning får myndigheter göra skyddade data tillgängliga till en nedsatt avgift eller kostnadsfritt, särskilt för små och medelstora företag, uppstarts företag, det civila samhället och utbildningsanstalter, för att ge incitament till vidareutnyttjande av vissa data (artikel 6.4). Regeringen föreslår inte att någon sådan möjlighet införs i nuläget. Det är dock inte uteslutet att på nytt överväga en reducerad avgift för vissa aktörer vid tillgängliggörande av skyddade data för vidareutnyttjande när en sådan marknad har utvecklats.

### *Övriga konsekvenser*

Regeringen bedömer att förslagen inte har någon betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättningen och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheten att nå de integrationspolitiska målen. Förslagen påverkar inte tillämpningen av EU:s dataförvaltningsförordning och bedöms i övrigt vara förenliga med EU-rätten. Förslagen bedöms inte heller medföra något behov av särskilda informationsinsatser.

Regeringen bedömer att förslagen inte aktualiserar EU:s anmälningsprocedurer för varor och tjänster. *Kommerskollegium*, som administrerar dessa anmälningsprocedurer, delar denna bedömning.

## 9 Författningskommentar

### 9.1 Förslaget till lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning

**1 §** Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), i denna lag benämnd EU:s dataförvaltningsförordning.

Ord och uttryck i lagen har samma betydelse som i EU:s dataförvaltningsförordning.

Paragrafen innehåller en upplysning om att lagen kompletterar EU:s dataförvaltningsförordning samt bestämmelser om ord och uttryck i lagen. Övervägandena finns i avsnitt 6.1.

I *första stycket* anges att lagen innehåller kompletterande bestämmelser till EU:s dataförvaltningsförordning. Hänvisningen till förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

Av *andra stycket* framgår att de ord och uttryck som används i lagen, exempelvis behörig myndighet och dataförmedlingstjänst, ska förstås på samma sätt som i EU:s dataförvaltningsförordning.

### **Tillsynsmyndighet**

**2 §** Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet enligt denna lag.

Tillsynsmyndigheten ska vara behörig myndighet för dataförmedlingstjänster enligt artikel 13 i EU:s dataförvaltningsförordning och för registrering av dataaltruismorganisationer enligt artikel 23 i EU:s dataförvaltningsförordning.

Paragrafen innehåller bestämmelser om vilken myndighet som ska vara tillsynsmyndighet och behörig myndighet enligt EU:s dataförvaltningsförordning. Övervägandena finns i avsnitt 6.2.

Av *första stycket* framgår att regeringen bestämmer vilken myndighet som ska vara tillsynsmyndighet enligt lagen.

Enligt *andra stycket* är tillsynsmyndigheten även behörig myndighet för dataförmedlingstjänster enligt artikel 13 och för registrering av dataaltruismorganisationer enligt artikel 23 i EU:s dataförvaltningsförordning. Vilka uppgifter tillsynsmyndigheten har som behörig myndighet framgår av EU:s dataförvaltningsförordning. Det handlar bl.a. om att sköta anmälningsförfarandet för leverantörer av dataförmedlingstjänster och registreringen av dataaltruismorganisationer (artiklarna 11 och 19), samarbeta med andra myndigheter (artikel 13), utöva tillsyn över leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer (artiklarna 14 och 24), föra och regelbundet uppdatera ett offentligt nationellt register över erkända dataaltruismorganisationer (artikel 17) samt hantera klagomål (artikel 27).

### **Uppgiftsskyldighet**

**3 §** De myndigheter som regeringen bestämmer ska på begäran lämna tillsynsmyndigheten de uppgifter som den behöver i sin tillsynsverksamhet.

I paragrafen regleras en skyldighet för de myndigheter som regeringen bestämmer att lämna de uppgifter till tillsynsmyndigheten som den behöver i sin tillsynsverksamhet. Övervägandena finns i avsnitt 6.3.5.

De myndigheter som regeringen bestämmer ska lämna tillsynsmyndigheten uppgifter som den behöver i sin tillsynsverksamhet. Det kan vara ekonomiska uppgifter av olika slag, t.ex. ekonomiska redovisningar från leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som andra myndigheter har fått inom ramen för sin tillsynsverksamhet.

4 § Tillsynsmyndigheten ska på begäran lämna de uppgifter som en annan myndighet behöver i sin tillsynsverksamhet.

Regeringen bestämmer vilka myndigheter som ska ha rätt att få uppgifter enligt första stycket.

I paragrafen regleras en skyldighet för tillsynsmyndigheten att lämna de uppgifter som en annan myndighet behöver i sin tillsynsverksamhet. Övervägandena finns i avsnitt 6.3.5.

Enligt *första stycket* ska tillsynsmyndigheten på begäran lämna de uppgifter som en annan myndighet behöver i sin tillsynsverksamhet. Det kan t.ex. vara uppgifter om hur data används av leverantörer av dataförmedlingstjänster och dataaltruismorganisationer i sina respektive verksamheter, kommersiella villkor eller andra uppgifter i leverantörer av dataförmedlingstjänsters och dataaltruismorganisationers verksamheter som den andra myndigheten behöver i sin tillsynsverksamhet.

Av *andra stycket* framgår att regeringen bestämmer vilka myndigheter som ska ha rätt till uppgifter enligt första stycket.

## Varning

5 § Tillsynsmyndigheten får meddela en varning till en leverantör av dataförmedlingstjänster som bryter mot anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 eller villkoren för överföring av andra data än personuppgifter till tredjeland enligt artikel 31 i EU:s dataförvaltningsförordning.

Paragrafen innehåller bestämmelser om när tillsynsmyndigheten får meddela en varning till en leverantör av dataförmedlingstjänster. Övervägandena finns i avsnitt 6.3.1.

Möjligheten att meddela en varning omfattar överträdelse av anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 och villkoren för överföring av andra data än personuppgifter (s.k. icke-personuppgifter enligt förordningen) till tredjeland enligt artikel 31 i EU:s dataförvaltningsförordning. Samma överträdelse kan leda till en sanktionsavgift enligt 9 §.

Anmälningsskyldigheten i artikel 11 i EU:s dataförvaltningsförordning innebär att leverantörer av dataförmedlingstjänster som avser att tillhandahålla dataförmedlingstjänster enligt förordningen ska lämna en anmälan till den behöriga myndigheten för dataförmedlingstjänster. Av bestämmelserna i artikel 11 framgår även vad en anmälan ska innehålla och till vilken medlemsstat anmälan ska göras.

I artikel 12 i EU:s dataförvaltningsförordning finns villkor för att få tillhandahålla dataförmedlingstjänster. Dessa reglerar bl.a. hur de kommersiella villkoren för dataförmedlingstjänsten får vara utformade (artikel 12 b), att det ska vidtas tillräckliga åtgärder för att säkerställa att data inte används i strid med t.ex. unionsrätten (artikel 12 j) och att det förs ett loggregister över dataförmedlingsverksamheten (artikel 12 o).

Artikel 31 i EU:s dataförvaltningsförordning reglerar förutsättningarna för internationell tillgång till och överföring av vissa skyddade data. Av bestämmelserna följer bl.a. att leverantörer av dataförmedlingstjänster ska vidta åtgärder för att förhindra internationell överföring av eller statlig tillgång till andra data än personuppgifter (icke-personuppgifter) som innehas

i unionen om en sådan överföring eller tillgång skulle strida mot unionsrätten eller den nationella rätten.

Det kan vara aktuellt att i vissa fall besluta om en varning för att få till stånd en frivillig rättelse innan en sanktionsavgift enligt 9 § övervägs eller vid mindre allvarliga överträdelser. Ett exempel på en sådan situation när en varning kan vara aktuell är om en leverantör av dataförmedlingstjänster av rent förbiseende råkat utelämna en uppgift i en anmälan enligt artikel 11.6. Ett annat exempel är om leverantören av dataförmedlingstjänster inte uppfyller något av villkoren i artiklarna 12 eller 31 och överträdelsen inte bedöms vara av så allvarligt slag att en sanktionsavgift behöver utgå vid en frivillig rättelse.

En varning bör i princip alltid meddelas i samband med att tillsynsmyndigheten överväger att begära att Europeiska kommissionen avlägsnar leverantören av dataförmedlingstjänster från kommissionens register enligt artikel 14.4 i EU:s dataförvaltningsförordning, om överträdelsen grundar sig på någon av artiklarna 11 eller 12.

**6 §** Tillsynsmyndigheten får meddela en varning till en fysisk eller juridisk person som har beviljats rätten att vidareutnyttja andra data än personuppgifter för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.

Paragrafen innehåller bestämmelser om när tillsynsmyndigheten får meddela en varning till en fysisk eller juridisk person som har beviljats rätten att vidareutnyttja andra data än personuppgifter. Övervägandena finns i avsnitt 6.3.1.

Möjligheten att meddela en varning omfattar överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning. Samma överträdelser kan leda till en sanktionsavgift enligt 10 §.

Av artikel 5.14 följer att fysiska eller juridiska personer som beviljats rätten att vidareutnyttja andra data än personuppgifter (icke-personuppgifter) endast får överföra dessa data till tredjeländer i enlighet med kraven i artiklarna 10, 12 och 13 i EU:s dataförvaltningsförordning.

Det kan vara aktuellt att i vissa fall besluta om en varning för att få till stånd en frivillig rättelse innan en sanktionsavgift enligt 10 § övervägs eller vid mindre allvarliga överträdelser.

**7 §** Tillsynsmyndigheten får meddela en varning till en erkänd dataaltruismorganisation som bryter mot

1. villkoren för registrering som erkänd dataaltruismorganisation enligt artiklarna 18, 20, 21 eller 22, eller

2. villkoren för överföring av andra data än personuppgifter till tredjeland enligt artikel 31 i EU:s dataförvaltningsförordning.

Paragrafen innehåller bestämmelser om tillsynsmyndighetens möjligheter att meddela en varning till en erkänd dataaltruismorganisation. Övervägandena finns i avsnitt 6.3.1.

Möjligheten att meddela en varning omfattar överträdelser av något av villkoren för registrering som erkänd dataaltruismorganisation enligt artiklarna 18, 20, 21 eller 22 i EU:s dataförvaltningsförordning, eller villkoren för överföring av andra data än personuppgifter (icke-personuppgifter) till tredjeland enligt artikel 31 i samma förordning.

I artikel 18 i EU:s dataförvaltningsförordning finns allmänna krav för registrering i ett offentligt nationellt register över erkända dataaltruismorganisationer. För att kunna registreras måste en dataaltruismorganisation bl.a. utföra dataaltruismåtgärder, vara en juridisk person och bedriva verksamheten på icke-vinstdrivande grund. Av artikel 20 följer ett transparenskrav som bl.a. innebär att en erkänd dataaltruismorganisation ska föra ett register över vilka som getts möjlighet att behandla den data som innehas av den erkända dataaltruismorganisationen. I artikel 21 finns särskilda krav för att skydda registrerade och datainnehavares rättigheter och intressen när det gäller deras data. Enligt artikel 22 ska Europeiska kommissionen ta fram en regelbok som fastställer ytterligare krav för att bl.a. säkerställa rättigheter för registrerade och datainnehavare i förhållande till dataaltruismorganisationer och säkerhetsmässiga krav för att skydda data. Vad som avses med registrerad och datainnehavare framgår av artikel 2 i förordningen.

Artikel 31 i EU:s dataförvaltningsförordning reglerar förutsättningarna för internationell tillgång och överföring av vissa skyddade data. Av bestämmelserna följer bl.a. att erkända dataaltruismorganisationer ska vidta åtgärder för att förhindra internationell överföring av eller statlig tillgång till andra data än personuppgifter (icke-personuppgifter) om en sådan överföring eller tillgång skulle strida mot unionsrätten eller den nationella rätten.

En varning bör alltid meddelas i samband med att tillsynsmyndigheten överväger att besluta att återkalla rätten att använda beteckningen dataaltruismorganisation som är erkänd i unionen och att avlägsna dataaltruismorganisationen från offentliga nationella register och offentliga unionsregister enligt artikel 24.5 i EU:s dataförvaltningsförordning, om överträdelsen grundar sig i någon av artiklarna 18, 20, 21 eller 22.

## **Föreläggande och vite**

**8 §** Tillsynsmyndigheten får besluta de förelägganden som behövs för att EU:s dataförvaltningsförordning, denna lag eller föreskrifter som har meddelats i avslutning till lagen ska följas.

Tillsynsmyndigheten får förena ett föreläggande enligt artikel 14 i EU:s dataförvaltningsförordning med vite.

Paragrafen innehåller bestämmelser om när tillsynsmyndigheten får meddela förelägganden och när sådana förelägganden får förenas med vite. Övervägandena finns i avsnitt 6.3.1.

Tillsynsmyndigheten utövar tillsyn över vidareutnyttjare, leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer enligt lagen och EU:s dataförvaltningsförordning. Tillsynsmyndigheten kan meddela de förelägganden som behövs för att bl.a. utöva sin tillsynsverksamhet. Myndigheten kan t.ex. besluta om ett föreläggande för att få en leverantör av dataförmedlingstjänster att upphöra med en överträdelse av ett eller flera av kraven i kapitel III i EU:s dataförvaltningsförordning (artikel 14.4). Myndigheten kan också förelägga vidareutnyttjare, leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer att komma in med uppgifter för att kontrollera att kraven i artikel 31 i EU:s dataförvaltningsförordning uppfylls.

Det är endast förelägganden som riktar sig till leverantörer av dataförmedlingstjänster enligt artikel 14 i EU:s dataförvaltningsförordning som får förenas med vite. Allmänna bestämmelser om vite finns i lagen (1985:206) om viten.

### **Sanktionsavgift**

**9 §** Tillsynsmyndigheten ska ta ut en sanktionsavgift från en leverantör av dataförmedlingstjänster vid överträdelser av

- anmälningsskyldigheten enligt artikel 11,
- villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12, eller
- villkoren för överföring av andra data än personuppgifter till tredjeland enligt artikel 31 i EU:s dataförvaltningsförordning.

Om det kan anses tillräckligt får tillsynsmyndigheten, i stället för att ta ut en sanktionsavgift vid överträdelser enligt första stycket, meddela en varning enligt 5 §.

Paragrafen reglerar tillsynsmyndighetens möjlighet att ta ut en sanktionsavgift från en leverantör av dataförmedlingstjänster. Övervägandena finns i avsnitt 6.3.2.

Tillsynsmyndigheten är enligt 2 § behörig myndighet för dataförmedlingstjänster.

Anmälningsskyldigheten i artikel 11 i EU:s dataförvaltningsförordning innebär att leverantörer av dataförmedlingstjänster som avser att tillhandahålla dataförmedlingstjänster ska lämna en anmälan till den behöriga myndigheten för dataförmedlingstjänster. Artikel 11 reglerar bl.a. vad en anmälan ska innehålla och till vilken medlemsstat anmälan ska göras. I artikel 12 finns villkor för att få tillhandahålla dataförmedlingstjänster. De avser t.ex. hur de kommersiella villkoren för dataförmedlingstjänsten får vara utformade (artikel 12 b), att det vidtas tillräckliga åtgärder för att säkerställa att data inte används i strid med t.ex. unionsrätten (artikel 12 j) och att det förs ett loggregister över dataförmedlingsverksamheten (artikel 12 o). Artikel 31 reglerar förutsättningarna för internationell tillgång och överföring av vissa skyddade data. Av bestämmelserna följer bl.a. att leverantörer av dataförmedlingstjänster ska vidta åtgärder för att förhindra internationell överföring av eller statlig tillgång till andra data än personuppgifter (icke-personuppgifter), om en sådan överföring eller tillgång skulle strida mot unionsrätten eller den nationella rätten. Sanktionsavgiften bygger på strikt ansvar.

När det gäller valet av sanktion framgår av paragrafen att utgångspunkten är att en sanktionsavgift ska beslutas. I andra stycket anges att tillsynsmyndigheten, om det kan anses tillräckligt, i stället för sanktionsavgift får meddela en varning. Tillsynsmyndigheten kan också avstå från att besluta om en sanktionsavgift om överträdelserna är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften (11 §). Varning är t.ex. avsedd att meddelas vid mindre allvarliga överträdelser, se kommentaren till 5 §.

**10 §** Tillsynsmyndigheten ska ta ut en sanktionsavgift av en fysisk eller juridisk person som har beviljats rätten att vidareutnyttja andra data än personuppgifter för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.



Om det kan anses tillräckligt får tillsynsmyndigheten, i stället för att ta ut en sanktionsavgift vid överträdelse enligt första stycket, meddela en varning enligt 6 §.

Paragrafen reglerar tillsynsmyndighetens möjlighet att ta ut en sanktionsavgift av en fysisk eller juridisk person som har beviljats rätten att vidareutnyttja andra data än personuppgifter. Övervägandena finns i avsnitt 6.3.2.

Av artikel 5.14 följer att fysiska eller juridiska personer som beviljats rätten att vidareutnyttja andra data än personuppgifter (icke-personuppgifter) endast får överföra dessa data till tredjeländer i enlighet med kraven i artiklarna 10, 12 och 13 i EU:s dataförvaltningsförordning. Sanktionsavgiften bygger på strikt ansvar.

När det gäller valet av sanktion framgår av paragrafen att utgångspunkten är att en sanktionsavgift ska beslutas. I andra stycket anges emellertid att tillsynsmyndigheten, om det kan anses tillräckligt, i stället för sanktionsavgift får meddela en varning. Varning är t.ex. avsedd att meddelas vid mindre allvarliga överträdelse, se kommentaren till 6 §. Tillsynsmyndigheten kan också i vissa fall avstå från att besluta om en sanktionsavgift (se 11 §).

**11 §** En sanktionsavgift enligt 9 eller 10 § ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

När avgiftens storlek bestäms ska hänsyn tas till

1. överträdelsens art, allvar, omfattning och varaktighet,
2. åtgärder som har vidtagits för att begränsa eller avhjälpa den skada som överträdelsen har orsakat,
3. tidigare överträdelse,
4. de ekonomiska vinster som har gjorts eller de förluster som har undvikits till följd av överträdelsen, och
5. försvårande eller förmildrande omständigheter utöver dem i 1–4.

Tillsynsmyndigheten får avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

I paragrafen regleras sanktionsavgiftens storlek. Övervägandena finns i avsnitt 6.3.3.

I *första stycket* regleras det lägsta respektive det högsta belopp som en sanktionsavgift enligt 9 eller 10 § ska uppgå till.

Av *andra stycket* framgår sådana omständigheter som ska beaktas när sanktionsavgiftens storlek bestäms. Uppräkningen i bestämmelsen är inte uttömmande. De omständigheter som räknas upp i punktlistan följer artikel 34 i EU:s dataförvaltningsförordning.

När det gäller överträdelsens art och allvar kan hänsyn tas till både det slag av överträdelse som är föremål för bedömning och till det mått av systematiskt handlande som ligger bakom överträdelsen. Vid bedömning av överträdelsens omfattning och varaktighet kan det finnas anledning att särskilt beakta om tillsynsmyndigheten utfärdat en varning för samma överträdelse. Åtgärder som kan ha vidtagits för att begränsa eller avhjälpa den skada som överträdelsen har orsakat kan t.ex. vara att leverantören av dataförmedlingstjänster eller en vidareutnyttjare har underrättat tillsynsmyndigheten om överträdelsen i syfte att begränsa skadan. Tidigare över-

trädelser ska beaktas i försvårande riktning. Det kan röra sig såväl om överträdelser av samma slag, som andra överträdelser för vilka sanktionsavgift kan utgå. Vidare ska särskild hänsyn tas till de ekonomiska vinster som har gjorts eller de förluster som har undvikits till följd av överträdelser. Slutligen ska även andra försvårande och förmildrande omständigheter beaktas när avgiftens storlek ska bestämmas. Det kan t.ex. vara omfattningen av den skada som överträdelserna orsakat registrerade eller datainnehavare. Vad som avses med registrerad och datainnehavare framgår av artikel 2 i EU:s dataförvaltningsförordning.

Enligt *tredje stycket* får tillsynsmyndigheten avstå från att ta ut sanktionsavgiften helt eller delvis om överträdelserna är ringa eller ursäktlig eller om det skulle vara oskäligt att ta ut avgiften. Ett skäl att sätta ned avgiften kan vara att leverantören av dataförmedlingstjänster eller en vidareutnyttjare har gjort allt som rimligen kan krävas för att förhindra den uppkomna skadan. Befrielse kan också övervägas när det är fråga om rena engångsföreteelser som inte ger intryck av att vara särskilt allvarliga och som inte har fått några uppenbara, eller i vart fall inte avsevärda, negativa konsekvenser. I rena bagatellartade fall bör någon avgift inte utgå.

En sanktionsavgift bör vidare kunna sättas ned helt eller delvis om exempelvis en leverantör av dataförmedlingstjänster eller en vidareutnyttjare drabbas av flera sanktionsavgifter vid samma provningstillfälle och den samlade reaktionen skulle bli alltför betungande. Det bör dock inte anses oskäligt att ta ut en sanktionsavgift enbart på grund av att överträdelserna exempelvis berott på att en leverantör av dataförmedlingstjänster eller en vidareutnyttjare inte känt till reglerna eller på grund av dålig ekonomi, tidsbrist eller bristande rutiner.

Frågan om en avgift ska sättas ned får avgöras efter en helhetsbedömning utifrån omständigheterna i det enskilda fallet. Möjligheten att sätta ned avgiften är en undantagsbestämmelse och bör tillämpas restriktivt.

**12 §** En sanktionsavgift får inte tas ut om överträdelserna omfattas av ett föreläggande som har förenats med vite och överträdelserna ligger till grund för en ansökan om utdömmande av vitet.

Paragrafen reglerar när en sanktionsavgift inte får tas ut. Övervägandena finns i avsnitt 6.3.2.

Av paragrafen framgår att en sanktionsavgift inte får beslutas om överträdelserna omfattas av ett föreläggande som har förenats med vite och överträdelserna ligger till grund för en ansökan om utdömmande av vitet.

**13 §** En sanktionsavgift får tas ut endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från den dag då överträdelserna ägde rum.

Ett beslut om sanktionsavgift ska delges.

I paragrafen regleras den borte tidsgränsen för när en sanktionsavgift får beslutas. Övervägandena finns i avsnitt 6.3.4.

En sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från den dag då överträdelserna ägde rum. För att någon ska anses ha fått tillfälle att yttra sig måste denne enligt 25 § förvaltningslagen (2017:900) ha underrättats om allt material av

betydelse för beslutet och fått tillfälle att inom en bestämd tid yttra sig över materialet. Bevisbördan för att detta har skett ligger på tillsynsmyndigheten. Tidsfristen räknas från när överträdelsen, dvs. den otillåtna eller felaktiga handlingen, ägde rum. När det gäller pågående överträdelser börjar preskriptionstiden löpa först när överträdelsen har upphört. Syftet med att ge den som avgiften ska tas ut av tillfälle att yttra sig är att ge denne möjlighet att påtala eventuella felaktigheter och omständigheter i utredningsmaterialet som kan utgöra skäl för befrielse från avgift innan beslut fattas.

Bestämmelser om delgivning finns i delgivningslagen (2010:1932).

**14 §** En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i tid, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

Paragrafen innehåller bestämmelser om betalningen av en sanktionsavgift. Övervägandena finns i avsnitt 6.3.4.

Av *andra stycket* framgår att tillsynsmyndigheten ska lämna en sanktionsavgift för indrivning om avgiften inte betalas i tid. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

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

Paragrafen reglerar preskriptionstiden för en sanktionsavgift. Övervägandena finns i avsnitt 6.3.4.

Enligt paragrafen faller en beslutad sanktionsavgift bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet fick laga kraft. Preskriptionstiden är absolut. Innebörden av detta är att fullgörande inte kan krävas efter det att fem år har gått sedan beslutet fått laga kraft, även om verkställighet har skett under femårsperioden avseende en del av avgiften. Det som preskriberas är den del av avgiften som ännu inte drivits in.

## **Avgifter**

**16 §** Tillsynsmyndigheten får ta ut avgifter från leverantörer av dataförmedlingstjänster för anmälan, registerhållning och tillsyn av leverantörer av dataförmedlingstjänster enligt EU:s dataförvaltningsförordning och denna lag.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om avgifterna.

Paragrafen reglerar möjligheten för tillsynsmyndigheten att ta ut avgifter från leverantörer av dataförmedlingstjänster. Övervägandena finns i avsnitt 6.4.

## Överklagande

**17 §** Tillsynsmyndighetens beslut enligt artiklarna 14, 19 och 24 i EU:s dataförvaltningsförordning eller enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen innehåller bestämmelser om överklagande av vissa beslut enligt EU:s dataförvaltningsförordning och av beslut som fattas med stöd av lagen. Övervägandena finns i avsnitt 6.5.

## 9.2 Förslaget till lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data

### 1 kap.

*1 a § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), i denna lag benämnd EU:s dataförvaltningsförordning.*

Paragrafen, som är ny, innehåller en upplysning om att lagen kompletterar EU:s dataförvaltningsförordning. Övervägandena finns i avsnitt 5.

Hänvisningen till EU:s dataförvaltningsförordning är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

**2 §** Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data eller skyddade data eller som begränsar en sådan rätt.

Lagen påverkar inte heller tillämpningen av bestämmelser i någon annan lag eller förordning om skyddet av personuppgifter.

Paragrafen anger hur lagen förhåller sig till författningar som reglerar tillgång till data eller skyddade data och skyddet av personuppgifter (se prop. 2021/22:225 s. 71 och 72). Övervägandena finns i avsnitt 5.2.

Ändringen i *första stycket* innebär att paragrafen även omfattar skyddade data enligt EU:s dataförvaltningsförordning. Vad som avses med skyddade data framgår av 4 §.

**3 §** Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data eller skyddade data än i denna lag, ska de kraven tillämpas.

Paragrafen anger hur lagen förhåller sig till författningar som reglerar hur data ska göras tillgängliga (se prop. 2021/22:225 s. 72). Övervägandena finns i avsnitt 5.2.

Ändringen i *första stycket* innebär att paragrafen även omfattar skyddade data enligt EU:s dataförvaltningsförordning. Vad som avses med skyddade data framgår av 4 §.

**4 §** I lagen avses med

*begäran om tillgängliggörande av data för vidareutnyttjande*: en begäran om att data eller skyddade data ska göras tillgängliga för vidareutnyttjande i enlighet med denna lag eller kapitel II i EU:s dataförvaltningsförordning,

*bulknedladdning*: nedladdning av en avgränsad datamängd,

*data*: information i digitalt format oberoende av medium,

*dynamiska data*: data som uppdateras ofta eller i realtid för att vara aktuella och relevanta att vidareutnyttja,

*forskningsdata*: data som till någon del är offentligt finansierade, som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet och som görs direkt tillgängliga för vidareutnyttjande genom en dataplattform som är allmänt åtkomlig,

*gränssnitt*: en regeluppsättning för dynamiskt datautbyte mellan programvaror,

*maskinläsbart format*: ett filformat som är strukturerat på ett sådant sätt att det enkelt kan läsas av ett datorprogram,

*offentligt företag*: ett företag som en eller flera myndigheter har ett bestämmande inflytande över och som är verksam

– inom de sektorer som framgår av 2 kap. 1 § och 5–8 §§ lagen (2016:1146) om upphandling inom försörjningssektorerna,

– som ett kollektivtrafikföretag enligt Europaparlamentets och rådets förordning (EG) nr 1370/2007 av den 23 oktober 2007 om kollektivtrafik på järnväg och väg och om upphävande av rådets förordning (EEG) nr 1191/69 och (EEG) nr 1107/70,

– som ett lufttrafikföretag som har allmän trafikplikt enligt artikel 16 i Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen, eller

– som ett rederi inom gemenskapen som uppfyller förpliktelser vid allmän trafik enligt artikel 4 i rådets förordning (EEG) nr 3577/92 av den 7 december 1992 om tillämpning av principen om frihet att tillhandahålla tjänster på sjötransportområdet inom medlemsstaterna (cabotage),

*offentligt styrt organ*: ett sådant organ som avses i 1 kap. 18 § lagen (2016:1145) om offentlig upphandling eller en sammanslutning av sådana organ,

*skyddade data*: sådana kategorier av data som avses i artikel 3.1 i EU:s dataförvaltningsförordning,

*vidareutnyttjande*: bearbetning av data från den offentliga sektorn för valfritt ändamål,

*värdefull datamängd*: data som förtecknas i en genomförandeakt som har meddelats med stöd av artikel 14.1 i öppna data-direktivet,

*öppna data-direktivet*: Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

I paragrafen definieras olika ord och uttryck i lagen (prop. 2021/22:225 s. 73–75). Övervägandena finns i avsnitt 5.2.

Ändringen i första stycket innebär att definitionen begäran om tillgängliggörande av data för vidareutnyttjande även omfattar skyddade data enligt EU:s dataförvaltningsförordning. Vidare införs skyddade data som ett nytt uttryck i lagen. Med skyddade data ska förstås sådana kategorier av data som avses i artikel 3.1 i EU:s dataförvaltningsförordning. Med skyddade data enligt artikel 3.1 i förordningen avses data som innehas av offentliga myndigheter och som är skyddade på grund av insynsskydd för kommersiella uppgifter, inklusive affärs-, yrkes- och företagshemligheter, insynsskydd för statistiska uppgifter, skydd av tredje parts immateriella rättigheter och skydd av personuppgifter, i den mån sådana uppgifter faller utanför tillämpningsområdet för Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

*7 a § Bestämmelserna om vidareutnyttjande av skyddade data ska endast tillämpas av myndigheter, dock inte av kultur- eller utbildningsinstitutioner.*

Paragrafen, som är ny, reglerar vilka som ska tillämpa lagens bestämmelser om vidareutnyttjande av skyddade data. Övervägandena finns i avsnitt 5.1.

Bestämmelserna om vidareutnyttjande av skyddade data ska endast tillämpas av myndigheter, vilket även följer av artikel 3.1 i EU:s dataförvaltningsförordning. Kultur- och utbildningsinstitutioner undantas uttryckligen från tillämpningsområdet för bestämmelserna om vidareutnyttjande av skyddade data enligt lagen. Det följer av artikel 3.1 i förordningen att bestämmelserna om vidareutnyttjande av skyddade data inte ska gälla för data som innehas av kultur- eller utbildningsinstitutioner.

## **8 § Lagen ska tillämpas**

1. när någon som har rätt att få tillgång till data *eller skyddade data* enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,

2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas,

3. när en myndighet på eget initiativ tillgängliggör skyddade data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, eller

4. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.

Trots första stycket ska lagen inte tillämpas

1. när data, i andra fall än som avses i första stycket 4, lämnas

a) mellan statliga och kommunala myndigheter,

b) från ett organ som enligt 1 kap. 5 § andra stycket jämföras med en myndighet eller ett offentligt företag till en statlig eller kommunal myndighet, eller

2. när en statlig eller kommunal myndighet tillhandahåller data i en konkurrensutsatt verksamhet.

Paragrafen klargör när lagen ska tillämpas (se prop. 2021/22:225 s. 77–79). Övervägandena finns i avsnitt 5.3.

Ändringen i *första stycket första punkten* innebär att lagen även ska tillämpas när någon som har rätt att få tillgång till skyddade data enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av sådan data för vidareutnyttjande.

*Första stycket tredje punkten*, som är ny, innebär att lagen ska tillämpas när en myndighet på eget initiativ tillgängliggör skyddade data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas. *Fjärde punkten* motsvarar nuvarande tredje punkten.

I *andra stycket första punkten* justeras hänvisningen till den nya fjärde punkten i första stycket.

## **2 kap.**

*5 a § En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska ställa upp villkor för vidareutnyttjandet i enlighet med artikel 5 i EU:s dataförvaltningsförordning.*

*En myndighet som tillgängliggör skyddade data till en vidareutnyttjare som avser att överföra dem till tredjeland i enlighet med artikel 5.10 i EU:s dataförvaltningsförordning är skyldig att anmäla de överträdelser av artikel 5.14 som myn-*

*digheten får kännedom om till tillsynsmyndigheten enligt lagen (2024:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.*

Paragrafen, som är ny, innehåller bestämmelser om villkor som en myndighet ska ställa upp vid tillgängliggörande av skyddade data för vidareutnyttjande och om en anmälningsskyldighet för tillgängliggörande myndigheter vid vissa överträdelse. Övervägandena finns i avsnitt 5.4 och 5.5.

Av artikel 5 följer bl.a. att de villkor som myndigheten ställer upp ska vara icke-diskriminerande, transparenta, proportionerliga och objektivt motiverade med hänsyn till den data som vidareutnyttjandet gäller.

För att anmälningsskyldigheten enligt *andra stycket* ska bli aktuell krävs att myndigheten har tillgängliggjort vissa typer av skyddade data för överföring till tredje land.

De överträdelse som ska anmälas är överträdelse enligt artikel 5.14 i EU:s dataförvaltningsförordning, som i sin tur hänvisar till artiklarna 5.10, 5.12 och 5.13. Artikel 5.10 innebär att en myndighet som tillåter vidareutnyttjare att överföra vissa kategorier av skyddade data till tredjeländ i vissa fall ska ställa upp avtalsmässiga villkor till vidareutnyttjaren. Artikel 5.12 reglerar en möjlighet för Europeiska kommissionen att anta genomförandeakter i vilka det bl.a. intygas att ett tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang säkerställer skydd för immateriella rättigheter och företagshemligheter. Av artikel 5.13 följer att kommissionen i vissa fall ska anta delegerade akter, som kompletterar förordningen, genom att fastställa särskilda villkor som ska tillämpas på överföring till tredjeländer av vissa kategorier av data, som inte är personuppgifter (icke-personuppgifter), som anses vara mycket känsliga.

För att myndigheten ska ha en skyldighet att anmäla överträdelse enligt artikel 5.14 i EU:s dataförvaltningsförordning krävs att myndigheten efter tillgängliggörandet fått kännedom om att vidareutnyttjaren har gjort sig skyldig till överträdelse av artikel 5.14.

### ***En gemensam informationspunkt***

**6 a §** *Den myndighet som regeringen bestämmer ska tillhandahålla en gemensam informationspunkt enligt artikel 8 i EU:s dataförvaltningsförordning.*

*En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska informera den myndighet som tillhandahåller den gemensamma informationspunkten om sådana data och villkoren för vidareutnyttjande av dessa.*

Paragrafen är ny och innehåller bestämmelser om den gemensamma informationspunkten enligt artikel 8 i EU:s dataförvaltningsförordning. Övervägandena finns i avsnitt 5.9.

Av EU:s dataförvaltningsförordning följer att den gemensamma informationspunkten ska tillhandahålla en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor tillsammans med relevant information som beskriver tillgängliga data, inbegripet åtminstone dataformatet och datastorleken samt villkoren för vidareutnyttjandet av dessa data (artikel 8.2). Den myndighet som tillgängliggör skyddade data för vidareutnyttjande enligt förordningen ska informera den myndighet som tillhandahåller den gemensamma informationspunkten om de uppgifter som ska tillhandahållas i den sökbara tillgångsförteckningen enligt artikel 8.2.

### **Behöriga organ enligt EU:s dataförvaltningsförordning**

*7 § Den eller de myndigheter som regeringen bestämmer ska vara behöriga organ enligt artikel 7 i EU:s dataförvaltningsförordning.*

Paragrafen, som är ny, innehåller bestämmelser om vilken eller vilka myndigheter som ska vara behöriga organ enligt EU:s dataförvaltningsförordning. Övervägandena finns i avsnitt 5.8.

### **3 kap.**

*1 a § En myndighet som innehar skyddade data får ge någon en exklusiv rätt att vidareutnyttja dessa data endast om det är tillåtet enligt artikel 4 i EU:s dataförvaltningsförordning.*

Paragrafen, som är ny, innehåller en upplysning om bestämmelserna i artikel 4 i EU:s dataförvaltningsförordning. Övervägandena finns i avsnitt 5.4.

Av artikel 4 i EU:s dataförvaltningsförordning framgår att huvudregeln är att exklusiva avtal är förbjudna. Enligt paragrafen får en myndighet som innehar skyddade data endast ge någon en exklusiv rätt att vidareutnyttja dessa data i den mån det är tillåtet enligt artikel 4.

### **4 kap.**

*2 a § En myndighet som tillgängliggör skyddade data för vidareutnyttjande får ta ut en avgift för tillgängliggörandet.*

*Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om avgiften.*

Paragrafen, som är ny, innehåller en rätt att ta ut en avgift för tillgängliggörande av skyddade data. Övervägandena finns i avsnitt 5.6.

### **5 kap.**

*1 § En myndighet ska inom fyra veckor avgöra ett ärende till följd av en begäran om tillgängliggörande av data för vidareutnyttjande.*

*Om en sådan begäran avser skyddade data ska ärendet avgöras inom åtta veckor.*

Tidsfristen enligt första eller andra stycket får förlängas med ytterligare fyra veckor, om en begäran är omfattande eller komplicerad. Myndigheten ska underrätta sökanden om förlängningen och redovisa skälen för den senast tre veckor från den dag då begäran kom in.

Paragrafen anger vilka tidsfrister som gäller vid handläggningen av ett ärende om tillgängliggörande av data (se prop. 2021/22:225 s. 94). Övervägandena finns i avsnitt 5.7.

Av *andra stycket*, som är nytt, framgår vilka tidsfrister som gäller vid handläggningen av ett ärende till följd av en begäran om tillgängliggörande av skyddade data. I sådana ärenden gäller i stället för vad som sägs i första stycket att ett ärende ska avgöras senast åtta veckor från den dag begäran kom in.

I *tredje stycket* förtydligas att möjligheten till förlängning gäller även det nya andra stycket.



## I

(Lagstiftningsakter)

## FÖRORDNINGAR

## EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2022/868

av den 30 maj 2022

om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

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 <sup>(1)</sup>,

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet <sup>(2)</sup>, och

av följande skäl:

- (1) I enlighet med fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ska en inre marknad inrättas och en ordning skapas som säkerställer att konkurrensen på den inre marknaden inte snedvrids. Fastställande av gemensamma regler och gemensam praxis i medlemsstaterna för utformning av en ram för dataförvaltning bör bidra till att dessa mål uppnås, samtidigt som grundläggande rättigheter respekteras fullt ut. Förstärkningen av unionens öppna strategiska oberoende bör också garanteras och ett internationellt fritt dataflöde samtidigt främjas.
- (2) Under det senaste årtiondet har den digitala tekniken förändrat ekonomin och samhället genom sin inverkan på alla verksamhetssektorer och det dagliga livet. I centrum för den omvandlingen står data: data driven innovation kommer att medföra enorma fördelar för både unionsmedborgare och ekonomin, till exempel genom förbättrad medicin och precisionsmedicin, genom tillhandahållande av ny mobilitet och genom dess bidrag till kommissionens meddelande av den 11 december 2019 om den europeiska gröna given. För att göra den datadrivna ekonomin inkluderande för alla unionsmedborgare måste särskild uppmärksamhet ägnas åt att minska den digitala klyftan, stimulera kvinnors deltagande i dataekonomin och främja europeisk spetskompetens inom tekniksektorn. Dataekonomin måste byggas på ett sätt som möjliggör välmående företag, särskilt mikroföretag och små och medelstora företag enligt definitionen i bilagan till kommissionens rekommendation 2003/361/EG <sup>(3)</sup> samt nystartade företag, där neutral dataåtkomst, dataportabilitet och interoperabilitet säkerställs och inläsningseffekter undviks. I sitt meddelande av den 19 februari 2020 om en EU-strategi för data (*EU-strategin för data*) beskrev kommissionen visionen om ett gemensamt europeiskt dataområde, som innebär en inre marknad för data, där data kan användas i enlighet med gällande lagstiftning oavsett var i unionen de fysiskt lagras, vilket bland annat skulle kunna vara avgörande för den snabba utvecklingen av teknik för artificiell intelligens.

<sup>(1)</sup> EUT C 286, 16.7.2021, s. 38.

<sup>(2)</sup> Europaparlamentets ståndpunkt av den 6 april 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 16 maj 2022.

<sup>(3)</sup> Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

Kommissionen efterlyste också ett fritt och säkert dataflöde med tredjeländer, med undantag och inskränkningar som rör allmän säkerhet, allmän ordning och andra legitima mål för unionens offentliga politik, i enlighet med internationella åtaganden, inbegripet om grundläggande rättigheter. För att förverkliga denna vision föreslog kommissionen att det inrättas domänspecifika gemensamma europeiska dataområden för datadelning och datapooling. I EU-strategin för data föreslås att sådana gemensamma europeiska dataområden skulle kunna omfatta områden såsom hälsa, mobilitet, tillverkning, finansiella tjänster, energi eller jordbruk, eller en kombination av sådana områden, till exempel energi och klimat, samt tematiska områden såsom den europeiska gröna given eller europeiska dataområden för offentlig förvaltning eller kompetens. Gemensamma europeiska dataområden bör göra data sökbara, tillgängliga, interoperabla och möjliga att vidareutnyttja (*Fairdataprinciperna*) och samtidigt säkerställa en hög nivå på cybersäkerheten. När det råder likvärdiga förutsättningar i dataekonomin konkurrerar företagen om tjänsternas kvalitet, inte om mängden data som de kontrollerar. I syfte att utforma, skapa och behålla likvärdiga förutsättningar i dataekonomin behövs sund styrning där de berörda parterna i ett gemensamt europeiskt dataområde behöver samarbeta och vara representerade.

- (3) Det är nödvändigt att förbättra villkoren för datadelning på den inre marknaden genom att skapa en harmoniserad ram för utbyte av data och föreskriva vissa grundläggande krav på dataförvaltning, med särskild omsorg om att underlätta samarbetet mellan medlemsstaterna. Denna förordning bör syfta till att vidareutveckla den gränslösa digitala inre marknaden samt ett datasamhälle och en dataekonomi som ställer människan i centrum och präglas av förtroende och säkerhet. Genom sektorspecifik unionsrätt kan, beroende på sektorns särdrag, nya och kompletterande delar utvecklas, anpassas och föreslås, såsom den planerade unionsrätten om det europeiska hälsodataområdet och om tillgång till fordonsdata. Dessutom regleras vissa sektorer av ekonomin redan av sektorspecifik unionsrätt som omfattar regler om den gränsöverskridande eller unionsomfattande delningen av eller tillgången till data, till exempel Europaparlamentets och rådets direktiv 2011/24/EU (\*) inom ramen för det europeiska hälsodataområdet, och relevanta lagstiftningsakter på transportområdet, till exempel Europaparlamentets och rådets förordningar (EU) 2019/1239 (†) och (EU) 2020/1056 (‡) samt Europaparlamentets och rådets direktiv 2010/40/EU (§) inom ramen för det europeiska dataområdet för rörlighet.

(\*) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

(†) Europaparlamentets och rådets förordning (EU) 2019/1239 av den 20 juni 2019 om inrättande av en europeisk kontaktpunkt för sjöfart och om upphävande av direktiv 2010/65/EU (EUT L 198, 25.7.2019, s. 64).

(‡) Europaparlamentets och rådets förordning (EU) 2020/1056 av den 15 juli 2020 om elektronisk godstransportinformation (EUT L 249, 31.7.2020, s. 33).

(§) Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (EUT L 207, 6.8.2010, s. 1).

Denna förordning bör därför inte påverka Europaparlamentets och rådets förordningar (EG) nr 223/2009<sup>(9)</sup>, (EU) 2018/858<sup>(10)</sup> och (EU) 2018/1807<sup>(11)</sup> samt direktiv 2000/31/EG<sup>(12)</sup>, 2001/29/EG<sup>(13)</sup>, 2004/48/EG<sup>(14)</sup>, 2007/2/EG<sup>(15)</sup>, 2010/40/EU, (EU) 2015/849<sup>(16)</sup>, (EU) 2016/943<sup>(17)</sup>, (EU) 2017/1132<sup>(18)</sup>, (EU) 2019/790<sup>(19)</sup> och (EU) 2019/1024<sup>(20)</sup> samt annan sektorsspecifik unionsrätt som reglerar tillgång till och vidareutnyttjande av data. Denna förordning bör inte påverka unionsrätten och nationell rätt om tillgång till och användningen av data för förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga åtgärder och inte heller det internationella samarbetet i det sammanhanget.

Denna förordning bör inte påverka medlemsstaternas befogenheter när det gäller deras verksamhet som rör allmän säkerhet, försvar och nationell säkerhet. Vidareutnyttjandet av data som är skyddade av sådana skäl och innehas av offentliga myndigheter, inbegripet data från upphandlingsförfaranden som omfattas av tillämpningsområdet för Europaparlamentets och rådets direktiv 2009/81/EG<sup>(21)</sup>, bör inte omfattas av denna förordning. Ett övergripande system för vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter och tillhandahållande av dataförmedlingstjänster och tjänster baserade på dataaltruism i unionen bör inrättas. De olika sektorernas särdrag kan göra att det behöver skapas sektorsspecifika databaserade system, som samtidigt ska bygga på kraven i denna förordning. Leverantörer av dataförmedlingstjänster som uppfyller kraven i denna förordning bör kunna använda beteckningen "leverantör av dataförmedlingstjänster som är erkända i unionen". Juridiska personer som vill stödja mål av allmänt intresse genom att tillhandahålla relevanta data baserat på dataaltruism i större skala och som uppfyller de krav som fastställs i denna förordning, bör kunna registrera sig som och använda beteckningen "dataaltruismorganisation som är erkänd i unionen". Om sektorsspecifik unionsrätt eller nationell rätt kräver att offentliga myndigheter, sådana leverantörer av dataförmedlingstjänster eller sådana juridiska personer (erkända dataaltruismorganisationer) uppfyller specifika ytterligare tekniska, administrativa eller organisatoriska krav, däribland genom ett auktorisations- eller certifieringssystem, bör de bestämmelserna i den sektorsspecifika unionsrätten eller nationella rätten också gälla.

<sup>(9)</sup> Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

<sup>(10)</sup> Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknads kontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG (EUT L 151, 14.6.2018, s. 1).

<sup>(11)</sup> Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (EUT L 303, 28.11.2018, s. 59).

<sup>(12)</sup> Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informations-samhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EGT L 178, 17.7.2000, s. 1).

<sup>(13)</sup> Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informations-samhället (EGT L 167, 22.6.2001, s. 10).

<sup>(14)</sup> Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter (EUT L 157, 30.4.2004, s. 45).

<sup>(15)</sup> Europaparlamentets och rådets direktiv 2007/2/EG av den 14 mars 2007 om upprättande av en infrastruktur för rumslig information i Europeiska gemenskapen (Inspire) (EUT L 108, 25.4.2007, s. 1).

<sup>(16)</sup> Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG (EUT L 141, 5.6.2015, s. 73).

<sup>(17)</sup> Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

<sup>(18)</sup> Europaparlamentets och rådets direktiv (EU) 2017/1132 av den 14 juni 2017 om vissa aspekter av bolagsrätt (EUT L 169, 30.6.2017, s. 46).

<sup>(19)</sup> Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG (EUT L 130, 17.5.2019, s. 92).

<sup>(20)</sup> Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (EUT L 172, 26.6.2019, s. 56).

<sup>(21)</sup> Europaparlamentets och rådets direktiv 2009/81/EG av den 13 juli 2009 om samordning av förfarandena vid tilldelning av vissa kontrakt för byggentreprenader, varor och tjänster av upphandlande myndigheter och enheter på försvars- och säkerhetsområdet och om ändring av direktiven 2004/17/EG och 2004/18/EG (EUT L 216, 20.8.2009, s. 76).

- (4) Denna förordning bör inte påverka tillämpningen av Europaparlamentets och rådets förordningar (EU) 2016/679<sup>(21)</sup> och (EU) 2018/1725<sup>(22)</sup> och av Europaparlamentets och rådets direktiv 2002/58/EG<sup>(23)</sup> och (EU) 2016/680<sup>(24)</sup> samt motsvarande bestämmelser i nationell rätt, inbegripet då personuppgifter och andra data än personuppgifter i en datamängd är ouplösligt sammanlänkade. Den här förordningen bör i synnerhet inte tolkas som att den skapar en ny rättslig grund för behandling av personuppgifter för någon av de reglerade verksamheterna, eller ändrar de informationskrav som fastställs i förordning (EU) 2016/679. Genomförandet av den här förordningen bör inte förhindra gränsöverskridande överföringar av data i enlighet med kapitel V i förordning (EU) 2016/679. Om den här förordningen står i strid med unionsrätten om skydd av personuppgifter eller nationell rätt som antagits i enlighet med sådan unionsrätt bör relevant unionsrätt eller nationell rätt om skydd av personuppgifter ha företräde. Det bör vara möjligt att betrakta dataskyddsmyndigheter som behöriga myndigheter inom ramen för den här förordningen. Om andra myndigheter fungerar som behöriga myndigheter enligt den här förordningen bör de göra detta på ett sätt som inte påverkar dataskyddsmyndigheternas tillsynsbefogenheter och behörigheter enligt förordning (EU) 2016/679.
- (5) Åtgärder på unionsnivå är nödvändiga för att öka förtroendet för datadelning genom att inrätta lämpliga mekanismer för de registrerades och datainnehavares kontroll över data som avser dem och för att ta itu med andra hinder för en väl fungerande och konkurrenskraftig datadriven ekonomi. Dessa åtgärder bör inte påverka tillämpningen av skyldigheter och åtaganden enligt internationella handelsavtal som ingås av unionen. En unionsomfattande styrningsram bör syfta till att skapa förtroende bland enskilda personer och företag när det gäller tillgång till samt kontroll, delning, användning och vidareutnyttjande av data, särskilt genom att fastställa lämpliga mekanismer för att de registrerade ska känna till sina rättigheter och kunna utöva dem på ett meningsfullt sätt, och när det gäller vidareutnyttjande av vissa typer av data som innehas av offentliga myndigheter, tillhandahållande av tjänster från leverantörer av dataförmedlingstjänster till registrerade, datainnehavare och dataanvändare samt insamling och behandling av data som fysiska och juridiska personer gör tillgängliga för altruistiska ändamål. I synnerhet kan större öppenhet om vad syftet med dataanvändningen är och under vilka villkor företag lagrar data bidra till att stärka förtroendet.
- (6) Tanken att data som har tagits fram eller samlats in av offentliga myndigheter eller andra enheter på offentliga budgetars bekostnad bör gynna samhället har länge varit en del av unionens politik. Genom direktiv (EU) 2019/1024 och sektorspecifik unionsrätt säkerställs att de offentliga myndigheterna gör en större del av de data de producerar lättillgängliga för användning och vidareutnyttjande. Vissa kategorier av data, såsom data som rör affärshemligheter, insynsskyddade statistiska data och data som skyddas av tredje parts immateriella rättigheter, inbegripet företagshemligheter och personuppgifter, i offentliga databaser görs dock ofta inte tillgängliga, inte ens för forskning eller innovativ verksamhet i allmänhetens intresse, trots att sådan tillgänglighet är möjligt i enlighet med tillämplig unionsrätt, särskilt förordning (EU) 2016/679 och direktiven 2002/58/EG och (EU) 2016/680. På grund av sådana datas känslighet måste vissa tekniska och rättsliga förfarandekrav uppfyllas innan de görs tillgängliga, inte minst för att säkerställa att andra personers rättigheter till sådana data iaktas eller för att begränsa den negativa effekten på de grundläggande rättigheterna, principen om icke-diskriminering och dataskyddet. Det är vanligen tidsödande och kunskapsintensiva att uppfylla sådana krav. Detta har lett till ett otillräckligt nyttjande av sådana data. Vissa medlemsstater håller på att inrätta strukturer, processer eller lagstiftning för att underlätta den typen av vidareutnyttjande, men detta är inte fallet i hela unionen. För att underlätta privata och offentliga enheters användning av data för europeisk forskning och innovation behövs tydliga villkor över hela unionen för tillgång till och användning av sådana data.

<sup>(21)</sup> 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) (EUT L 119, 4.5.2016, s. 1).

<sup>(22)</sup> Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

<sup>(23)</sup> Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

<sup>(24)</sup> 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 (EUT L 119, 4.5.2016, s. 89).

- (7) Det finns teknik som möjliggör analyser för databaser som innehåller personuppgifter, såsom anonymisering, differentiell integritet, generalisering, undertryckande och randomisering, användningen av syntetiska data eller liknande metoder och andra toppmoderna integritetsbevarande metoder som kan bidra till en mer integritetsvänlig databehandling. Medlemsstaterna bör ge stöd till offentliga myndigheter så att de kan optimera användningen av sådan teknik och därigenom göra en så stor mängd data som möjligt tillgänglig för delning. Tillämpningen av sådan teknik, tillsammans med övergripande konsekvensbedömningar avseende dataskydd och andra skyddsåtgärder, kan bidra till större säkerhet i användningen och vidareutnyttjandet av personuppgifter och bör kunna säkerställa att företagsdata som rör affärshemligheter kan vidareutnyttjas för forsknings-, innovations- och statistikändamål på ett säkert sätt. I många fall innebär tillämpningen av sådan teknik, sådana konsekvensbedömningar och sådana andra skyddsåtgärder att data endast kan användas och vidareutnyttjas i en säker behandlingsmiljö som tillhandahålls eller kontrolleras av den offentliga myndigheten. Det finns erfarenheter på unionsnivå från sådana säkra behandlingsmiljöer som används för forskning om statistiska mikrodata på grundval av kommissionens förordning (EU) nr 557/2013<sup>(2)</sup>. När det gäller personuppgifter bör behandlingen av dessa i allmänhet baseras på en eller flera av de rättsliga grunder för behandling som anges i artiklarna 6 och 9 i förordning (EU) 2016/679.
- (8) I enlighet med förordning (EU) 2016/679 bör principerna för dataskyddet inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller längre är identifierbar. Återidentifiering av registrerade på grundval av anonymiserade dataset bör vara förbjuden. Detta bör inte påverka möjligheten att bedriva forskning om anonymiseringsteknik, i synnerhet för att säkerställa informationssäkerhet, förbättra befintlig anonymiseringsteknik och bidra till anonymiseringens övergripande robusta karaktär, som genomförs i enlighet med förordning (EU) 2016/679.
- (9) För att underlätta skyddet av personuppgifter och konfidentiella uppgifter och för att påskynda förfarandet med att göra sådana uppgifter tillgängliga för vidareutnyttjande inom ramen för denna förordning bör medlemsstaterna uppmantra de offentliga myndigheterna att ta fram och tillgängliggöra data i enlighet med den princip om *inbyggd öppenhet och öppenhet som standard* som avses i artikel 5.2 i direktiv (EU) 2019/1024 och att främja framställning och upphandling av data i format och strukturer som möjliggör snabb anonymisering.
- (10) De kategorier av data som innehas av offentliga myndigheter och som bör vidareutnyttjas enligt denna förordning faller utanför tillämpningsområdet för direktiv (EU) 2019/1024, som utesluter uppgifter som inte är tillgängliga på grund av insynsskydd för statistiska och kommersiella uppgifter och data som ingår i verk eller andra alster till vilka tredje man innehar immateriella rättigheter. Data som rör affärshemligheter inbegriper data som skyddas av företagshemligheter, skyddad know-how och annan information vars otillbörliga röjande skulle påverka företagets marknadsställning eller finansiella sundhet. Denna förordning bör tillämpas på personuppgifter som faller utanför tillämpningsområdet för direktiv (EU) 2019/1024 i den mån som bestämmelserna om tillgång till handlingar utesluter eller begränsar tillgången till sådana data av skäl som rör dataskydd, privatlivet och den enskilda personens integritet, särskilt i enlighet med dataskyddsbestämmelserna. Vidareutnyttjande av uppgifter som kan innehålla företagshemligheter bör ske utan att det påverkar tillämpningen av direktiv (EU) 2016/943, som fastställer ramen för tillåtet anskaffande, användande eller röjande av företagshemligheter.
- (11) Denna förordning bör inte göra det obligatoriskt att tillåta vidareutnyttjande av data som innehas av offentliga myndigheter. Mer specifikt, bör varje medlemsstat därför kunna besluta om data ska göras tillgängliga för vidareutnyttjande, även i fråga om syftena med och tillämpningsområdet för denna åtkomst. Denna förordning bör komplettera och inte påverka tillämpningen av mer specifika skyldigheter för offentliga myndigheter att tillåta vidareutnyttjande av data som fastställs i sektorsspecifikt unionsrätt eller nationell rätt. Allmänhetens rätt att få tillgång till officiella handlingar kan betraktas som ett allmänt intresse. Med hänsyn till den roll som allmänhetens rätt att få tillgång till officiella handlingar och öppenheten spelar i ett demokratiskt samhälle bör denna förordning inte heller påverka tillämpningen av nationell rätt om beviljande av tillgång till och utlämnande av officiella handlingar. Tillgång till officiella handlingar kan i synnerhet beviljas i enlighet med nationell rätt utan att föreskriva särskilda villkor eller genom att föreskriva särskilda krav som inte föreskrivs i denna förordning.

<sup>(2)</sup> Kommissionens förordning (EU) nr 557/2013 av den 17 juni 2013 om tillämpning av Europaparlamentets och rådets förordning (EG) nr 223/2009 om europeisk statistik vad gäller tillgång till konfidentiella uppgifter för vetenskapliga syften och om upphävande av kommissionens förordning (EG) nr 831/2002 (EUT L 164, 18.6.2013, s. 16).

- (12) Det system för vidareutnyttjande som föreskrivs i denna förordning bör tillämpas på sådana data vars tillhandahållande ingår i den offentliga verksamhet som bedrivs av de berörda offentliga myndigheterna, enligt lag eller andra bindande regler i medlemsstaterna. Om sådana regler saknas bör den offentliga verksamheten fastställas i enlighet med gängse administrativ praxis i medlemsstaterna, förutsatt att den offentliga verksamheten är tydligt avgränsad och föremål för översyn. Den offentliga verksamheten kan fastställas generellt eller från fall till fall för enskilda offentliga myndigheter. Eftersom offentliga företag inte omfattas av definitionen av offentlig myndighet bör de data som innehas av offentliga företag inte omfattas av denna förordning. Data som innehas av kulturinstitutioner, såsom bibliotek, arkiv och museer samt orkestrar, operor, baletter och teatrar, och av utbildningsanstalter bör inte omfattas av denna förordning eftersom de verk och andra handlingar som de innehar till övervägande del omfattas av tredje parts immateriella rättigheter. Organisationer som bedriver forskning och organisationer som finansierar forskning kan också organiseras som offentliga myndigheter eller offentligrättsliga organ.

Denna förordning bör tillämpas på sådana hybridorganisationer endast i deras egenskap av organisationer som bedriver forskning. Om en organisation som bedriver forskning innehar data som en del av en specifik offentlig-privat sammanslutning med organisationer från den privata sektorn eller andra offentliga myndigheter, offentlig-rättsliga organ eller hybridorganisationer som bedriver forskning, dvs. som är organiserade som antingen offentliga myndigheter eller offentliga företag, med bedrivande av forskning som huvudsakligt syfte, bör inte heller dessa data omfattas av denna förordning. I relevanta fall bör medlemsstaterna kunna tillämpa denna förordning på offentliga företag eller privata företag som utför uppdrag inom offentlig sektor eller tillhandahåller tjänster av allmänt intresse. Utbytet av data, helt och hållet inom ramen för fullgörandet av deras offentliga uppdrag, mellan offentliga myndigheter i unionen eller mellan offentliga myndigheter i unionen och offentliga myndigheter i tredjeländer eller internationella organisationer, samt utbytet av data mellan forskare för icke-kommersiella vetenskapliga forskningsändamål, bör inte omfattas av bestämmelserna i denna förordning om vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter.

- (13) Offentliga myndigheter bör följa konkurrensrätten när de fastställer principerna för vidareutnyttjande av data som de innehar, och undvika att ingå avtal vars syfte eller verkan kan vara att skapa exklusiva rättigheter för vidareutnyttjande av vissa data. Sådana avtal bör endast vara möjliga om det är motiverat och nödvändigt för tillhandahållandet av en tjänst eller tillhandahållandet av en produkt av allmänt intresse. Detta kan vara fallet om den exklusiva användningen av data är det enda sättet att maximera de samhällliga fördelarna av berörda data, till exempel om det bara finns en enda enhet (som har specialiserat sig på behandling av en viss datamängd) som kan tillhandahålla den tjänst eller produkt som gör det möjligt för den offentliga myndigheten att tillhandahålla en tjänst eller tillhandahålla en produkt av allmänt intresse. Sådana arrangemang bör dock ingås i enlighet med tillämplig unionsrätt eller nationell rätt och bli föremål för regelbunden översyn baserad på en marknadsanalys för att fastställa om en sådan exklusivitet fortfarande är nödvändig. Dessutom bör sådana arrangemang, beroende på vad som är lämpligt, vara förenliga med relevanta regler för statligt stöd och bör ingås för en begränsad period som inte bör överstiga tolv månader. För att säkerställa öppenhet bör sådana exklusiva avtal offentliggöras online i en form som är förenlig med relevant unionsrätt om offentlig upphandling. Om en exklusiv rätt till vidareutnyttjande av data inte är förenlig med denna förordning bör den exklusiva rätten vara ogiltig.
- (14) Förbjudna exklusiva avtal och andra metoder eller arrangemang som rör vidareutnyttjande av data som innehas av offentliga myndigheter och som inte uttryckligen beviljar exklusiva rättigheter men som rimligen kan förväntas begränsa tillgången till data för vidareutnyttjande och som har ingåtts eller redan var införda innan den dag då denna förordning träder i kraft, bör inte förnyas efter det att deras giltighetstid har löpt ut. När det gäller avtal på obestämd tid eller med lång löptid bör de upphöra att gälla inom 30 månader från den dag då denna förordning träder i kraft.
- (15) I denna förordning bör det fastställas villkor för vidareutnyttjande av skyddade data som ska gälla för offentliga myndigheter utsetta till behöriga enligt nationell rätt att bevilja eller vägra tillgång för vidareutnyttjande, och som inte ska påverka rättigheter eller skyldigheter avseende tillgång till sådana data. Dessa villkor bör vara icke-diskriminerande, transparenta, proportionella och objektivt motiverade utan att begränsa konkurrensen, med särskilt fokus på att främja små och medelstora företags och nystartade företags tillgång till sådana data. Villkoren för vidareutnyttjande bör utformas på ett sätt som främjar vetenskaplig forskning så att det, till exempel, som regel bör anses vara icke-diskriminerande att privilegiera vetenskaplig forskning. Offentliga myndigheter som tillåter vidareutnyttjande bör förfoga över de tekniska medel som krävs för att säkerställa skyddet av tredje parts rättigheter och intressen och bör ges befogenhet att begära nödvändig information från vidareutnyttjaren. Villkoren för vidareutnyttjande av data bör begränsas till vad som är nödvändigt för att skydda tredje parts rättigheter och intressen i data och integriteten hos de offentliga myndigheternas it- och kommunikationssystem. Offentliga myndigheter bör tillämpa sådana villkor som bäst gagnar vidareutnyttjarens intressen utan att detta leder till en oproportionerlig börda för de offentliga myndigheterna. Villkoren för vidareutnyttjande av data bör utformas på ett sätt som säkerställer effektiva skyddsåtgärder för personuppgifter. Före överföring bör personuppgifter vara

anonymiserade så att de registrerade inte kan identifieras, och data som innehåller affärshemligheter bör ändras på ett sådant sätt att ingen konfidentiell information lämnas ut. Om tillhandahållandet av anonymiserade eller ändrade data inte skulle tillgodose vidareutnyttjarens behov, förutsatt att eventuella krav på att genomföra en konsekvensbedömning avseende dataskydd och samråda med tillsynsmyndigheten enligt artiklarna 35 och 36 i förordning (EU) 2016/679 uppfylls och om riskerna för de registrerades rättigheter och deras intressen är minimala, kan det tillåtas att vidareutnyttja uppgifterna på plats eller på distans inom en säker behandlingsmiljö.

Detta skulle kunna vara ett lämpligt arrangemang för vidareutnyttjande av pseudonymiserade data. Dataanalyser i sådana säkra behandlingsmiljöer bör övervakas av den offentliga myndigheten för att skydda tredje parts rättigheter och intressen. I synnerhet bör personuppgifter överföras till en tredje part för vidareutnyttjande endast om en rättslig grund inom ramen för dataskyddslagstiftningen tillåter en sådan överföring. Icke-personuppgifter bör endast överföras om det saknas skäl att tro att en kombination av dataset som inte består av personuppgifter kan leda till identifiering av de registrerade. Detta bör även gälla pseudonymiserade data som behåller sin status som personuppgifter. Vid återidentifiering av registrerade bör en skyldighet att anmäla en sådan uppgiftsincident till den offentliga myndigheten gälla utöver en skyldighet att anmäla en sådan uppgiftsincident till en tillsynsmyndighet och den registrerade i enlighet med förordning (EU) 2016/679. I tillämpliga fall bör de offentliga myndigheterna underlätta vidareutnyttjande av data efter att de registrerade samtyckt eller datainnehavare med lämpliga tekniska metoder gett sitt tillstånd till vidareutnyttjande av data som rör dem. I det avseendet bör den offentliga myndigheten göra sitt bästa för att bistå potentiella vidareutnyttjare som behöver sådant samtycke eller tillstånd genom att inrätta tekniska mekanismer som gör det möjligt att vidarebefordra begäranden om samtycke eller tillstånd från vidareutnyttjare, när detta är praktiskt genomförbart. Ingen kontaktinformation bör lämnas som gör det möjligt för vidareutnyttjare att kontakta registrerade eller datainnehavare direkt. Om den offentliga myndigheten översänder en begäran om samtycke eller tillstånd bör den säkerställa att den registrerade eller datainnehavaren tydligt informeras om möjligheten att vägra samtycke eller tillstånd.

- (16) För att underlätta och främja användningen av data som innehas av offentliga myndigheter för vetenskaplig forskning uppmantras offentliga myndigheter att utarbeta en harmoniserad strategi och harmoniserade förfaranden för att göra dessa data enkelt tillgängliga för vetenskaplig forskning i allmänhetens intresse. Det skulle bland annat kunna innebära att man skapar rationaliserade administrativa förfaranden, standardiserade dataformat, informativa metadata om metod- och datainsamlingsvalen samt standardiserade datafält som möjliggör enkel sammanslagning av dataset från olika källor till data från den offentliga sektorn om detta är relevant för analysen. Målet för dessa metoder bör vara att främja offentligt finansierade och framtagna data för vetenskaplig forskning i enlighet med principen *så öppen som möjligt, så begränsad som nödvändigt*.
- (17) Immateriella rättigheter som innehas av tredje part bör inte påverkas av denna förordning. Denna förordning bör inte påverka vare sig förekomsten av immateriella rättigheter hos offentliga myndigheter eller deras äganderätt av desamma, eller begränsa utövandet av dessa rättigheter på något sätt. De skyldigheter som införs i enlighet med denna förordning bör endast tillämpas i den mån de är förenliga med internationella avtal om skydd av immateriella rättigheter, i synnerhet Bernkonventionen för skydd av litterära och konstnärliga verk (Bernkonventionen), avtalet om handelsrelaterade aspekter av immaterialrätter (Trips-avtalet) och Världsgenerationen för den intellektuella äganderättens fördrag om upphovsrätt (WCT) samt unionsrätt eller nationell rätt om immateriella rättigheter. Offentliga myndigheter bör emellertid använda sin upphovsrätt på ett sätt som underlättar vidareutnyttjande.
- (18) Data som omfattas av immateriella rättigheter och företagshemligheter bör endast överföras till en tredje part om överföringen är laglig enligt unionsrätten eller nationell rätt eller med rättsinnehavarens samtycke. Om offentliga myndigheter är innehavare av en databasproducenters rätt som föreskrivs i artikel 7.1 i Europaparlamentets och rådets direktiv 96/9/EG<sup>(20)</sup>, bör de inte utöva denna rätt för att förhindra vidareutnyttjande av data eller begränsa vidareutnyttjande utöver de gränser som fastställs i denna förordning.

<sup>(20)</sup> Europaparlamentets och rådets direktiv 96/9/EG av den 11 mars 1996 om rättsligt skydd för databaser (EGT L 77, 27.3.1996, s. 20).

- (19) Företagen och de registrerade bör kunna förlita sig på att vidareutnyttjandet av vissa kategorier av skyddade data som innehåser av de offentliga myndigheterna kommer att ske på ett sätt som är i enlighet med deras rättigheter och intressen. Ytterligare skyddsåtgärder bör därför införas för situationer där vidareutnyttjande av sådana data från den offentliga sektorn sker på grundval av behandling av data utanför den offentliga sektorn, såsom ett krav på att offentliga myndigheter säkerställer att fysiska och juridiska personers rättigheter och intressen är fullt skyddade, särskilt med avseende på personuppgifter, kommersiellt känsliga data och immateriella rättigheter, i alla situationer, inklusive om sådana uppgifter överförs till tredjeländer. Offentliga myndigheter bör inte tillåta vidareutnyttjandet av information som lagras av försäkringsföretag eller andra tjänsteleverantörer i e-hälsotillämpningar i syfte att diskriminera vid prissättning, eftersom detta skulle strida mot den grundläggande rätten till tillgång till hälso- och sjukvård.
- (20) För att upprätthålla rättvis konkurrens och den öppna marknadsekonomin är det dessutom av största vikt att skyddade data av icke-personuppgiftskaraktär skyddas, särskilt företagshemligheter, men även icke-personuppgifter som avser innehåll som skyddas av immateriella rättigheter, från olaglig tillgång som kan leda till stöld av immateriella rättigheter eller industrispionage. För att säkerställa skyddet av datainnehavarnas rättigheter eller intressen bör det vara möjligt att överföra icke-personuppgifter som ska skyddas från olaglig eller otillåten åtkomst i enlighet med unionsrätten eller nationell rätt och som innehåser av offentliga myndigheter till tredjeländer, men endast om lämpliga skyddsåtgärder för användningen av data tillhandahålls. Sådana lämpliga skyddsåtgärder bör inbegripa ett krav att den offentliga myndigheten överför skyddade data till en vidareutnyttjare endast om den vidareutnyttjaren avtalsmässigt åtar sig att skydda dessa data. En vidareutnyttjare som avser att överföra skyddade data till ett tredjeländ fullgöra de skyldigheter som fastställs i denna förordning även efter det att berörda data har överförts till tredjelandet. För att säkerställa att sådana skyldigheter fullgörs korrekt bör vidareutnyttjaren också godta att den medlemsstat där den offentliga myndighet är belägen som tillät vidareutnyttjandet är behörig vid rättslig tvistlösning.
- (21) Lämpliga skyddsåtgärder bör även anses ha vidtagits om det i tredjelandet till vilket icke-personuppgifter har överförts, finns likvärdiga åtgärder som säkerställer att uppgifterna omfattas av en skyddsnivå liknande den som tillämpas enligt unionsrätten, särskilt vad gäller skyddet av företagshemligheter och immateriella rättigheter. När så motiveras på grund av betydande antal begäranden i hela unionen om vidareutnyttjandet av icke-personuppgifter i specifika tredjeländer bör kommissionen för detta ändamål kunna intyga, genom genomförandeakter, att ett tredjeländ tillhandahåller en skyddsnivå som i allt väsentligt är likvärdig med den som föreskrivs i unionsrätten. Kommissionen bör bedöma om sådana genomförandeakter är nödvändiga på grundval av informationen från medlemsstaterna via Europeiska datainnovationsstyrelsen. Sådana genomförandeakter skulle försäkra de offentliga myndigheterna om att vidareutnyttjande av data som innehåser av offentliga myndigheter i det berörda tredjelandet inte skulle hota dessa datas skyddade karaktär. Bedömningen av skyddsnivån i det berörda tredjelandet bör i synnerhet ta hänsyn till relevant allmän rätt och sektorspecifik rätt, inklusive om allmän säkerhet, försvar, nationell säkerhet och straffrätt när det gäller tillgång till och skydd av data som inte är personuppgifter, eventuell åtkomst för de offentliga myndigheterna i det tredjelandet till de uppgifter som överförs, huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter med ansvar för att säkerställa och kontrollera efterlevnaden av den rättsliga ordning som säkerställer tillgång till sådana data, tredjelandets internationella åtaganden i fråga om dataskydd, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system.

Det är särskilt viktigt att det finns effektiva rättsmedel för datainnehavare, offentliga myndigheter eller leverantörer av dataförmedlingsjänster i det berörda tredjelandet i samband med överföring av icke-personuppgifter till det tredjelandet. Sådana skyddsåtgärder bör därför inbegripa tillgång till verkställbara rättigheter och effektiva rättsmedel. Sådana genomförandeakter bör inte påverka rättsliga skyldigheter eller kontraktsmässiga arrangemang som en vidareutnyttjare redan har fullgjort för att skydda icke-personuppgifter, särskilt industridata, och offentliga myndigheters rätt att ålägga vidareutnyttjare att uppfylla villkoren för vidareutnyttjande, i enlighet med denna förordning.

- (22) Vissa tredjeländer antar lagar, förordningar och andra rättsakter som syftar till att direkt överföra eller ge statlig tillgång till icke-personuppgifter som finns i unionen och som fysiska och juridiska personer som står under medlemsstaternas jurisdiktion har kontroll över. Beslut och domar av domstolar i tredjeländer eller beslut av förvaltningsmyndigheter i tredjeländer som innehåller krav på sådan överföring eller tillgång till icke-personuppgifter ska vara verkställbara, om de grundar sig på ett gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. I vissa fall kan det uppstå situationer där skyldigheten att överföra eller ge tillgång till icke-personuppgifter som härrör från ett tredjelands rätt står i strid med en skyldighet att skydda sådana data enligt unionsrätten eller nationell rätt, särskilt när det gäller skyddet av den enskilda personens grundläggande rättigheter eller en medlemsstats grundläggande intressen med



avseende på nationell säkerhet eller försvar samt skyddet av kommersiellt känsliga uppgifter och skyddet av immateriella rättigheter, inbegripet avtalsskyldigheter i fråga om konfidentiell behandling i enlighet med sådan rätt. I avsaknad av internationella avtal som reglerar sådana frågor bör överföring av eller tillgång till icke-personuppgifter endast tillåtas om det, i synnerhet, har kontrollerats att tredjeländets rättssystem omfattar krav på att beslutets eller domens skäl och proportionalitet anges, att beslutet eller domen är specifik till sin karaktär och att den motiverade invändningen från mottagaren är föremål för prövning av en behörig domstol i tredjelandet, som har befogenhet att vederbörligen beakta de relevanta rättsliga intressena för den som tillhandahåller sådana uppgifter.

Offentliga myndigheter, fysiska eller juridiska personer som beviljats rätten att vidareutnyttja data, leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer bör dessutom, om de undertecknar avtal med andra privata partner, säkerställa att icke-personuppgifter som innehålls i unionen görs tillgängliga i eller överförs till tredjeländer endast i enlighet med unionsrätten eller den berörda medlemsstatens nationella rätt.

- (23) I syfte att ytterligare främja förtroendet för unionens dataekonomi är det avgörande att de skyddsåtgärder för unionsmedborgare, den offentliga sektorn och företag som säkerställer kontroll över dessas strategiska och känsliga uppgifter genomförts och att unionsrätt, värden och standarder upprätthålls inom bland annat, men inte enbart, områdena säkerhet, dataskydd och konsumentskydd. För att förhindra olaglig åtkomst till icke-personuppgifter bör de offentliga myndigheterna, de fysiska eller juridiska personer som beviljats rätten att vidareutnyttja data, leverantörerna av dataförmedlingstjänster och erkända dataaltruismorganisationer, vidta alla rimliga åtgärder för att förhindra åtkomst till de system där icke-personuppgifter lagras, inbegripet kryptering av data eller företagspolicyer. För det ändamålet bör det säkerställas att offentliga myndigheter, fysiska eller juridiska personer som beviljats rätten att vidareutnyttja data, leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer uppfyller samtliga relevanta tekniska standarder, uppförandekoder och certifieringar på unionsnivå.
- (24) För att bygga upp förtroendet för mekanismer för vidareutnyttjande kan det vara nödvändigt att införa strängare villkor för vissa typer av icke-personuppgifter som kan komma att identifieras som mycket känsliga i framtida särskilda unionslagstiftningsakter, när det gäller överföring till tredjeländer, om en sådan överföring skulle kunna äventyra unionens offentligpolitiska mål, i linje med internationella åtaganden. Till exempel på hälsoområdet kan vissa dataset som innehåller av aktörer i det allmänna hälso- och sjukvårdssystemet, t.ex. offentliga sjukhus, fastställas som mycket känsliga hälsodata. Andra relevanta sektorer är transport, energi, miljö och finans. För att säkerställa en harmoniserad praxis i hela unionen bör sådana typer av mycket känsliga offentliga icke-personuppgifter definieras i unionsrätten, till exempel inom ramen för det europeiska hälsodataområdet eller annan sektorspecifik rätt. Dessa villkor för överföring av sådana uppgifter till tredjeländer bör fastställas i delegerade akter. Villkoren bör vara proportionella, icke-diskriminerande och nödvändiga för att upprätthålla de legitima offentligpolitiska mål för unionen som fastställs, såsom skydd av folkhälsan, säkerhet, miljö, allmän moral, konsumentskydd, integritet och skydd av personuppgifter. Villkoren bör motsvara de risker som identifierats i förhållande till känsligheten hos sådana data, bland annat när det gäller risken för återidentifiering av enskilda personer. Sådana villkor kan omfatta villkor för överföringen eller tekniska arrangemang, såsom krav på användning av en säker behandlingsmiljö, begränsningar när det gäller vidareutnyttjande av data i tredjeländer eller kategorier av personer som har rätt att överföra sådana data till tredjeland eller har tillgång till dem i tredjelandet. I undantagsfall kan sådana villkor också omfatta begränsningar av överföringen av data till tredjeländer för att skydda allmänintresset.
- (25) Offentliga myndigheter bör kunna ta ut avgifter för vidareutnyttjande av data, men bör också kunna tillåta vidareutnyttjande till en nedsatt avgift eller kostnadsfritt, till exempel för vissa kategorier av vidareutnyttjande såsom icke-kommersiellt vidareutnyttjande eller vidareutnyttjande för forskningsändamål, eller små och medelstora företags, nystartade företags, civilsamhällets och utbildningsanstalters vidareutnyttjande, för att ge incitament för sådant vidareutnyttjande i syfte att stimulera forskning och innovation och stödja företag som är en viktig källa till innovation och vanligtvis har svårare att själva samla in relevanta data, i enlighet med reglerna för statligt stöd. I det specifika sammanhanget bör forskningsändamål anses inbegripa alla forskningsrelaterade ändamål oaktat den berörda forskningsinstitutionens organisatoriska eller finansiella struktur, med undantag för forskning som bedrivs

av ett företag och som syftar till att utveckla, förbättra eller optimera produkter eller tjänster. Sådana avgifter bör, vara transparenta, icke-diskriminerande och begränsade till de nödvändiga kostnaderna och bör inte begränsa konkurrensen. En förteckning över kategorier av vidareutnyttjare som betalar lägre avgift eller helt slipper avgift bör offentliggöras tillsammans med de kriterier som använts för upprättandet av förteckningen.

- (26) För att ge incitament till vidareutnyttjande av särskilda kategorier av data som innehas av offentliga myndigheter bör medlemsstaterna inrätta en gemensam informationspunkt som ska fungera som ett gränssnitt för vidareutnyttjare som vill vidareutnyttja dessa data. Denna informationspunkt bör ha ett sektorsövergripande uppdrag och vid behov komplettera arrangemang på sektorsnivå. Den gemensamma informationspunkten bör kunna förlita sig på automatiska metoder när den överför förfrågningar eller ansökningar om vidareutnyttjande. En tillräcklig mänsklig tillsyn i överföringsprocessen bör säkerställas. Befintliga praktiska arrangemang som till exempel portaler för öppna data skulle kunna användas för detta syfte. Den enda informationspunkten bör ha en förteckning över resurser som innehåller en översikt över alla tillgängliga datakällor, däribland de datakällor som finns tillgängliga vid sektorsspecifika, regionala eller lokala informationspunkter, tillsammans med relevant information som beskriver tillgängliga data. Dessutom bör medlemsstaterna utse, inrätta eller underlätta inrättandet av behöriga organ för att stödja verksamheten inom offentliga myndigheter som tillåter vidareutnyttjande av vissa kategorier av skyddade data. Deras uppgifter kan inbegripa att bevilja tillgång till data, om detta föreskrivs enligt sektorsspecifik unionsrätt eller nationell rätt. Dessa behöriga organ bör ge bistånd till offentliga myndigheter med hjälp av den senaste tekniken, bland annat avseende hur data bäst struktureras och lagras för att göra dem lättillgängliga, i synnerhet genom applikationsprogrammeringsgränssnitt, samt göra data interoperabla, överförbara och sökbara, med beaktande av bästa praxis för databehandling samt eventuella befintliga tillsynsstandarder och tekniska standarder och säkra databehandlingsmiljöer, som möjliggör dataanalys med bevarande av informationens integritet.

De behöriga organen bör agera i enlighet med den offentliga myndighetens instruktioner. En sådan biståndsstruktur skulle kunna bistå de registrerade och datainnehavarna att hantera samtycke eller tillstånd för vidareutnyttjande, inbegripet samtycke och tillstånd till vissa områden av vetenskaplig forskning, om vedertagna etiska standarder för vetenskaplig forskning iakttas. De behöriga myndigheterna bör inte ha någon tillsynsfunktion, då denna uteslutande ska utövas av tillsynsmyndigheter enligt förordning (EU) 2016/679. Databehandlingen bör, utan att det påverkar dataskyddsmyndigheternas tillsynsbefogenheter, utföras under ansvar av den offentliga myndighet som ansvarar för det register som innehåller dessa data, och som förblir personuppgiftsansvarig enligt definitionen i förordning (EU) 2016/679 i den mån personuppgifter berörs. Medlemsstaterna bör kunna ha ett eller flera behöriga organ, som kan vara verksamma inom olika sektorer. De offentliga myndigheternas interna avdelningar skulle även kunna fungera som behöriga organ. Ett behörigt organ skulle kunna vara en offentlig myndighet som bistår andra offentliga myndigheter när det gäller att tillåta vidareutnyttjande av data, om så är relevant, eller en offentlig myndighet som själv ger tillstånd till vidareutnyttjande. Biståndet till andra offentliga myndigheter bör omfatta att på begäran informera dem om bästa praxis när det gäller att uppfylla de krav som fastställs i den här förordningen, bland annat de tekniska medlen för tillhandahållande av en säker behandlingsmiljö eller de tekniska metoderna för att säkerställa integritet och konfidentiell behandling när tillgång ges till vidareutnyttjande av data som omfattas av tillämpningsområdet för den här förordningen.

- (27) Dataförmedlingstjänster förväntas spela en nyckelroll i dataekonomin, i synnerhet när det gäller att stödja och främja metoder för frivillig datadelning mellan företag eller att underlätta datadelning när det gäller skyldigheter som fastställs i unionsrätten eller nationell rätt. De skulle kunna bli ett verktyg för att underlätta utbyte av stora mängder relevanta data. Leverantörer av dataförmedlingstjänster, vilka även kan omfatta offentliga myndigheter, som erbjuder tjänster som kopplar samman de olika aktörerna kan bidra till en effektiv samkörning av data och till att underlätta bilateral datadelning. Specialiserade dataförmedlingstjänster som är oberoende av registrerade, datainnehavare och dataanvändare skulle kunna underlätta framväxten av nya datadrivna ekosystem som är oberoende av aktörer med betydande marknadsinflytande, samtidigt som de möjliggör icke-diskriminerande tillgång till dataekonomin för aktörer av alla storlekar, särskilt små och medelstora företag och nystartade företag med begränsade ekonomiska, rättsliga eller administrativa resurser. Detta kommer att vara av särskild vikt i samband med inrättandet av gemensamma europeiska dataområden, nämligen ändamåls- eller sektorspecifika eller sektorsöverskridande interoperabla ramar med gemensamma standarder och praxisformer för delning eller gemensam behandling av data bl.a. för utvecklingen av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällsinitiativ. Dataförmedlingstjänsterna skulle kunna innefatta bilateral eller multilateral delning av data eller inrättandet av plattformar eller databaser som möjliggör datadelning eller gemensamt utnyttjande av data, liksom inrättandet av en särskild infrastruktur för sammankoppling av registrerade och datainnehavare med dataanvändare.

- (28) Denna förordning bör omfatta tjänster som syftar till att med tekniska, rättsliga eller andra medel upprätta affärsförbindelser för datadelning mellan ett obestämt antal registrerade och datainnehavare, å ena sidan, och dataanvändare, å andra sidan, inbegripet för utövande av de registrerades rättigheter avseende personuppgifter. Om företag eller andra enheter erbjuder flera datarelaterade tjänster bör endast sådan verksamhet som direkt berör tillhandahållandet av dataförmedlingstjänster omfattas av denna förordning. Tillhandahållande av molnlagring, analys, programvara för datadelning, webbläsare, insticksprogram för webbläsare eller e-posttjänster bör inte anses vara dataförmedlingstjänster i den mening som avses i denna förordning, under förutsättning att sådana tjänster endast tillhandahåller tekniska verktyg för registrerade eller datainnehavare för delning av data med andra, men tillhandahållande av sådana verktyg varken syftar till att upprätta en affärsförbindelse mellan datainnehavare och dataanvändare eller ger leverantören av dataförmedlingstjänster möjlighet att erhålla information om upprättandet av affärsförbindelser som syftar till datadelning. Exempel på dataförmedlingstjänster inkluderar datamarknader där företag kan göra data tillgängliga för andra, organisatörer av ekosystem för datadelning som är öppna för alla intresserade parter, till exempel inom ramen för gemensamma europeiska dataområden, samt datapooler som inrättas gemensamt av flera juridiska eller fysiska personer i avsikten att licensiera användningen av sådana datapooler till alla intresserade parter på ett sätt som innebär att alla deltagare som bidrar till datapooler belönas för sitt bidrag.

Detta skulle exkludera tjänster som erhåller data från datainnehavare och aggregerar, berikar eller omvandlar data i syfte att avsevärt öka deras värde och licensierar användningen av resulterande data till dataanvändare, utan att upprätta en affärsförbindelse mellan datainnehavare och dataanvändare. Dessutom skulle det exkludera tjänster som uteslutande används av en datainnehavare för att möjliggöra användning av de data som den datainnehavaren innehar, eller som används av flera juridiska personer i en sluten grupp, inbegripet leverantörs- eller kundrelationer eller samarbeten som grundar sig på avtal, särskilt sådana som har som huvudsakligt syfte att säkerställa funktioner för föremål och enheter som är anslutna till sakernas internet.

- (29) Tjänster som är inriktade på förmedling av upphovsrättsligt skyddat innehåll, däribland onlineleverantör av delningstjänster för innehåll enligt definitionen i artikel 2.6 i direktiv (EU) 2019/790, bör inte omfattas av den här förordningen. Tillhandahållare av konsoliderad handelsinformation enligt definitionen i artikel 2.1.35 i Europaparlamentets och rådets förordning (EU) nr 600/2014<sup>(7)</sup> och leverantörer av kontoinformationstjänster enligt definitionen i artikel 4.19 i Europaparlamentets och rådets direktiv (EU) 2015/2366<sup>(8)</sup> bör inte anses vara leverantörer av dataförmedlingstjänster vid tillämpning av den här förordningen. Den här förordningen bör inte tillämpas på tjänster som erbjuds av offentliga myndigheter för att underlätta antingen vidareutnyttjande av skyddade data som innehas av offentliga myndigheter i enlighet med den här förordningen eller användning av andra data, i den mån dessa tjänster inte syftar till att upprätta affärsförbindelser. Dataaltruismorganisationer som regleras i denna förordning bör inte anses erbjuda dataförmedlingstjänster förutsatt att dessa tjänster inte upprättar en affärsförbindelse mellan potentiella dataanvändare, å ena sidan, och registrerade och datainnehavare som tillgängliggör data utifrån altruistiska ändamål, å andra sidan. Andra tjänster som inte syftar till att upprätta affärsförbindelser, till exempel databaser som syftar till att möjliggöra vidareutnyttjande av vetenskapliga forskningsdata i enlighet med principerna om öppen tillgång bör inte anses vara dataförmedlingstjänster i den mening som avses i den här förordningen.
- (30) En särskild kategori av dataförmedlingstjänster omfattar leverantörer av tjänster som erbjuder sina tjänster till registrerade. Sådana leverantörer av dataförmedlingstjänster strävar efter att stärka de registrerades handlingsförmåga och särskilt enskilda personers kontroll över de uppgifter som avser dem. Sådana leverantörer hjälper enskilda personer att utöva sina rättigheter enligt förordning (EU) 2016/679, särskilt att hantera deras givande och återkallande av samtycke till databehandling, rätten att få tillgång till sina egna personuppgifter, rätten till rättelse av felaktiga personuppgifter, rätten till radering eller rätten "att bli bortglömd", rätten att begränsa behandlingen och rätten till dataportabilitet, som gör det möjligt för registrerade att flytta sina personuppgifter från en personuppgiftsansvarig till en annan. I det sammanhanget är det viktigt att sådana leverantörers affärsmodell säkerställer att det inte finns några dåligt anpassade incitament som uppmuntrar enskilda personer att använda sådana tjänster för att tillgängliggöra mer data som avser dem för behandling än vad som skulle ligga i deras intresse. Detta skulle kunna innebära rådgivning till enskilda personer om möjlig användning av deras data och hur de gör due diligence-kontroller av dataanvändare innan de tillåts kontakta registrerade, i syfte att undvika bedrägerier. I vissa situationer kan det vara önskvärt att samla faktiska data inom ett personligt dataområde, så att

<sup>(7)</sup> Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84).

<sup>(8)</sup> Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betal tjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).

behandlingen kan ske inom det området utan att personuppgifter överförs till tredje part, för att maximera skyddet av personuppgifter och integritet. Sådana personliga dataområden skulle kunna innehålla statiska personuppgifter, däribland namn, adress och födelsedatum, samt dynamiska data som genereras av en enskild person, genom till exempel användning av en onlinetjänst eller ett föremål anslutet till sakernas internet. De skulle också kunna användas för att lagra verifierade identitetsuppgifter, såsom passnummer eller socialförsäkringsuppgifter samt behörighetsuppgifter, såsom körkort, examensbevis eller uppgifter om bankkonton.

- (31) Datakooperativ strävar efter att uppnå ett antal mål, särskilt att stärka enskilda personers ställning när det gäller att fatta välgrundade beslut innan de samtycker till dataanvändning, påverka dataanvändarorganisationers villkor och bestämmelser knutna till dataanvändning på ett sätt som ger gruppens enskilda medlemmar bättre valmöjligheter, eller eventuellt finna lösningar på meningsmotsättningar mellan enskilda medlemmar i en grupp om hur data kan användas om dessa data är relaterade till flera registrerade inom den gruppen. I det sammanhanget är det viktigt att slå fast att rättigheterna enligt förordning (EU) 2016/679 är personliga rättigheter som tillhör den registrerade och att registrerade inte kan avsäga sig sådana rättigheter. Datakooperativ skulle också kunna vara ett användbart verktyg för emansföretag samt små och medelstora företag som ofta är jämförbara med enskilda personer när det gäller kunskap om datadelning.
- (32) För att öka förtroendet för sådana dataförmedlingstjänster, i synnerhet när det gäller användningen av data och uppfyllandet av de villkor som de registrerade och datainnehavarna sätter upp, är det nödvändigt att upprätta ett regelverk på unionsnivå som fastställer krav med hög harmoniseringsgrad avseende ett tillförlitligt tillhandahållande av sådana dataförmedlingstjänster och som genomförs av de behöriga myndigheterna. Det regelverket kommer att bidra till att säkerställa att de registrerade och datainnehavarna samt dataanvändarna får bättre kontroll över tillgången till och användningen av deras data, i enlighet med unionsrätten. Kommissionen skulle även kunna uppmuntra och underlätta utarbetandet av uppförandekoder på unionsnivå med deltagande av berörda parter, särskilt vad avser interoperabilitet. Både i situationer där datadelning sker i samband med företagstjänster och när datadelning sker i samband med konsumenttjänster bör leverantörer av dataförmedlingstjänster erbjuda en ny "européisk" dataförvaltning genom att i säkra en åtskillnad i dataekonomin mellan tillhandahållandet, förmedlingen och användningen av data. Leverantörer av dataförmedlingstjänster skulle också kunna göra särskild teknisk infrastruktur tillgänglig för sammankoppling av registrerade och datainnehavare med dataanvändare. I detta avseende är det särskilt viktigt att utforma denna infrastruktur på ett sådant sätt att små och medelstora företag och nystartade företag inte stöter på några tekniska eller andra hinder för sitt deltagande i dataekonomin.

Leverantörer av dataförmedlingstjänster bör tillåtas att erbjuda ytterligare särskilda verktyg till datainnehavare eller de registrerade för det särskilda syftet att underlätta utbytet av data, exempelvis i form av tillfällig lagring, kuratering, konvertering, anonymisering och pseudonymisering. Dessa verktyg och tjänster bör användas endast på uttrycklig begäran eller efter uttryckligt godkännande av datainnehavaren eller den registrerade, och tredjepartsverktyg som erbjuds i detta sammanhang bör inte användas data för andra ändamål. Samtidigt bör leverantörer av dataförmedlingstjänster tillåtas anpassa de data som utbyts, för att göra dem mer användbara för dataanvändaren om dataanvändaren så önskar, eller att förbättra interoperabiliteten genom, till exempel, att konvertera dessa data till specifika format.

- (33) Det är viktigt att möjliggöra en konkurrensutsatt miljö för datadelning. En viktig faktor för att öka förtroendet och datainnehavarnas, de registrerades och dataanvändarnas kontroll över dataförmedlingstjänster är att leverantörerna av dataförmedlingstjänster är neutrala när det gäller de data som utbyts mellan datainnehavare eller de registrerade och dataanvändare. Leverantörerna av dataförmedlingstjänster bör därför endast fungera som förmedlare i transaktionerna och inte använda de data som utbyts för några andra ändamål. De kommersiella villkoren, inklusive prissättning, för tillhandahållandet av dataförmedlingstjänster bör inte vara beroende av huruvida en potentiell datainnehavare eller dataanvändare använder andra tjänster, däribland lagring, analys, artificiell intelligens eller andra databaserade tillämpningar, som tillhandahålls av samma leverantör av dataförmedlingstjänster eller en närliggande enhet, och i så fall i vilken utsträckning datainnehavaren eller dataanvändaren använder sådana andra tjänster. Detta kommer också förutsätta en strukturell åtskillnad mellan dataförmedlingstjänsten och alla andra tjänster som erbjuds, så att intressekonflikter undviks. Därmed bör dataförmedlingstjänsten erbjudas via en juridisk person som är separat från all övrig verksamhet som bedrivs av leverantören av dataförmedlingstjänster. Emellertid bör leverantörer av dataförmedlingstjänster kunna använda de data som tillhandahålls av datainnehavaren för att förbättra sina dataförmedlingstjänster.

Leverantörer av dataförmedlingstjänster bör endast kunna ställa sina egna eller tredje parts verktyg till datainnehavares, de registrerades eller dataanvändares förfogande för att underlätta utbytet av data, exempelvis verktyg för konvertering eller kuratering av data, efter den registrerades eller datainnehavarens uttryckliga begäran eller godkännande. De tredjepartsverktyg som erbjuds i detta sammanhang bör inte använda data för andra ändamål än de som är relaterade till dataförmedlingstjänster. Leverantörer av dataförmedlingstjänster som

förmedlar ett utbyte av data mellan enskilda personer som registrerade och juridiska personer som dataanvändare bör, utöver att axla sitt förvaltaruppdrag gentemot de enskilda personerna, säkerställa att de agerar i de registrerades intresse. Frågor om ansvar för alla materiella och immateriella skador och brister som uppstår till följd av agerandet av leverantören av dataförmedlingstjänster bör tas upp i det berörda avtalet, på grundval av nationella ansvarsordningar.

- (34) Leverantörer av dataförmedlingstjänster bör vidta rimliga åtgärder för att säkerställa interoperabilitet inom en sektor och mellan olika sektorer i syfte att säkerställa en korrekt fungerande inre marknad. Rimliga åtgärder skulle bland annat kunna innebära att man följer de befintliga standarder som allmänt används i den sektor inom vilken leverantören av dataförmedlingstjänster är verksam. Europeiska datainnovationsstyrelsen bör underlätta framtagningen av ytterligare branschstandarder där det är nödvändigt. Leverantörer av dataförmedlingstjänster bör i god tid genomföra de åtgärder för interoperabilitet mellan dataförmedlingstjänster som antagits av Europeiska datainnovationsstyrelsen.
- (35) Denna förordning bör inte påverka skyldigheten för leverantörer av dataförmedlingstjänster att uppfylla kraven i förordning (EU) 2016/679 och tillsynsmyndigheternas skyldighet att säkerställa efterlevnaden av den förordningen. Den här förordningen bör inte påverka skyddet av personuppgifter i de fall då leverantörer av dataförmedlingstjänster behandlar personuppgifter. I de fall då leverantörer av dataförmedlingstjänster är personuppgiftsansvariga eller personuppgiftsbiträden enligt definitionerna i förordning (EU) 2016/679 är de bundna av bestämmelserna i den förordningen.
- (36) Leverantörer av dataförmedlingstjänster förväntas ha infört förfaranden och åtgärder för att ålägga sanktioner för bedrägliga eller otillbörliga metoder i samband med parter som söker åtkomst via deras dataförmedlingstjänster, inbegripet genom åtgärder såsom uteslutning av dataanvändare som bryter mot tjänstevillkoren eller mot befintlig rätt.
- (37) Leverantörer av dataförmedlingstjänster bör också vidta åtgärder för att säkerställa att konkurrensrätten följs och inrätta förfaranden för det ändamålet. Detta gäller i synnerhet sådana situationer där datadelning gör det möjligt för företag att få kännedom om faktiska eller potentiella konkurrenters marknadsstrategier. Typisk information som är känslig i konkurrenshänseende är till exempel information om kunduppgifter, framtida priser, produktionskostnader, kvantiteter, omsättning, försäljning eller kapacitet.
- (38) Ett anmälningsförfarande för dataförmedlingstjänster bör inrättas för att säkerställa att dataförvaltning inom unionen är baserad på ett tillförlitligt utbyte av data. Vinsterna av en tillförlitlig miljö kan bäst uppnås genom ett införande av ett antal krav för tillhandahållandet av dataförmedlingstjänster, men utan något krav på ett uttryckligt beslut eller en uttrycklig administrativ åtgärd av den behöriga myndigheten för dataförmedlingstjänster för tillhandahållandet av sådana tjänster. Anmälningsförfarandet bör inte medföra otillbörliga hinder för små och medelstora företag, nystartade företag och civilsamhällesorganisationer och bör vara förenlig med principen om icke-diskriminering.
- (39) För att stödja ett effektivt gränsöverskridande tillhandahållande av tjänster bör leverantören av dataförmedlingstjänster åläggas att sända en anmälan endast till den behöriga myndigheten för dataförmedlingstjänster från den medlemsstat där leverantörens huvudsakliga verksamhetsställe är beläget eller där leverantörens rättsliga ombud finns. En sådan anmälan bör inte innefatta mer än en ren förklaring om avsikten att tillhandahålla sådana tjänster och bör endast kompletteras genom tillhandahållande av den information som anges i denna förordning. Efter relevant anmälan bör leverantören av dataförmedlingstjänster kunna inleda sin verksamhet i varje medlemsstat utan ytterligare anmälningskyldigheter.
- (40) Det anmälningsförfarande som fastställs i denna förordning bör inte påverka tillämpningen av särskilda kompletterande bestämmelser för tillhandahållandet av dataförmedlingstjänster som är tillämpliga genom sektorspecifik rätt.
- (41) Det huvudsakliga verksamhetsstället för en leverantör av dataförmedlingstjänster i unionen bör vara platsen för dess centrala förvaltning i unionen. Det huvudsakliga verksamhetsstället för en leverantör av dataförmedlingstjänster i unionen bör fastställas i enlighet med objektiva kriterier och bör avse det faktiska och reella utövandet av ledningsverksamheten. Den verksamhet som bedrivs av en leverantör av dataförmedlingstjänster bör överensstämma med den nationella rätten i den medlemsstat där denne har sitt huvudsakliga verksamhetsställe.

- (42) För att säkerställa att leverantörerna av dataförmedlingstjänster uppfyller de villkor som fastställs i denna förordning bör de ha sitt huvudsakliga verksamhetsställe i unionen. Om en leverantör av dataförmedlingstjänster som inte är etablerad i unionen erbjuder tjänster inom unionen bör leverantören utse en rättslig företrädare. Det är nödvändigt att utse en rättslig företrädare i sådana fall med tanke på att sådana leverantörer av dataförmedlingstjänster hanterar både personuppgifter och data som rör affärshemligheter och det därmed är nödvändigt att övervaka att leverantörerna av dataförmedlingstjänster efterlever denna förordning. I syfte att fastställa om en sådan leverantör av dataförmedlingstjänster erbjuder tjänster inom unionen bör det kontrolleras om det är uppenbart att leverantören av dataförmedlingstjänster planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart det faktum att en webbplats är tillgänglig i unionen eller att det finns en e-postadress eller andra kontaktuppgifter för leverantören av dataförmedlingstjänster eller att man använder ett språk som används i det tredjeland där leverantören av dataförmedlingstjänster är etablerad, bör inte anses räcka för att fastställa en sådan avsikt. Emellertid kan sådana faktorer som användning av ett visst språk eller en viss valuta som allmänt används i en eller flera medlemsstater, och möjlighet att beställa tjänster på detta språk, eller att användare i unionen omnämns, göra det uppenbart att leverantören av dataförmedlingstjänster planerar att erbjuda tjänster inom unionen.

En utsedd rättslig företrädare bör agera på uppdrag av leverantören av dataförmedlingstjänster och det bör vara möjligt för behöriga myndigheter för dataförmedlingstjänster att vända sig till den rättsliga företrädaren utöver eller i stället för leverantören av dataförmedlingstjänster, även i händelse av en överträdelse, i syfte att inleda verkställighetsförfaranden mot en leverantör av dataförmedlingstjänster som inte uppfyller kraven och som inte är etablerad i unionen. Den rättsliga företrädaren bör utses genom en skriftlig fullmakt från leverantören av dataförmedlingstjänster att agera på dess vägnar med avseende på leverantörens skyldigheter enligt denna förordning.

- (43) För att hjälpa de registrerade och datainnehavare att enkelt identifiera, och därigenom öka sitt förtroende för leverantörer av dataförmedlingstjänster som är erkända i unionen bör det inrättas en gemensam logotyp som är igenkännlig i hela unionen, utöver beteckningen "leverantörer av dataförmedlingstjänster som är erkända i unionen".
- (44) De behöriga myndigheterna för dataförmedlingstjänster som utses för att övervaka leverantörer av dataförmedlingstjänsters uppfyllande av kraven i denna förordning bör väljas på grundval av sin kapacitet och sakkunskap avseende horisontellt eller sektorsbaserat datautbyte. De bör vara oberoende av alla leverantörer av dataförmedlingstjänster samt transparenta och opartiska i utförandet av sina arbetsuppgifter. Medlemsstaterna bör meddela kommissionen dessa behöriga myndigheter för dataförmedlingstjänsters identitet. De behöriga myndigheterna för dataförmedlingstjänsters behörighet och befogenheter bör inte påverka dataskyddsmyndigheternas befogenheter. I synnerhet i alla frågor som rör en bedömning av efterlevnaden av förordning (EU) 2016/679 bör den behöriga myndigheten för dataförmedlingstjänster, i tillämpliga fall, efterfråga ett yttrande eller beslut av den behöriga tillsynsmyndighet som inrättats i enlighet med den förordningen.
- (45) Det finns en stor potential för mål av allmänt intresse vid användningen av data som tillhandahålls frivilligt av de registrerade på grundval av deras informerade samtycke eller, när det gäller icke-personuppgifter som tillhandahålls av datainnehavare. Sådana mål skulle kunna inkludera hälso- och sjukvård, bekämpande av klimatförändringar, förbättring av mobiliteten, främjande av utveckling, framställning och spridning av officiell statistik, förbättrat tillhandahållande av offentliga tjänster eller politiskt beslutsfattande. Stöd till vetenskaplig forskning bör också anses vara ett mål av allmänt intresse. Denna förordning bör syfta till att bidra till framväxten av tillräckligt stora datapooler som görs tillgängliga baserat på dataaltruism för att möjliggöra dataanalys och maskininlärning, i hela unionen. För att uppnå det målet bör medlemsstaterna kunna inrätta organisatoriska eller tekniska arrangemang, eller båda, som underlättar dataaltruism. Sådana arrangemang skulle kunna innefatta tillgång till lättanvända verktyg för registrerade eller datainnehavare för givande av samtycke eller tillstånd till altruistisk användning av deras data, anordnande av informationskampanjer eller ett strukturerat utbyte mellan behöriga myndigheter avseende hur offentlig politik, såsom förbättring av trafik och folkhälsa och bekämpning av klimatförändringar, kan gynnas av dataaltruism. För det ändamålet bör medlemsstaterna kunna fastställa nationella strategier för dataaltruism. Registrerade bör endast kunna erhålla ersättning för de kostnader som de ådrar sig när de gör sina data tillgängliga för mål av allmänt intresse.
- (46) Registreringen av erkända dataaltruismorganisationer och användningen av beteckningen "dataaltruismorganisation" som är erkänd i unionen" förväntas leda till upprättandet av centrallager för databaser. En registrering i en medlemsstat skulle gälla i hela unionen, och förväntas främja en gränsöverskridande användning av data inom unionen och framväxten av datapooler som täcker flera medlemsstater. Datainnehavare skulle kunna ge tillstånd till behandling av deras icke-personuppgifter för ett antal ändamål som inte är fastställda vid den tidpunkt då de ger sitt

tillstånd. Sådana erkända dataaltruismorganisationers uppfyllande av ett antal krav som fastställs i denna förordning bör skapa förtroende för att de data som tillhandahålls för altruistiska ändamål faktiskt tjänar ett mål av allmänt intresse. Sådant förtroende bör i synnerhet uppnås genom att ha en etableringsort eller en rättslig företrädare inom unionen, samt från kravet att erkända dataaltruismorganisationer är icke-vinstdrivande organisationer, från transparenskrav och från särskilda skyddsmekanismer för att skydda de registrerades och företagens rättigheter och intressen.

Ytterligare skyddsmekanismer bör inkludera att göra det möjligt att behandla relevanta data inom en säker behandlingsmiljö som drivs av de erkända dataaltruismorganisationerna, tillsynsmekanismer som etiska råd eller styrelser, inbegripet företrädare från det civila samhället för att säkerställa att de personuppgiftsansvariga upprätthåller höga standarder när det gäller forskningsetik och skydd av grundläggande rättigheter, effektiva och tydligt förmedlade tekniska metoder för att när som helst dra tillbaka eller ändra sitt samtycke, på grundval av personuppgiftsbiträdenas informationsskyldighet enligt förordning (EU) 2016/679, samt möjligheter för de registrerade att hålla sig underrättade om användningen av de data som de tillhandahållit. Registrering som en erkänd dataaltruismorganisation bör inte vara en förutsättning för att bedriva dataaltruismverksamhet. Kommissionen bör genom delegerade akter utarbeta en regelbok i nära samarbete med dataaltruismorganisationer och berörda parter. Efterlevnad av den regelboken bör vara ett krav för registrering som en erkänd dataaltruismorganisation.

- (47) För att hjälpa de registrerade och datainnehavare att enkelt identifiera, och därigenom öka sitt förtroende för, erkända dataaltruismorganisationer bör det inrättas en gemensam logotyp som är igenkännlig i hela unionen. Den gemensamma logotypen bör åtföljas av en QR-kod med en länk till det offentliga unionsregistret över erkända dataaltruismorganisationer.
- (48) Denna förordning bör inte påverka inrättandet av, organisationen av eller funktionssättet för enheter som önskar bedriva dataaltruism i enlighet med nationell rätt och bygger på krav i nationell rätt för bedrivande av laglig verksamhet i en medlemsstat som icke-vinstdrivande organisation.
- (49) Denna förordning bör inte påverka inrättandet av, organisationen av eller funktionssättet för andra enheter än offentliga myndigheter som bedriver delning av data och innehåll på grundval av öppna licenser och därmed bidrar till att skapa gemensamma resurser som är tillgängliga för alla. Detta bör inbegripa öppna samarbetsplattformar för kunskapsdelning, vetenskapliga och akademiska databaser med öppen åtkomst, plattformar för programvaruutveckling med öppen källkod och plattformar för sammanställning av innehåll med öppen åtkomst.
- (50) Erkända dataaltruismorganisationer bör kunna samla in relevanta data direkt från fysiska och juridiska personer eller behandla data som samlats in av andra. Dataaltruismorganisationer skulle kunna behandla insamlade data för ändamål som de själva fastställer, eller så skulle de, i förekommande fall, kunna tillåta tredjeparter att utföra behandlingen för dessa ändamål. I de fall då erkända dataaltruismorganisationer är personuppgiftsansvariga eller personuppgiftsbiträden enligt definitionerna i förordning (EU) 2016/679 är de bundna av bestämmelserna i den förordningen. Generellt skulle dataaltruism bygga på de registrerades samtycke i den mening som avses i artiklarna 6.1 a och 9.2 a i förordning (EU) 2016/679 vilket bör uppfylla kraven för lagligt samtycke i enlighet med artiklarna 7 och 8 i den förordningen. I enlighet med förordning (EU) 2016/679 skulle ändamål som rör vetenskaplig forskning kunna stödjas genom samtycke till vissa forskningsområden så länge som de är förenliga med allmänt erkända etiska normer för vetenskaplig forskning eller till vissa forskningsområden eller delar av forskningsprojekt. I artikel 5.1 b i förordning (EU) 2016/679 fastställs att ytterligare behandling för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i förordning (EU) 2016/679 inte ska anses vara oförenlig med de ursprungliga ändamålen. Nyttjandebegränsningarna för icke-personuppgifter bör återfinnas i det tillstånd som ges av datainnehavaren.
- (51) De behöriga myndigheter för registrering av dataaltruismorganisationer som utses för att övervaka erkända dataaltruismorganisationers uppfyllande av kraven i denna förordning bör väljas på grundval av sin kapacitet och sakkunskap. De bör vara oberoende av alla dataaltruismorganisationer samt transparenta och opartiska i utförandet av sina arbetsuppgifter. Medlemsstaterna bör meddela kommissionen dessa behöriga myndigheter för registrering av dataaltruismorganisationers identitet. De behöriga myndigheterna för registrering av dataaltruismorganisationers behörighet och befogenheter bör inte påverka dataskyddsmyndigheternas befogenheter. I synnerhet i alla frågor som rör en bedömning av efterlevnaden av förordning (EU) 2016/679 bör den behöriga myndigheten för registrering av dataaltruismorganisationer, i tillämpliga fall, efterfråga ett yttrande eller beslut av den behöriga tillsynsmyndighet som inrättats i enlighet med den förordningen.

- (52) För att främja förtroendet och få till stånd ökad rättssäkerhet och användarvänlighet vad gäller förfarandet för beviljande och tillbakadragande av samtycke, i synnerhet i samband med vetenskaplig forskning och statistisk användning av data som tillhandahålls baserat på altruism, bör ett europeiskt formulär för dataaltruism utarbetas och användas i samband med altruistisk dataindelning. Ett sådant formulär bör för de registrerade bidra till ytterligare transparens om att tillgången till och användningen av deras data kommer att ske i enlighet med deras samtycke och även i full överensstämmelse med dataskyddsbestämmelserna. Formuläret bör också göra det lättare att bevilja och dra tillbaka samtycke och kunna användas för att rationalisera företagets dataaltruism och tillhandahålla en mekanism som tillåter sådana företag att dra tillbaka sitt samtycke till användningen av data. För att ta hänsyn till de enskilda sektorernas särdrag, även ur ett dataskyddsperspektiv, bör det europeiska formuläret för samtycke till dataaltruism baseras på moduler, så att det kan anpassas till enskilda sektorer och olika syften.
- (53) För att genomförandet av dataförvaltningsramen ska bli framgångsrikt bör en europeisk datainnovationsstyrelse inrättas, i form av en expertgrupp. Europeiska datainnovationsstyrelsen bör bestå av företrädare för alla medlemsstaters behöriga myndigheter för dataförmedlingstjänster och behöriga myndigheter för registrering av dataaltruismorganisationer, Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, Europeiska unionens cybersäkerhetsbyrå (Enisa), kommissionen, EU-företrädaren för små och medelstora företag eller en företrädare utsedd av nätverket av företrädare för små och medelstora företag och andra företrädare för relevanta organ inom enskilda sektorer samt organ med specifik sakkunskap. Europeiska datainnovationsstyrelsen bör bestå av ett antal undergrupper, inbegripet en undergrupp för deltagande av berörda parter bestående av relevanta företrädare för näringslivet, såsom hälsa, miljö, jordbruk, transport, energi, industriell tillverkning, medier, kulturella och kreativa sektorer och statistik, samt för forskningsvärlden, den akademiska världen, civilsamhället, standardiseringsorganisationer, berörda gemensamma europeiska dataområden och andra berörda intressenter och tredje parter, bland annat organ med specifik sakkunskap såsom nationella statistikbyråer.
- (54) Europeiska datainnovationsstyrelsen bör bistå kommissionen i samordningen av nationella arbetsmetoder och strategier på de områden som omfattas av denna förordning och stödjandet av sektorsövergripande dataanvändning genom iakttagande av principerna i den europeiska interoperabilitetsramen och genom användning av europeiska och internationella standarder och specifikationer (inklusive genom EUs flerpartsforum för IKT-standardisering, basvokabulären och byggsstenarna inom Fonden för ett sammanlänkat Europa), och bör beakta det standardiseringsarbete som bedrivs inom enskilda sektorer eller områden. Arbetet med teknisk standardisering skulle kunna innefatta fastställandet av prioriteringar för utvecklingen av standarder och fastställandet och upprätthållandet av ett antal tekniska och rättsliga standarder för överföring av data mellan två behandlingsmiljöer som gör det möjligt att organisera dataområden, framför allt för att klarlägga och särskilja vilka standarder och praxisformer som är sektorsöverskridande och vilka som är sektorspecifika. Europeiska datainnovationsstyrelsen bör samarbeta med sektorsorgan, nätverk eller expertgrupper och andra sektorsövergripande organisationer som hanterar vidareutnyttjandet av data. När det gäller dataaltruism bör Europeiska datainnovationsstyrelsen bistå kommissionen i utarbetandet av formuläret för dataaltruism, efter samråd med Europeiska dataskyddsstyrelsen. Genom att föreslå riktlinjer för gemensamma europeiska dataområden bör Europeiska datainnovationsstyrelsen stödja utvecklingen av en fungerande europeisk dataekonomi på grundval av dessa dataområden, i enlighet med den europeiska datastrategin.
- (55) Medlemsstaterna bör fastställa regler om tillämpliga sanktioner vid överträdelse av denna förordning och bör vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. De sanktioner som föreskrivs bör vara effektiva, proportionella och avskräckande. Stora skillnader mellan sanktionsreglerna skulle kunna snedvrída konkurrensen på den digitala inre marknaden. I det avseendet skulle det vara fördelaktigt med en harmonisering av dessa regler.
- (56) För att säkerställa en effektiv efterlevnad av denna förordning och se till att leverantörer av dataförmedlingstjänster och enheter som vill registrera sig som erkända dataaltruismorganisationer kan få tillgång till och genomföra förfarandena för anmälan och registrering helt online och över gränserna, bör sådana förfaranden erbjudas genom den gemensamma digitala ingång som inrättas i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1724<sup>(29)</sup>. Dessa förfaranden bör läggas till i förteckningen över förfaranden i bilaga II till förordning (EU) 2018/1724.
- (57) Förordning (EU) 2018/1724 bör därför ändras i enlighet med detta.

<sup>(29)</sup> Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (EUT L 295, 21.11.2018, s. 1).



- (58) I syfte att säkerställa denna förordnings ändamålsenlighet, bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på att komplettera denna förordning genom att fastställa särskilda villkor som är tillämpliga på överföring till tredjeländer av vissa kategorier av icke-personuppgifter som anses vara mycket känsliga i särskilda unionslagstiftningsakter och genom att ta fram en regelbok för erkända dataaltruismorganisationer, som dessa organisationer ska följa och som föreskriver informationskrav, tekniska krav och säkerhetskrav samt färdplaner för kommunikation och interoperabilitetsstandarder. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning<sup>(90)</sup>. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.
- (59) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen tilldelas genomförandebefogenheter för att bistå offentliga myndigheter och vidareutnyttjare med deras efterlevnad av de villkor för vidareutnyttjande som fastställs i denna förordning genom att fastställa standardavtalsklausuler för vidareutnyttjares överföring av icke-personuppgifter till ett tredjeländ, intyga att ett tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang är likvärdiga med det skydd som säkerställs genom unionsrätten, utforma den gemensamma logotypen för leverantörer av dataförmedlingstjänster och den gemensamma logotypen för erkända dataaltruismorganisationer samt utarbeta och utveckla det europeiska formuläret för samtycke till dataaltruism. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011<sup>(91)</sup>.
- (60) Denna förordning bör inte påverka tillämpningen av konkurrensreglerna, särskilt artiklarna 101 och 102 i EUF-fördraget. De åtgärder som föreskrivs i denna förordning bör inte användas för att begränsa konkurrensen på ett sätt som strider mot EUF-fördraget. Detta gäller i synnerhet reglerna om utbyte av information som är känslig i konkurrenshänseende mellan faktiska och potentiella konkurrenter via dataförmedlingstjänster.
- (61) Samråd har skett med Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen i enlighet med artikel 42.1 i förordning (EU) 2018/1725 som avgav sitt yttrande den 10 mars 2021.
- (62) De vägledande principerna för denna förordning är respekten för de grundläggande rättigheterna och de principer som erkänns främst genom Europeiska unionens stadga om de grundläggande rättigheterna, inklusive rätten till privatliv, skyddet av personuppgifter, näringsfriheten, rätten till egendom och integreringen av personer med funktionsnedsättning. När det gäller det sistnämnda bör offentliga myndigheter och tjänster inom ramen för denna förordning, i förekommande fall, uppfylla kraven i Europaparlamentets och rådets direktiv (EU) 2016/2102<sup>(92)</sup> och (EU) 2019/882<sup>(93)</sup>. Vidare bör hänsyn tas till design för alla i samband med informations- och kommunikationsteknik, som är ett medvetet och systematiskt försök att aktivt tillämpa principer, metoder och verktyg för att främja universell design inom datorrelaterad teknik, däribland internetbaserad teknik, och därigenom undvika behovet av anpassningar i efterhand eller specialiserad design.
- (63) Eftersom målen för denna förordning, nämligen vidareutnyttjande inom unionen av vissa kategorier av data som innehas av offentliga myndigheter samt inrättandet av en ram för anmälan av och tillsyn över tillhandahållandet av datadelningstjänster, en ram för frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål och en ram för inrättandet av en europeisk datainnovationsstyrelse, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av deras omfattning och verkningar, 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 denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

<sup>(90)</sup> EUT L 123, 12.5.2016, s. 1.

<sup>(91)</sup> 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).

<sup>(92)</sup> Europaparlamentets och rådets direktiv (EU) 2016/2102 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer (EUT L 327, 2.12.2016, s. 1).

<sup>(93)</sup> Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

#### KAPITEL I

##### Allmänna bestämmelser

##### Artikel 1

#### Innehåll och tillämpningsområde

1. I denna förordning fastställs följande:
  - a) Villkoren för vidareutnyttjande inom unionen av vissa kategorier av data som innehas av offentliga myndigheter.
  - b) En ram för anmälan av och tillsyn över tillhandahållandet av dataförmedlingstjänster.
  - c) En ram för frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål.
  - d) En ram för inrättandet av en europeisk datainnovationsstyrelse.
2. Denna förordning medför inte någon skyldighet för offentliga myndigheter att tillåta vidareutnyttjande av data och befriar inte heller offentliga myndigheter från deras skyldigheter i fråga om konfidentiell behandling enligt unionsrätten eller nationell rätt.

Denna förordning ska inte påverka

- a) tillämpningen av särskilda bestämmelser i unionsrätten eller nationell rätt om tillgång till eller vidareutnyttjande av vissa kategorier av data, särskilt när det gäller beviljandet av tillgång till och utlämnandet av officiella handlingar, och
- b) offentliga myndigheters skyldigheter enligt unionsrätten eller nationell rätt att tillåta vidareutnyttjande av data eller krav som rör behandling av icke-personuppgifter.

I de fall då en sektorsspecifik unionsrätt eller nationell rätt föreskriver att offentliga myndigheter, leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer ska uppfylla särskilda ytterligare tekniska, administrativa eller organisatoriska krav, däribland genom ett auktorisations- eller certifieringssystem, ska de bestämmelserna i den sektorsspecifika unionsrätten eller den nationella rätten också tillämpas. Eventuella sådana särskilda ytterligare krav ska vara icke-diskriminerande, proportionella och objektivt motiverade.

3. Unionsrätt och nationell rätt om skydd av personuppgifter ska tillämpas på alla personuppgifter som behandlas i samband med denna förordning. Denna förordning påverkar i synnerhet inte tillämpningen av förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiven 2002/58/EG och (EU) 2016/680, inklusive vad gäller tillsynsmyndigheternas befogenheter och behörighet. Om den här förordningen står i strid med unionsrätten om skydd av personuppgifter eller nationell rätt som antagits i enlighet med sådan unionsrätt, bör den relevanta unionsrätten eller nationella rätten om skydd av personuppgifter ha företräde. Den här förordningen skapar inte någon rättslig grund för behandling av personuppgifter och påverkar inte heller några av de skyldigheter och rättigheter som anges i förordningarna (EU) 2016/679 eller (EU) 2018/1725 eller direktiven 2002/58/EG eller (EU) 2016/680.
4. Denna förordning påverkar inte tillämpningen av konkurrensrätten.
5. Denna förordning påverkar inte medlemsstaternas befogenheter när det gäller deras verksamhet som rör allmän säkerhet, försvar och nationell säkerhet.

## Artikel 2

## Definitioner

I denna förordning gäller följande definitioner:

1. *data*: varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, sådana fakta eller sådan information, däribland i form av ljudinspelningar, bildinspelningar eller audiovisuella inspelningar).
2. *vidareutnyttjande*: fysiska eller juridiska personers användning av data som innehas av offentliga myndigheter för andra kommersiella eller icke-kommersiella ändamål än det ursprungliga ändamål inom den offentliga verksamheten för vilket de framställdes, med undantag för utbyte av data mellan offentliga myndigheter som enbart sker i samband med deras offentliga verksamhet.
3. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.
4. *icke-personuppgifter*: andra data än personuppgifter.
5. *samtycke*: samtycke enligt definitionen i artikel 4.11 i förordning (EU) 2016/679.
6. *tillstånd*: att ge dataanvändare rätt att behandla icke-personuppgifter.
7. *registrerad*: registrerad som avses i artikel 4.1 i förordning (EU) 2016/679.
8. *datainnehavare*: en juridisk person, inklusive en offentlig myndighet och internationella organisationer, eller en fysisk person som inte är en registrerad i förhållande till de specifika uppgifterna i fråga, som i enlighet med tillämplig unionsrätt eller nationell rätt har rätt att bevilja tillgång till eller dela vissa personuppgifter eller icke-personuppgifter.
9. *dataanvändare*: fysisk eller juridisk person som har laglig tillgång till vissa personuppgifter eller icke-personuppgifter och som har rätt att, även enligt förordning (EU) 2016/679 när det gäller personuppgifter, använda dessa data för kommersiella eller icke-kommersiella ändamål.
10. *datadelning*: en registrerads eller datainnehavares tillhandahållande av data till en dataanvändare för gemensam eller individuell användning av dessa delade data, baserat på frivilliga avtal, unionsrätt eller nationell rätt, direkt eller via en förmedlare, till exempel inom ramen för öppna eller kommersiella licenser mot en avgift eller kostnadsfritt.
11. *dataförmedlingstjänst*: en tjänst som syftar till att med tekniska, rättsliga eller andra medel upprätta affärsförbindelser för datadelning mellan ett obestämt antal registrerade och datainnehavare, å ena sidan, och dataanvändare, å andra sidan, inbegripet för att utöva de registrerades rättigheter avseende personuppgifter, med uteslutande av åtminstone följande:
  - a) Tjänster som erhåller data från datainnehavare och aggregerar, berikar eller omvandlar data i syfte att avsevärt öka deras värde och licensierar användningen av resulterande data till dataanvändare, utan att upprätta en affärsförbindelse mellan datainnehavare och dataanvändare.
  - b) Tjänster som är inriktade på förmedling av upphovsrättsligt skyddat innehåll.
  - c) Tjänster som uteslutande används av en datainnehavare för att möjliggöra användning av de data som den datainnehavaren innehar, eller som används av flera juridiska personer en sluten grupp, inbegripet leverantörs- eller kundrelationer eller samarbeten som grundar sig på avtal, särskilt sådana som har som huvudsakligt syfte att säkerställa funktionerna för föremål och enheter som är anslutna till sakernas internet.
  - d) Datadelningstjänster som erbjuds av offentliga myndigheter som inte syftar till att upprätta affärsförbindelser.
12. *behandling*: behandling enligt definitionen i artikel 4.2 i förordning (EU) 2016/679 när det gäller personuppgifter eller artikel 3.2 i förordning (EU) 2018/1807 när det gäller icke-personuppgifter.
13. *tillgång*: dataanvändning i enlighet med särskilda tekniska, rättsliga eller organisatoriska krav, utan att det nödvändigtvis innefattar överföring eller nedladdning av data.
14. *huvudsakligt verksamhetsställe* för en juridisk person: platsen för dess centrala förvaltning i unionen.

15. *datakooperativs tjänster*: dataförmedlingstjänster som tillhandahålls av en organisationsstruktur i vilken registrerade, enmansföretag eller små och medelstora företag är medlemmar, och vars huvudsakliga syften är att hjälpa medlemmarna att utöva sina rättigheter avseende vissa data, så att de bland annat kan fatta välgrundade beslut innan de samtycker till databehandling, att utbyta synpunkter om de ändamål och villkor för databehandling som bäst företräder sina medlemmars intressen när det gäller deras data och att förhandla om villkoren för databehandling för sina medlemmar innan de ger tillstånd till behandling av icke-personuppgifter eller lämnar sitt samtycke till behandling av personuppgifter.
16. *dataaltruism*: den frivilliga delningen av data på grundval av de registrerades samtycke till behandling av personuppgifter som rör dem, eller tillstånd från datainnehavare att tillåta användning av deras icke-personuppgifter utan något krav på eller mottagande av ersättning utöver ersättning för de kostnader som de ådragit sig när de gör uppgifterna tillgängliga för mål av allmänintresse, som det föreskrivs i nationell rätt i förekommande fall, såsom hälso- och sjukvård, bekämpande av klimatförändringar, förbättring av mobiliteten, främjande av utveckling, framställning och spridning av officiell statistik, förbättrat tillhandahållande av offentliga tjänster, politiskt beslutsfattande eller vetenskaplig forskning av allmänt intresse.
17. *offentliga myndigheter*: statliga, regionala eller lokala myndigheter och offentligrättsliga organ, eller sammanslutningar av en eller flera sådana myndigheter eller av ett eller flera sådana offentligrättsliga organ.
18. *offentligrättsliga organ*: organ som har följande egenskaper:
  - a) De har särskilt inrättats för att tillgodose behov av allmänt intresse, och är inte av industriell eller kommersiell art.
  - b) De är juridiska personer.
  - c) De finansieras till största delen av statliga, regionala eller lokala myndigheter, eller andra offentligrättsliga organ, står under administrativ tillsyn av sådana myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, av regionala eller lokala myndigheter eller av andra offentligrättsliga organ.
19. *offentligt företag*: varje företag över vilket de offentliga myndigheterna har ett direkt eller indirekt bestämmande inflytande till följd av ägarförhållande, finansiellt deltagande eller gällande regler; inom ramen för denna definition ska offentliga myndigheter anses utöva bestämmande inflytande när dessa myndigheter, direkt eller indirekt,
  - a) äger större delen av det tecknade kapitalet i företaget,
  - b) kontrollerar majoriteten av de rösträtter som är knutna till företagets emitterade aktier,
  - c) kan utse fler än hälften av ledamöterna i företagets förvaltningsorgan, styrelseorgan eller övervakande organ.
20. *säker behandlingsmiljö*: fysisk eller virtuell miljö och organisatoriska metoder för att säkerställa överensstämmelse med unionsrätten, såsom förordning (EU) 2016/679, särskilt vad gäller de registrerades rättigheter, immateriella rättigheter samt insynsskydd, integritet och tillgänglighet för kommersiella och statistiska uppgifter, samt med tillämplig nationell rätt, och göra det möjligt för den enhet som tillhandahåller den säkra behandlingsmiljön att fastställa och övervaka alla databehandlingsåtgärder, inbegripet förevisandet, lagringen, nedladdningen och exporten av data och beräkningen av härledda data med hjälp av dataalgoritmer.
21. *rättslig företrädare*: en fysisk eller juridisk person etablerad i unionen som uttryckligen utsetts för att agera på uppdrag av en i unionen ej etablerad leverantör av dataförmedlingstjänster eller i unionen ej etablerad enhet som för syften av allmänt intresse samlar in data som tillhandahålls av fysiska eller juridiska personer baserat på dataaltruism, till vilken de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer kan vända sig till utöver eller i stället för leverantören av dataförmedlingstjänster eller enheten när det gäller skyldigheterna enligt denna förordning, inklusive när det gäller att inleda verkställighetsförfaranden mot en leverantör av dataförmedlingstjänster eller enhet som inte uppfyller kraven och som inte är etablerad i unionen.

## KAPITEL II

**Vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga myndigheter**

## Artikel 3

**Kategorier av data**

1. Detta kapitel ska tillämpas på data som innehas av offentliga myndigheter och som är skyddade på grund av
  - a) insynsskydd för kommersiella uppgifter, inklusive affärs-, yrkes- och företagshemligheter,
  - b) insynsskydd för statistiska uppgifter,
  - c) skydd av tredje parts immateriella rättigheter, eller
  - d) skydd av personuppgifter, i den mån sådana uppgifter faller utanför tillämpningsområdet för direktiv (EU) 2019/1024.
2. Detta kapitel ska inte tillämpas på
  - a) data som innehas av offentliga företag,
  - b) data som innehas av public service-bolag och deras dotterbolag och av andra organ eller deras dotterbolag för fullgörandet av ett uppdrag att verka i allmänhetens tjänst på radio- eller tv-området,
  - c) data som innehas av kulturinstitutioner och utbildningsinstitutioner,
  - d) data som innehas av offentliga myndigheter och är skyddade av skäl som rör allmän säkerhet, försvar eller nationell säkerhet, eller
  - e) data vars tillhandahållande inte omfattas av den offentliga verksamhet som bedrivs av de berörda offentliga myndigheterna, såsom den definieras i lagstiftning eller andra bindande regler i den berörda medlemsstaten eller, om sådana regler saknas, såsom den definieras i enlighet med gängse administrativ praxis i denna, förutsatt att den offentliga verksamheten är tydligt avgränsad och föremål för översyn.
3. Detta kapitel påverkar inte tillämpningen av
  - a) unionsrätten, nationell rätt och internationella avtal som unionen eller medlemsstaterna är parter i och som avser skydd av de kategorier av data som avses i punkt 1, och
  - b) unionsrätt och nationell rätt om tillgång till handlingar.

## Artikel 4

**Förbud mot exklusiva avtal**

1. Det ska vara förbjudet med avtal eller annan praxis som rör vidareutnyttjande av data som innehas av offentliga myndigheter och som omfattar kategorier av data som avses i artikel 3.1, vilka omfattar beviljande av exklusiva rättigheter eller vars syfte eller verkan omfattar beviljande av sådana exklusiva rättigheter eller begränsning av tillgången till data för vidareutnyttjande av andra enheter än parterna i sådana avtal eller sådan annan praxis.
2. Med avvikelse från punkt 1 får en exklusiv rättighet beviljas för vidareutnyttjande av data som avses i den punkten i den mån som det är nödvändigt för tillhandahållande av en tjänst eller tillhandahållande av en produkt av allmänt intresse som annars inte skulle vara möjligt.
3. En exklusiv rättighet som avses i punkt 2 ska beviljas genom en administrativ åtgärd eller ett kontraktsmässigt arrangemang i enlighet med tillämplig unionsrätt eller nationell rätt och i enlighet med principerna om transparens, likabehandling och icke-diskriminering.
4. Perioden för en exklusiv rättighet till vidareutnyttjande av data får inte överstiga tolv månader. När ett avtal har ingåtts ska avtalets löptid vara samma som perioden för den exklusiva rättigheten.

5. Beviljandet av en exklusiv rättighet i enlighet med punkterna 2, 3 och 4, inklusive skälen till varför detta beviljande är nödvändigt, ska vara transparenta och göras allmänt tillgängliga online i en form som är förenlig med relevant unionslagsrätt om offentlig upphandling.

6. Avtal eller andra metoder som omfattas av tillämpningsområdet för det förbud som avses i punkt 1, som inte uppfyller de villkor som fastställs i punkterna 2 och 3 och som ingicks före den 23 juni 2022 ska upphöra att gälla när det tillämpliga avtalet löper ut och i vilket fall senast den 24 december 2024.

#### Artikel 5

#### Villkor för vidareutnyttjande

1. Offentliga myndigheter som enligt nationell rätt är behöriga att bevilja eller vägra tillgång till vidareutnyttjandet av en eller flera kategorier av data som avses i artikel 3.1 ska offentliggöra villkoren för att tillåta sådant vidareutnyttjande samt förfarandet för att begära vidareutnyttjandet via den gemensamma informationspunkt som avses i artikel 8. När de beviljar eller vägrar tillgång till vidareutnyttjande får de bistås av de behöriga organ som avses i artikel 7.1.

Medlemsstaterna ska säkerställa att offentliga myndigheter är försedda med nödvändiga resurser för att efterleva denna artikel.

2. Villkoren för vidareutnyttjande ska vara icke-diskriminerande, transparenta, proportionerliga och objektivt motiverade med hänsyn till kategorierna av data, vidareutnyttjandets syfte och typerna av data för vilka vidareutnyttjande tillåts. Dessa villkor får inte användas för att begränsa konkurrensen.

3. Offentliga myndigheter ska i enlighet med unionsrätt och nationell rätt säkerställa att uppgifternas skyddade karaktär bevaras. De kan föreskriva följande krav:

- a) Att tillgång till vidareutnyttjande av data beviljas endast om den offentliga myndigheten eller det behöriga organet efter begäran om vidareutnyttjande har säkerställt att data har
  - i) anonymiserats, när det gäller personuppgifter, och
  - ii) ändrats, aggregerats eller behandlats med någon annan metod för kontroll av utlämnande, när det gäller affärshemligheter, inbegripet företagshemligheter eller innehåll som skyddas av immateriella rättigheter.
- b) Att tillgång till och vidareutnyttjande av data på distans sker inom en säker behandlingsmiljö som tillhandahålls eller kontrolleras av den offentliga myndigheten.
- c) Att tillgång till och vidareutnyttjande av data säkerställs i de fysiska lokaler där den säkra behandlingsmiljön är belägen i enlighet med höga säkerhetsnormer, förutsatt att fjärråtkomst inte kan tillåtas utan att tredje parters rättigheter och intressen hotas.

4. Om vidareutnyttjande har tillåtits i enlighet med punkt 3 b och c, ska offentliga myndigheter införa villkor som bevarar integriteten för de tekniska systemens funktionssätt i den säkra behandlingsmiljön. Offentliga myndigheter ska förbehålla sig rätten att verifiera processen, metoderna och alla resultat från den behandling av data som görs av vidareutnyttjaren för att bevara integriteten i dataskyddet och förbehålla sig rätten att förbjuda användningen av resultat som innehåller information som hotar tredje parters rättigheter och intressen. Beslutet att förbjuda användningen av resultat ska vara lättbegripligt och tydligt för vidareutnyttjaren.

5. Såvida det i den nationella rätten inte föreskrivs särskilda skyddsåtgärder för tillämpliga skyldigheter i fråga om konfidentiell behandling avseende det vidareutnyttjande av data som avses i artikel 3.1, ska den offentliga myndigheten ställa som villkor för vidareutnyttjandet av data som tillhandahålls i enlighet med punkt 3 i den här artikeln att vidareutnyttjaren uppfyller en skyldighet i fråga om konfidentiell behandling som förbjuder utlämnande av information som äventyrar tredje parts rättigheter och intressen som vidareutnyttjaren kan ha erhållit trots de skyddsåtgärder som införts. Det ska vara förbjudet för vidareutnyttjare att återidentifiera de registrerade som uppgifterna gäller, och vidareutnyttjarna ska vidta tekniska och operativa åtgärder för att förhindra återidentifiering och underrätta den offentliga myndigheten om alla uppgiftsincidenter som leder till att berörda registrerade återidentifieras. Vid otillåtet vidareutnyttjande av icke-personuppgifter ska vidareutnyttjaren utan dröjsmål, och när så är lämpligt med bistånd från den offentliga myndigheten, underrätta de juridiska personer vars rättigheter och intressen kan påverkas.

6. I de fall då vidareutnyttjande av data inte kan tillåtas i enlighet med de skyldigheter som fastställs i punkterna 3 och 4 i denna artikel, och det inte finns någon rättslig grund för överföring av data inom ramen för förordning (EU) 2016/679, ska den offentliga myndigheten, i den utsträckning det är tillåtet i enlighet med unionsrätten och nationell rätt, göra sitt yttersta för att bistå potentiella vidareutnyttjare som begär de registrerades samtycke eller tillstånd från datainnehavare vars rättigheter och intressen kan påverkas av ett sådant vidareutnyttjande, om detta är möjligt utan en oproportionell börda för den offentliga myndigheten. När den tillhandahåller sådant bistånd får den offentliga myndigheten bistås av de behöriga organ som avses i artikel 7.1.

7. Vidareutnyttjande av data ska endast tillåtas i enlighet med immateriella rättigheter. En databasproducents rätt som föreskrivs i artikel 7.1 i direktiv 96/9/EG får inte utövas av offentliga myndigheter för att förhindra vidareutnyttjande av data eller begränsa vidareutnyttjandet i högre grad än vad som anges i den här förordningen.

8. Om data som begärs anses vara konfidentiella i enlighet med unionsrätten eller nationell rätt om affärshemligheter eller insynskydd för statistiska uppgifter, ska de offentliga myndigheterna säkerställa att dessa konfidentiella data inte röjs till följd av att vidareutnyttjande tillåts, såvida inte sådant vidareutnyttjande är tillåtet i enlighet med punkt 6.

9. I de fall då en vidareutnyttjare avser att överföra icke-personuppgifter som är skyddade på grund av de skäl som anges i artikel 3.1 till ett tredjeland, ska vidareutnyttjaren underrätta den offentliga myndigheten om sin avsikt att överföra sådana uppgifter och om syftet med en sådan överföring vid tidpunkten för begäran om vidareutnyttjande av dessa data. Vid vidareutnyttjande i enlighet med punkt 6 i den här artikeln, ska vidareutnyttjaren, när så är lämpligt med bistånd från den offentliga myndigheten, underrätta den juridiska personen vars rättigheter och intressen kan påverkas av denna avsikt, om detta syfte och de lämpliga skyddsåtgärderna. Den offentliga myndigheten får inte tillåta vidareutnyttjandet om inte den juridiska personen ger sitt tillstånd till överföringen.

10. Offentliga myndigheter får överföra konfidentiella data som inte är personuppgifter eller data som skyddas av immateriella rättigheter till en vidareutnyttjare som avser att överföra dessa data till ett annat tredjeland än ett land som utsetts i enlighet med punkt 12 endast om vidareutnyttjaren avtalsmässigt åtar sig att

- a) fullgöra de skyldigheter som införts i enlighet med punkterna 7 och 8 även efter att data överförts till det berörda tredjelandet, och
- b) godta jurisdiktionen för domstolarna i den överförande offentliga myndighetens medlemsstat när det gäller eventuella tvister som rör efterlevnaden av punkterna 7 och 8.

11. Offentliga myndigheter ska, när så är lämpligt och i den utsträckning de kan, ge vidareutnyttjare vägledning och bistånd i fullgörandet av de skyldigheter som avses i punkt 10 i denna artikel.

För att bistå de offentliga myndigheterna och vidareutnyttjarna får kommissionen anta genomförandeakter som fastställer standardavtalsklausuler för fullgörande av de skyldigheter som avses i punkt 10 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 33.3.

12. När så motiveras på grund av ett betydande antal begäranden i hela unionen om vidareutnyttjandet av icke-personuppgifter i specifika tredjeländer får kommissionen anta genomförandeakter i vilka det intygas att ett tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang

- a) säkerställer ett skydd för immateriella rättigheter och företagshemligheter som i allt väsentligt är likvärdigt med det skydd som säkerställs genom unionsrätten,
- b) tillämpas och verkställs på ett effektivt sätt, och
- c) omfattar effektiva rättsmedel.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 33.3.

13. Enligt särskilda unionslagstiftningsakter kan vissa kategorier av icke-personuppgifter som innehas av offentliga myndigheter anses vara mycket känsliga vid tillämpningen av denna artikel, när överföringen av dem till tredjeländer kan äventyra unionens offentligpolitiska mål, exempelvis säkerhet och folkhälsa, eller leda till risk för återidentifiering av anonymiserade data som inte är personuppgifter. Om en sådan akt antas ska kommissionen anta delegerade akter i enlighet med artikel 32 som kompletterar denna förordning genom att fastställa särskilda villkor som ska tillämpas på överföring av sådana uppgifter till tredjeländer.

Dessa särskilda villkor ska baseras på typen av de kategorier av icke-personuppgifter som anges i den särskilda unionslagstiftningsakten och skälen för att anse dessa kategorier vara mycket känsliga, med beaktande av riskerna för återidentifiering av anonymiserade data som inte är personuppgifter. De ska vara icke-diskriminerande och begränsade till vad som är nödvändigt för att uppnå de unionens offentligpolitiska mål som anges i den akten, i enlighet med unionens internationella skyldigheter.

Om så krävs enligt de särskilda unionslagstiftningsakter som avses i första stycket, kan sådana särskilda villkor innefatta villkor som är tillämpliga på överföring eller tekniska avtal i detta hänseende, begränsningar vad gäller vidareutnyttjande av data i tredjeländer eller kategorier av personer som har rätt att överföra sådana data till tredjeländer eller, i exceptionella fall, begränsningar vad gäller överföring till tredjeländer.

14. De fysiska eller juridiska personer som beviljades rätten att vidareutnyttja icke-personuppgifter får endast överföra dessa data till de tredjeländer för vilka kraven i punkterna 10, 12 och 13 uppfylls.

#### Artikel 6

#### Avgifter

1. Offentliga myndigheter som tillåter vidareutnyttjande av de kategorier av data som avses i artikel 3.1 får ta ut en avgift för att tillåta vidareutnyttjandet av sådana data.
2. Avgifter som tas ut i enlighet med punkt 1 ska vara transparenta, icke-diskriminerande, proportionella och objektivt motiverade och får inte begränsa konkurrensen.
3. Offentliga myndigheter ska säkerställa att alla avgifter också kan betalas online med hjälp av allmänt tillgängliga gränsoverskridande betalningstjänster, utan diskriminering på grund av betaltjänstleverantörens etableringsort, betalningsinstrumentets utfärdandeort eller den plats där betalkontot finns inom unionen.
4. När offentliga myndigheter tar ut avgifter ska de vidta åtgärder för att ge incitament till vidareutnyttjande av de kategorier av data som avses i artikel 3.1 för icke-kommersiella ändamål, såsom vetenskaplig forskning, och av små och medelstora företag och uppstarts företag i enlighet med reglerna för statligt stöd. I detta avseende får de offentliga myndigheterna också göra dessa data tillgängliga till en nedsatt avgift eller kostnadsfritt, särskilt för små och medelstora företag och uppstarts företag, det civila samhället och utbildningsanstalter. Offentliga myndigheter får därför upprätta en förteckning över kategorier av vidareutnyttjare för vilka data för vidareutnyttjande ska göras tillgängliga till en nedsatt avgift eller kostnadsfritt. Förteckningen och kriterierna för upprättande av den ska offentliggöras.
5. Avgifterna ska härledas från kostnaderna för att genomföra förfarandet för begäran om vidareutnyttjande av de kategorier av data som avses i artikel 3.1, och vara begränsade till nödvändiga kostnader i samband med
  - a) reproduktion, tillhandahållande och spridning av data,
  - b) klarering av upphovsrätt,
  - c) anonymisering eller andra former av framställning av personuppgifter och affärshemligheter som föreskrivs i artikel 5.3,
  - d) underhåll av den säkra behandlingsmiljön,
  - e) förvärvande av rätten att tillåta vidareutnyttjande i enlighet med detta kapitel av tredje parter utanför den offentliga sektorn, och
  - f) bistånd till vidareutnyttjare som begär de registrerades samtycke och tillstånd från datainnehavare vars rättigheter och intressen kan påverkas av ett sådant vidareutnyttjande.



6. Kriterierna och metoden för beräkning av avgifter ska fastställas av medlemsstaterna och offentliggöras. Offentliga myndigheter ska offentliggöra en beskrivning av huvudkategorierna av kostnader och reglerna för fördelning av kostnader.

#### Artikel 7

##### Behöriga organ

1. För utförandet av de uppgifter som avses i denna artikel ska varje medlemsstat utse ett eller flera behöriga organ, som får vara behöriga för särskilda sektorer, för att bistå de offentliga myndigheter som beviljar eller vägrar tillgång för vidareutnyttjande av de kategorier av data som avses i artikel 3.1. Medlemsstaterna får antingen inrätta ett eller flera nya behöriga organ eller förlita sig på befintliga offentliga myndigheter eller interna avdelningar inom offentliga myndigheter som uppfyller de villkor som fastställs i denna förordning.

2. De behöriga organen får ges befogenhet att bevilja tillgång till vidareutnyttjande av de kategorier av data som avses i artikel 3.1, i enlighet med unionsrätten eller nationell rätt som medger att sådan tillgång beviljas. När de beviljar eller vägrar tillgång för vidareutnyttjande ska artiklarna 4, 5, 6 och 9 tillämpas på dessa behöriga organ.

3. Behöriga organ ska ha tillräckliga juridiska, ekonomiska och tekniska resurser och personalresurser för att utföra de uppgifter som de anförtrots, inbegripet de nödvändiga tekniska kunskaperna för att kunna följa relevant unionsrätt eller nationell rätt om systemen för tillgång till de kategorier av data som avses i artikel 3.1.

4. Det bistånd som föreskrivs i punkt 1 ska, när så är nödvändigt, innefatta följande:

- a) Tekniskt stöd för att tillhandahålla en säker behandlingsmiljö för att ge tillgång till vidareutnyttjande av data.
- b) Vägledning och tekniskt stöd om hur data bäst kan struktureras och lagras så att dessa data är lättillgängliga.
- c) Tekniskt stöd för pseudonymisering och för att säkerställa databehandling på ett sätt som effektivt bevarar integriteten, konfidentialiteten, dataintegriteten och tillgängligheten för den information som finns i de data för vilka vidareutnyttjande tillåts, däribland teknik för anonymisering, generalisering, undertryckande och randomisering av personuppgifter eller andra toppmoderna integritetsbevarande metoder och radering av kommersiellt känslig information, däribland affärshemligheter eller innehåll som är skyddat av immateriella rättigheter.
- d) Bistånd till offentliga myndigheter, i förekommande fall, för att stödja vidareutnyttjare när de begär registrerades samtycke till vidareutnyttjande eller datainnehavares tillstånd i linje med deras särskilda beslut, däribland om den jurisdiktion där databehandlingen är avsedd att utföras, och bistånd till offentliga myndigheter när de behöver inrätta tekniska mekanismer som gör det möjligt att vidarebefordra begäranden om samtycke eller tillstånd från vidareutnyttjare, när detta är praktiskt genomförbart.
- e) Bistånd till offentliga myndigheter vid bedömningen av tillräckligheten i de avtalsmässiga åtaganden som görs av en vidareutnyttjare i enlighet med artikel 5.10.

5. Varje medlemsstat ska senast den 24 september 2023 meddela kommissionen vilka behöriga organ som utsetts i enlighet med punkt 1. Varje medlemsstat ska också meddela kommissionen alla senare ändringar av dessa behöriga organs identitet.

#### Artikel 8

##### Gemensamma informationspunkter

1. Medlemsstaterna ska säkerställa att all relevant information om tillämpningen av artiklarna 5 och 6 finns tillgänglig och lätt åtkomlig via en gemensam informationspunkt. Medlemsstaterna ska inrätta ett nytt organ eller utse ett befintligt organ som gemensam informationspunkt. Den gemensamma informationspunkten kan vara länkad till sektoriella, regionala eller lokala informationspunkter. En gemensam informationspunkts funktioner får vara automatiserade förutsatt att den offentliga myndigheten säkerställer tillräckligt stöd.

2. Den gemensamma informationspunkten ska vara behörig att ta emot förfrågningar eller ansökningar om vidareutnyttjande av de kategorier av data som avses i artikel 3.1 och ska när så är möjligt och lämpligt automatiskt överföra dessa till de behöriga offentliga myndigheter som avses i artikel 7.1, i förekommande fall. Den gemensamma informationspunkten ska på elektronisk väg tillhandahålla en sökbar tillgångsförteckning som innehåller en översikt över alla tillgängliga datakällor, däribland, i relevanta fall, de datakällor som finns tillgängliga vid sektorspecifika, regionala och lokala informationspunkter, tillsammans med relevant information som beskriver tillgängliga data, inbegripet åtminstone dataformatet och datastorleken samt villkoren för vidareutnyttjandet av dessa data.

3. Den gemensamma informationspunkten får inrätta en separat, förenklad och väldokumenterad informationskanal för små och medelstora företag och nystartade företag som möter deras behov och förmågor i samband med begäran av vidareutnyttjande av de kategorier av data som avses i artikel 3.1.

4. Kommissionen ska inrätta en europeisk gemensam åtkomstpunkt som erbjuder ett sökbart elektroniskt register över tillgängliga data i nationella gemensamma informationspunkter och ytterligare information om hur man begär data via dessa nationella gemensamma informationspunkter.

#### Artikel 9

### Behandling av begäranden om vidareutnyttjande

1. Såvida inte kortare tidsfrister har fastställts i enlighet med nationell rätt ska de behöriga offentliga myndigheterna eller de behöriga organ som avses i artikel 7.1 anta ett beslut om begäran om vidareutnyttjande av de kategorier av data som avses i artikel 3.1 inom två månader från dagen för mottagandet av begäran.

Vid exceptionellt omfattande och komplicerade begäranden om vidareutnyttjande får denna tvåmånadersperiod förlängas med högst 30 dagar. I sådana fall ska de behöriga offentliga myndigheterna eller de behöriga organ som avses i artikel 7.1 underrätta den sökande så snart som möjligt om att mer tid krävs för att genomföra förfarandet, tillsammans med skälen till dröjsmålet.

2. Fysiska eller juridiska personer som direkt påverkas av ett beslut såsom avses i punkt 1 ska ha effektiv rätt till överprövning i den medlemsstat där det relevanta organet är lokaliserat. Denna rätt till överprövning ska föreskrivas i nationell rätt och inbegripa möjlighet till omprövning av en opartisk myndighet som besitter lämplig sakkunskap, såsom den nationella konkurrensmyndigheten, den berörda myndigheten för tillgång till handlingar, den tillsynsmyndighet som inrättats i enlighet med förordning (EU) 2016/679 eller en nationell rättslig myndighet, vars beslut är bindande för den berörda offentliga myndigheten eller det berörda behöriga organet.

#### KAPITEL III

### Krav som är tillämpliga på dataförmedlingstjänster

#### Artikel 10

### Dataförmedlingstjänster

Tillhandahållandet av följande dataförmedlingstjänster ska uppfylla artikel 12 och ska omfattas av ett anmälningsförfarande:

- Förmedlingstjänster mellan datainnehavare och potentiella dataanvändare, däribland tillhandahållandet av tekniska eller andra metoder för att möjliggöra sådana tjänster; dessa tjänster kan innefatta bilaterala eller multilaterala utbyten av data eller inrättandet av plattformar eller databaser som möjliggör utbyte eller gemensam användning av data, liksom inrättandet av annan särskild infrastruktur för sammankoppling av datainnehavare med dataanvändare.
- Förmedlingstjänster mellan de registrerade som önskar göra sina personuppgifter tillgängliga, och potentiella dataanvändare, däribland tillhandahållandet av tekniska eller andra metoder för att möjliggöra sådana tjänster, och i synnerhet som möjliggör utövandet av de registrerades rättigheter som föreskrivs i förordning (EU) 2016/679.
- Datakooperativs tjänster.

## Artikel 11

**Anmälning från leverantörer av dataförmedlingstjänster**

1. Varje leverantör av dataförmedlingstjänster som avser att tillhandahålla de dataförmedlingstjänster som avses i artikel 10 ska lämna en anmälan till den behöriga myndigheten för dataförmedlingstjänster.
2. Vid tillämpning av denna förordning ska en leverantör av dataförmedlingstjänster med verksamhetsställen i mer än en medlemsstat anses omfattas av jurisdiktionen i den medlemsstat där den har sitt huvudsakliga verksamhetsställe, utan att det påverkar unionslagrätten som reglerar gränsöverskridande skadeståndstalan och tillhörande förfaranden.
3. En leverantör av dataförmedlingstjänster som inte är etablerad i unionen men som i unionen erbjuder de dataförmedlingstjänster som avses i artikel 10 ska utse en rättslig företrädare i en av de medlemsstater där dessa tjänster erbjuds.

För att säkerställa efterlevnaden av denna förordning ska leverantören av dataförmedlingstjänster ge den rättslige företrädaren uppdraget att utöver eller i stället för denna kunna kontaktas av behöriga myndigheter för dataförmedlingstjänster eller registrerade och datainnehavare i alla frågor som rör de tillhandahållna dataförmedlingstjänsterna. Den rättslige företrädaren ska samarbeta med de behöriga myndigheterna för dataförmedlingstjänster och, på begäran, för dessa på ett övergripande sätt påvisa de åtgärder som vidtagits och de bestämmelser som införts av leverantören av dataförmedlingstjänster för att säkerställa överensstämmelse med denna förordning.

Leverantören av dataförmedlingstjänster ska anses omfattas av jurisdiktionen i den medlemsstat där den rättslige företrädaren finns. Att en leverantör av dataförmedlingstjänster utser en rättslig företrädare ska inte påverka eventuella rättsliga åtgärder som kan vidtas mot leverantören av dataförmedlingstjänster.

4. Efter att ha lämnat en anmälan i enlighet med punkt 1 får leverantören av dataförmedlingstjänster inleda verksamheten i enlighet med de villkor som fastställs i detta kapitel.
5. Den anmälan som avses i punkt 1 ska ge leverantören av dataförmedlingstjänster rätt att tillhandahålla dataförmedlingstjänster i alla medlemsstater.
6. Den anmälan som avses i punkt 1 ska innehålla följande uppgifter:
  - a) Namnet på leverantören av dataförmedlingstjänster.
  - b) Dataförmedlingstjänsteleverantörens rättsliga status, form, ägarstruktur, relevanta dotterföretag och, om leverantören av dataförmedlingstjänster är registrerad i ett handelsregister eller annat liknande offentligt nationellt register, registreringsnummer
  - c) Adressen till dataförmedlingstjänsteleverantörens huvudsakliga verksamhetsställe i unionen, i förekommande fall, och, om tillämpligt, eventuella underordnade filialer i en annan medlemsstat, eller till den rättslige företrädaren.
  - d) En offentlig webbplats med fullständig och uppdaterad information om leverantören av dataförmedlingstjänster och verksamheten, inbegripet åtminstone den information som avses i leden a, b, c och f.
  - e) Dataförmedlingstjänsteleverantörens kontaktpersoner och kontaktuppgifter.
  - f) En beskrivning av den dataförmedlingstjänst som leverantören av dataförmedlingstjänster avser att tillhandahålla och en uppgift om de kategorier som förtecknas i artikel 10 som dessa dataförmedlingstjänster omfattas av.
  - g) Beräknat startdatum för verksamheten, om ett annat än anmälningsdatumet.
7. Den behöriga myndigheten för dataförmedlingstjänster ska säkerställa att anmälningsförfarandet är icke-diskriminerande och inte snedvrider konkurrensen.

8. På begäran av leverantören av dataförmedlingstjänster ska den behöriga myndigheten för dataförmedlingstjänster inom en vecka från och med en vederbörligen och fullständigt genomförd anmälan utfärda en standardiserad förklaring som bekräftar att leverantören av dataförmedlingstjänster har inkommit med den anmälan som avses i punkt 1 och att anmälan innehåller de uppgifter som avses i punkt 6.

9. På begäran av leverantören av dataförmedlingstjänster ska den behöriga myndigheten för dataförmedlingstjänster bekräfta att leverantören av dataförmedlingstjänster uppfyller denna artikel och i artikel 12. När leverantören av dataförmedlingstjänster har mottagit en sådan bekräftelse får den i sin skriftliga och muntliga kommunikation använda beteckningen "leverantör av dataförmedlingstjänster som är erkänd i unionen" samt en gemensam logotyp.

För att säkerställa att leverantörer av dataförmedlingstjänster som är erkända i unionen lätt kan identifieras i hela unionen ska kommissionen genom genomförandeakter fastställa den gemensamma logotypens utformning. Leverantörer av dataförmedlingstjänster som är erkända i unionen ska tydligt visa den gemensamma logotypen på alla online- och offline-publikationer som anknuter till deras dataförmedlingsverksamhet.

Dessa genomförandeakter ska antas i enlighet med det rådgivande förfarande som avses i artikel 33.2.

10. Den behöriga myndigheten för dataförmedlingstjänster ska på elektronisk väg och utan dröjsmål underrätta kommissionen om varje ny anmälan. Kommissionen ska föra och regelbundet uppdatera ett offentligt register över alla leverantörer av dataförmedlingstjänster som tillhandahåller sina tjänster i unionen. De uppgifter som avses i punkt 6 a, b, c, d, f och g ska offentliggöras i det offentliga registret.

11. Den behöriga myndigheten för dataförmedlingstjänster får ta ut avgifter för anmälan i enlighet med nationell rätt. Sådana avgifter ska vara proportionella och objektiva och baseras på de administrativa kostnaderna för de behöriga myndigheterna för dataförmedlingstjänsters övervakning av efterlevnaden och andra marknadskontrollåtgärder avseende anmälningar av leverantörer av dataförmedlingstjänster. För små och medelstora företag samt nystartade företag får den behöriga myndigheten ta ut en nedsatt avgift eller avstå från avgiften.

12. Leverantörer av dataförmedlingstjänster ska underrätta den behöriga myndigheten för dataförmedlingstjänster om alla ändringar av den information som tillhandahållits i enlighet med punkt 6 inom 14 dagar från dagen för ändringen.

13. När en leverantör av dataförmedlingstjänster upphör med sin verksamhet ska den inom 15 dagar underrätta den berörda behöriga myndighet för dataförmedlingstjänster som fastställts i enlighet med punkterna 1, 2 och 3.

14. Den behöriga myndigheten för dataförmedlingstjänster ska på elektronisk väg och utan dröjsmål underrätta kommissionen om varje underrättelse som avses i punkterna 12 och 13. Kommissionen ska uppdatera det offentliga registret över leverantörer av dataförmedlingstjänster i unionen i enlighet med detta.

#### Artikel 12

#### Villkor för tillhandahållande av dataförmedlingstjänster

Tillhandahållandet av de dataförmedlingstjänster som avses i artikel 10 ska omfattas av följande villkor:

- a) Leverantören av dataförmedlingstjänster får inte använda de data för vilka dataförmedlingstjänsterna tillhandahålls för andra ändamål än att ställa dem till dataanvändarnas förfogande och ska tillhandahålla dataförmedlingstjänsterna via en separat juridisk person.
- b) De kommersiella villkoren, inklusive prissättningen, för tillhandahållandet av dataförmedlingstjänster till en datainnehavare eller dataanvändare får inte knytas till huruvida datainnehavaren eller dataanvändaren använder andra tjänster från samma leverantör av dataförmedlingstjänster eller en närstående enhet, och i så fall i vilken utsträckning datainnehavaren eller dataanvändaren använder sådana andra tjänster.

- c) De data som samlas in om en fysisk eller juridisk persons aktivitet för tillhandahållandet av dataförmedlingstjänsten, däribland datum, tid, geolokaliseringsdata, aktivitetens varaktighet och kopplingar till andra fysiska eller juridiska personer som har inrättats av den person som använder dataförmedlingstjänsten får endast användas för utvecklingen av denna dataförmedlingstjänst, vilket kan innebära användning av data för att upptäcka bedrägerier eller för cybersäkerhet, och ska på begäran göras tillgängliga för datainnehavare.
- d) Leverantören av dataförmedlingstjänster ska främja ett utbyte av data i det format som den erhåller dessa data från en registrerad eller en datainnehavare, ska endast konvertera data till särskilda format för att öka interoperabiliteten inom och mellan sektorer, eller om datainnehavaren så begär eller detta föreskrivs i unionsrätten, eller för att säkerställa harmonisering med internationella eller europeiska datastandarder och ska erbjuda registrerade och datainnehavare en möjlighet till undantag avseende dessa konverteringar, såvida inte konverteringen föreskrivs i unionsrätten.
- e) Dataförmedlingstjänster får omfatta erbjudande av ytterligare särskilda verktyg och tjänster till datainnehavare eller de registrerade för det särskilda syftet att underlätta utbytet av data, exempelvis i form av tillfällig lagring, kuratering, konvertering, anonymisering och pseudonymisering, varvid sådana verktyg endast får användas på uttrycklig begäran eller efter uttryckligt godkännande av datainnehavaren eller den registrerade, och tredjepartsverktyg som erbjuds i sammanhanget inte får användas för andra ändamål.
- f) Leverantören av dataförmedlingstjänster ska säkerställa att förfarandet för tillgång till dess tjänster är rättvist, transparent och icke-diskriminerande för både registrerade och datainnehavare samt för dataanvändare, även när det gäller prissättning och villkor för tjänsten.
- g) Leverantören av dataförmedlingstjänster ska ha infört förfaranden för att förhindra bedrägerier eller otillbörliga metoder i samband med parter som önskar sådan tillgång via dess dataförmedlingstjänster.
- h) Leverantören av dataförmedlingstjänster ska, vid sin insolvens, säkerställa en rimlig kontinuitet i tillhandahållandet av sina dataförmedlingstjänster och, när sådana dataförmedlingstjänster säkerställer lagring av data, ha mekanismer på plats för att möjliggöra att datainnehavarna och dataanvändarna kan få tillgång till, överföra eller hämta sina data, och om sådana dataförmedlingstjänster tillhandahålls mellan registrerade och dataanvändare, göra det möjligt för registrerade att utöva sina rättigheter.
- i) Leverantören av dataförmedlingstjänster ska vidta lämpliga åtgärder för att säkerställa interoperabiliteten med andra dataförmedlingstjänster genom bland annat allmänt använda öppna standarder inom den sektor i vilken leverantören av dataförmedlingstjänster är verksam.
- j) Leverantören av dataförmedlingstjänster ska vidta tillräckliga tekniska, rättsliga och organisatoriska åtgärder för att förhindra sådan överföring av eller tillgång till icke-personuppgifter som strider mot unionsrätten eller den nationella rätten i den berörda medlemsstaten.
- k) Leverantören av dataförmedlingstjänster ska utan dröjsmål informera datainnehavarna vid ootillåten överföring av, tillgång till eller användning av icke-personuppgifter som den har delat.
- l) Leverantören av dataförmedlingstjänster ska vidta nödvändiga åtgärder för att säkerställa en lämplig säkerhetsnivå för lagringen, behandlingen och överföringen av icke-personuppgifter, och leverantören av dataförmedlingstjänster ska vidare säkerställa högsta säkerhet för lagringen och överföringen av information som är känslig i konkurrenshänseende.
- m) Leverantören av dataförmedlingstjänster som erbjuder tjänster åt de registrerade ska handla i deras bästa intresse när den främjar deras utövande av sina rättigheter, i synnerhet genom att informera och, i lämpliga fall, ge de registrerade råd på ett koncist, transparent, begripligt och lättåtkomligt sätt om dataanvändarnas avsedda dataanvändningar och de standardvillkor som är förbundna med sådan användning, innan de registrerade ger sitt samtycke.
- n) Om en leverantör av dataförmedlingstjänster tillhandahåller verktyg för att erhålla de registrerades samtycke eller erhålla tillstånd att behandla data som tillhandahålls av datainnehavare, ska den i relevanta fall ange inom vilken tredjelandsjurisdiktion som dataanvändningen är avsedd att äga rum och förse de registrerade med verktyg för att både ge och återkalla sitt samtycke och datainnehavarna med verktyg för att både ge och återkalla tillstånd för behandling av data.
- o) Leverantören av dataförmedlingstjänster ska föra ett loggregister över dataförmedlingsverksamheten.

## Artikel 13

**Behöriga myndigheter för dataförmedlingstjänster**

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter för att utföra uppgifter i samband med anmälningsförfarandet för dataförmedlingstjänster och ska meddela kommissionen dessa behöriga myndigheters identitet senast den 24 september 2023. Varje medlemsstat ska även meddela kommissionen alla eventuella senare ändringar av dessa behöriga myndigheters identitet.
2. De behöriga myndigheterna för dataförmedlingstjänster ska uppfylla de krav som anges i artikel 26.
3. Befogenheterna för de utsedda behöriga myndigheterna för dataförmedlingstjänsters ska inte påverka befogenheterna för dataskyddsmyndigheterna, de nationella konkurrensmyndigheterna, de myndigheter som ansvarar för cybersäkerhet och andra relevanta sektorsmyndigheter. Dessa myndigheter ska i enlighet med sina respektive befogenheter enligt unionsrätten och nationell rätt etablera ett starkt samarbete och utbyta den information som behövs för att de ska kunna utföra sina uppgifter i förhållande till leverantörerna av dataförmedlingstjänster, och ska eftersträva att de beslut som fattas vid tillämpningen av denna förordning är konsekventa.

## Artikel 14

**Övervakning av efterlevnaden**

1. De behöriga myndigheterna för dataförmedlingstjänster ska övervaka och utöva tillsyn över leverantörer av dataförmedlingstjänsters efterlevnad av kraven i detta kapitel. De behöriga myndigheterna för dataförmedlingstjänster får även övervaka och utöva tillsyn över leverantörer av dataförmedlingstjänsters efterlevnad på grundval av en begäran från en fysisk eller juridisk person.
2. De behöriga myndigheterna för dataförmedlingstjänster ska ha befogenhet att från leverantörer av dataförmedlingstjänster eller deras rättsliga företrädare begära all information som är nödvändig för att kontrollera uppfyllandet av kraven i detta kapitel. Varje begäran om information ska stå i proportion till uppgiftens utförande och innehålla en motivering.
3. I de fall då den behöriga myndigheten för dataförmedlingstjänster finner att en leverantör av dataförmedlingstjänster inte uppfyller ett eller flera av kraven i detta kapitel ska den meddela leverantören av dataförmedlingstjänster dessa iakttagelser och ge den möjlighet att yttra sig, inom 30 dagar från mottagandet av meddelandet.
4. Den behöriga myndigheten för dataförmedlingstjänster ska ha befogenhet att kräva att den överträdelse som avses i punkt 3 upphör, inom en rimlig tidsperiod eller omedelbart vid allvarlig överträdelse, och ska vidta ändamålsenliga och proportionella åtgärder för att säkerställa efterlevnaden. I det hänseendet ska den behöriga myndigheten för dataförmedlingstjänster, när så är lämpligt, ha befogenhet att
  - a) genom administrativa förfaranden ålägga avskräckande ekonomiska sanktioner, som får inbegripa löpande viten och sanktioner med retroaktiv verkan, inleda rättsliga förfaranden för åläggande av sanktionsavgifter, eller bådadera,
  - b) kräva att inledandet eller avbrytandet av tillhandahållandet av dataförmedlingstjänsten skjuts upp tills villkoren, enligt den behöriga myndigheten för dataförmedlingstjänsters begäran, har ändrats, eller
  - c) kräva att tillhandahållandet av dataförmedlingstjänsten upphör om allvarliga eller upprepade överträdelser inte har åtgärdats trots utfärdat meddelande enligt punkt 3.

Den behöriga myndigheten för dataförmedlingstjänster ska begära att kommissionen avlägsnar leverantören av dataförmedlingstjänster från registret över leverantörer av dataförmedlingstjänster när den har utfärdat föreläggande om att tillhandahållandet av dataförmedlingstjänsten ska upphöra i enlighet med första stycket c.

Om en leverantör av dataförmedlingstjänster åtgärdar överträdelserna, ska den leverantören av dataförmedlingstjänster på nytt anmäla detta till den behöriga myndigheten för dataförmedlingstjänster. Den behöriga myndigheten för dataförmedlingstjänster ska underrätta kommissionen om varje förnyad anmälan.

5. Om en leverantör av dataförmedlingstjänster som inte är etablerad i unionen inte utser en rättslig företrädare, eller om den rättsliga företrädaren inte på begäran av den behöriga myndigheten för dataförmedlingstjänster lämnar de nödvändiga upplysningar som på ett övergripande sätt visar efterlevnad av denna förordning, ska den behöriga myndigheten för dataförmedlingstjänster ha befogenhet att skjuta upp inledandet av eller att avbryta tillhandahållandet av dataförmedlingstjänsten tills en rättslig företrädare utses eller nödvändig information lämnas.

6. De behöriga myndigheterna för dataförmedlingstjänster ska utan dröjsmål underrätta den berörda leverantören av dataförmedlingstjänster om de åtgärder som vidtas i enlighet med punkterna 4 och 5, och de skäl som de baseras på samt de nödvändiga åtgärder som ska vidtas för att åtgärda bristerna i fråga, och ska fastställa en rimlig tidsperiod, vilken ska vara högst 30 dagar, för leverantören av dataförmedlingstjänsters uppfyllande av dessa krav.

7. Om en leverantör av dataförmedlingstjänster har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i en medlemsstat, men tillhandahåller tjänster i andra medlemsstater, ska den behöriga myndigheten för dataförmedlingstjänster i den medlemsstat där det huvudsakliga verksamhetsstället är belägen eller där den rättsliga företrädaren är lokaliserad och de behöriga myndigheterna för dataförmedlingstjänster i dessa andra medlemsstater samarbeta och bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna för dataförmedlingstjänster för utförande av deras uppgifter inom ramen för denna förordning och motiverade begäranden om att de tillsynsåtgärder som avses i denna artikel ska vidtas.

Om en behörig myndighet för dataförmedlingstjänster i en medlemsstat begär bistånd från en myndighet för dataförmedlingstjänster i annan medlemsstat ska den lämna en motiverad begäran. Den behöriga myndigheten för dataförmedlingstjänster ska, i fall av en sådan begäran, lämna ett svar utan dröjsmål och inom en tidsram som står i proportion till hur brådskande begäran är.

All information som utbyts inom ramen för assistans som begärs och tillhandahålls enligt denna punkt får användas endast med avseende på det ärende för vilket den har begärts.

#### Artikel 15

#### Undantag

Detta kapitel ska inte tillämpas på erkända dataaltruismorganisationer eller andra icke-vinstdrivande enheter i den mån som deras verksamhet består i att samla in data för ändamål av allmänt intresse som tillhandahålls av fysiska eller juridiska personer baserat på dataaltruism, såvida inte dessa organisationer och enheter syftar till att upprätta affärsförbindelser mellan, å ena sidan, ett obestämt antal registrerade och datainnehavare och, å andra sidan, dataanvändare.

#### KAPITEL IV

#### Dataaltruism

#### Artikel 16

#### Nationella arrangemang för dataaltruism

Medlemsstaterna får införa organisatoriska eller tekniska arrangemang, eller bådadera, för att underlätta dataaltruism. För det ändamålet får medlemsstaterna fastställa nationella strategier för dataaltruism. Dessa nationella strategier får framför allt bistå registrerade, när dessa frivilligt gör data som avser dem och som innehas av offentliga myndigheter tillgängliga för dataaltruism, och ange den nödvändiga information som ska tillhandahållas de registrerade om vidareutnyttjandet av deras data i allmänt intresse.

Om en medlemsstat utarbetar sådana nationella strategier ska den underrätta kommissionen om detta.

#### Artikel 17

##### Offentliga register över erkända dataaltruismorganisationer

1. Varje behörig myndighet för registrering av dataaltruismorganisationer ska föra och regelbundet uppdatera ett offentligt nationellt register över erkända dataaltruismorganisationer.

2. Kommissionen ska i informationssyfte hålla ett offentligt unionsregister över erkända dataaltruismorganisationer. Förutsatt att en enhet är registrerad i det offentliga nationella registret över erkända dataaltruismorganisationer i enlighet med artikel 18 får den använda beteckningen "dataaltruismorganisation som är erkänd i unionen" i sin skriftliga och muntliga kommunikation samt en gemensam logotyp.

För att säkerställa att erkända dataaltruismorganisationer lätt kan identifieras i hela unionen ska kommissionen genom genomförandeakter fastställa utformningen för den gemensamma logotypen. Erkända dataaltruismorganisationer ska tydligt visa den gemensamma logotypen på alla publikationer online och offline som anknuter till deras dataaltruismverksamhet. Den gemensamma logotypen ska åtföljas av en QR-kod med en länk till det offentliga unionsregistret över erkända dataaltruismorganisationer.

Dessa genomförandeakter ska antas i enlighet med det rådgivande förfarande som avses i artikel 33.2.

#### Artikel 18

##### Allmänna krav för registrering

För att kvalificera sig för registrering i ett offentligt nationellt register över erkända dataaltruismorganisationer ska en enhet

- a) utföra dataaltruismåtgärder,
- b) vara en juridisk person som bildats i enlighet med nationell rätt för att uppfylla mål av allmänt intresse, som det föreskrivs i nationell rätt i förekommande fall,
- c) bedriva verksamhet på icke-vinstdrivande grund och vara rättsligt fristående från alla enheter som bedriver verksamhet på vinstdrivande grund,
- d) utföra sina dataaltruismåtgärder via en struktur som är funktionellt fristående från dess övriga åtgärder.
- e) följa den regelbok som avses i artikel 22.1 senast 18 månader efter dagen för ikraftträdandet av de delegerade akter som avses i den punkten.

#### Artikel 19

##### Registrering av erkända dataaltruismorganisationer

1. En enhet som uppfyller kraven i artikel 18 får lämna in en ansökan om registrering i det offentliga nationella registret över erkända dataaltruismorganisationer i den medlemsstat där den är etablerad.

2. En enhet som uppfyller kraven i artikel 18 och har verksamhetsställen i fler än en medlemsstat får inlämna en ansökan om registrering i det offentliga nationella registret över erkända dataaltruismorganisationer i den medlemsstat där den har sitt huvudsakliga verksamhetsställe.

3. En enhet som uppfyller kraven i artikel 18 men som inte är etablerad i unionen ska utse en rättslig företrädare i en av de medlemsstater i vilka dataaltruismtjänsterna erbjuds.



För att säkerställa efterlevnaden av denna förordning ska enheten ge den rättsliga företrädaren uppdraget att utöver eller i stället för denna kunna kontaktas av behöriga myndigheter för registrering av dataaltruismorganisationer eller registrerade och datainnehavare i alla frågor som rör den enheten. Den rättsliga företrädaren ska samarbeta med de behöriga myndigheterna för registrering av dataaltruismorganisationer och, på begäran, för dessa på ett övergripande sätt påvisa de åtgärder som vidtagits och bestämmelser som införts av enheten för att säkerställa överensstämmelse med denna förordning.

Enheten ska anses omfattas av jurisdiktionen i den medlemsstat där den rättsliga företrädaren finns. En sådan enhet får lämna in en ansökan om registrering i det offentliga nationella registret över erkända dataaltruismorganisationer i den medlemsstaten. Att enheten utser en rättslig företrädare ska inte påverka rättsliga åtgärder som kan vidtas mot enheten.

4. De ansökningar om registrering som avses i punkterna 1, 2 och 3 ska innehålla följande uppgifter:

- a) Enhetens namn.
- b) Enhetens rättsliga status, form och, om enheten är registrerad i ett offentligt nationellt register, registreringsnummer.
- c) Enhetens stadgar, i förekommande fall.
- d) Enhetens inkomstkällor.
- e) Adressen till enhetens huvudsakliga verksamhetsställe i unionen, i förekommande fall, och, om tillämpligt, eventuella underordnade filialer i en annan medlemsstat, eller till den rättsliga företrädaren.
- f) En offentlig webbplats med fullständig och uppdaterad information om enheten och verksamheten, inbegripet åtminstone den information som avses i leden a, b, d, e och h.
- g) Enhetens kontaktpersoner och kontaktoppgifter.
- h) De mål av allmänt intresse som enheten avser att främja när den samlar in data.
- i) Den typ av data som enheten avser att kontrollera eller behandla och, när det gäller personuppgifter, en angivelse av kategorierna av personuppgifter.
- j) Alla andra handlingar som visar att kraven i artikel 18 uppfylls.

5. När enheten har lämnat all nödvändig information i enlighet med punkt 4, och efter det att den behöriga myndigheten för registrering av dataaltruismorganisationer har utvärderat ansökan om registrering och konstaterat att enheten uppfyller kraven i artikel 18, ska den registrera enheten i det offentliga nationella registret över erkända dataaltruismorganisationer inom tolv veckor efter mottagandet av ansökan om registrering. Registreringen ska gälla i alla medlemsstater.

Den behöriga myndigheten för registrering av dataaltruismorganisationer ska underrätta kommissionen om alla registreringar. Kommissionen ska föra in registreringarna i det offentliga unionsregistret över erkända dataaltruismorganisationer.

6. De uppgifter som avses i punkt 4 a, b, f, g och h ska offentliggöras i det relevanta offentliga nationella registret över erkända dataaltruismorganisationer.

7. En erkänd dataaltruismorganisation ska underrätta den relevanta behöriga myndigheten för registrering av dataaltruismorganisationer om alla ändringar av de uppgifter som tillhandahållits i enlighet med punkt 4 inom 14 dagar från dagen för ändringen.

Den behöriga myndigheten för registrering av dataaltruismorganisationer ska utan dröjsmål underrätta kommissionen om varje sådan underrättelse på elektronisk väg. På grundval av en sådan underrättelse ska kommissionen utan dröjsmål uppdatera det offentliga unionsregistret över erkända dataaltruismorganisationer.

## Artikel 20

**Transparenskrav**

1. En erkänd dataaltruismorganisation ska föra fullständiga och noggranna register över
  - a) alla fysiska eller juridiska personer som getts möjlighet att behandla data som innehas av den erkända dataaltruismorganisationen, och deras kontaktuppgifter,
  - b) datum eller varaktighet för behandlingen av personuppgifter eller användning av icke-personuppgifter,
  - c) behandlingens ändamål som det angetts av den fysiska eller juridiska person som getts möjlighet till behandling,
  - d) avgifter som betalas av fysiska eller juridiska personer som behandlar data, i förekommande fall.
2. En erkänd dataaltruismorganisation ska utarbeta och till den relevanta behöriga myndigheten för registrering av dataaltruismorganisationer sända en årlig verksamhetsrapport som ska innehålla minst följande:
  - a) Information om den erkända dataaltruismorganisationens verksamhet.
  - b) En beskrivning av hur de mål av allmänt intresse som föranledde insamlingen av data har främjats under det aktuella budgetåret.
  - c) En förteckning över alla fysiska och juridiska personer som tillåtits att behandla de data som enheten innehar, inbegripet en sammanfattande beskrivning av de mål av allmänt intresse som är tänkta att uppnås genom sådan databehandling och en beskrivning av de tekniska metoder som använts, inbegripet en beskrivning av de tekniker som använts för skyddet av personlig integritet och dataskydd.
  - d) En sammanfattning av resultaten av de databehandlingar som tillåtits av den erkända dataaltruismorganisationen, i förekommande fall.
  - e) Information om den erkända dataaltruismorganisationens inkomstkällor, i synnerhet alla intäkter från beviljandet av tillgång till data, och om utgifter.

## Artikel 21

**Särskilda krav för att skydda de registrerades och datainnehavarnas rättigheter och intressen när det gäller deras data**

1. En erkänd dataaltruismorganisation ska på ett klart och lättbegripligt sätt underrätta registrerade eller datainnehavare innan deras data behandlas
  - a) om de mål av allmänt intresse och, om tillämpligt, de särskilda, uttryckligt angivna och berättigade ändamål för vilka personuppgifter ska behandlas, och för vilka den tillåter att deras data behandlas av dataanvändare, och
  - b) om lokaliseringen och målen av allmänt intresse i fråga om vilka den tillåter behandling som utförs i ett tredjeland, om behandlingen utförs av den erkända dataaltruismorganisationen.
2. Den erkända dataaltruismorganisationen får inte använda data för några andra mål än de mål av allmänt intresse för vilka den registrerade eller datainnehavaren tillåter behandling. Den erkända dataaltruismorganisationen får inte använda vilseledande marknadsföringsmetoder i samband med förfrågan om tillhandahållande av data.
3. Den erkända dataaltruismorganisationen ska tillhandahålla verktyg för inhämtande av samtycke från registrerade eller tillstånd att behandla data som datainnehavare har gjort tillgängliga. Den erkända dataaltruismorganisationen ska också tillhandahålla verktyg för enkelt återkallande av sådant samtycke eller tillstånd.
4. Den erkända dataaltruismorganisationen ska vidta åtgärder för att säkerställa en lämplig säkerhetsnivå för lagringen och behandlingen av icke-personuppgifter som den har samlat in på grundval av dataaltruism.
5. Den erkända dataaltruismorganisationen ska utan dröjsmål informera datainnehavarna vid otillåten överföring av, tillgång till eller användning av icke-personuppgifter som den har delat.

6. Om den erkända dataaltruismorganisationen underlättar tredjeparters behandling av data, bland annat genom att tillhandahålla verktyg för att erhålla de registrerades samtycke eller erhålla tillstånd att behandla data som tillhandhålls av datainnehavare, ska den i relevanta fall, ange inom vilken tredjelandsjurisdiktion som dataanvändningen är avsedd att äga rum.

#### Artikel 22

##### Regelbok

1. Kommissionen ska anta delegerade akter i enlighet med artikel 32 med avseende på att komplettera denna förordning genom skapandet av en regelbok som fastställer
  - a) lämpliga informationskrav som säkerställer att registrerade och datainnehavare, innan ett samtycke eller tillstånd för dataaltruism ges, tillhandahålls tillräckligt utförlig, tydlig och transparent information om användningen av data, verktygen för givande och återkallande av samtycke eller tillstånd och de åtgärder som vidtagits för att undvika missbruk av de data som delas med dataaltruismorganisationen,
  - b) lämpliga tekniska och säkerhetsmässiga krav för att säkerställa en lämplig nivå av säkerhet för lagringen och behandlingen av data samt för verktygen för givande och återkallande av samtycke eller tillstånd,
  - c) kommunikationsfärdplaner med multidisciplinär ansats för att öka medvetenheten om dataaltruism, om erhållen status som "dataaltruismorganisation som är erkänd i unionen" och om regelboken bland berörda parter, särskilt datainnehavare och registrerade som kan tänka sig att dela med sig av sina data,
  - d) rekommendationer om relevanta interoperabilitetsstandarder.
2. Den regelbok som avses i punkt 1 ska utarbetas i nära samarbete med dataaltruismorganisationer och berörda parter.

#### Artikel 23

##### Behöriga myndigheter för registrering av dataaltruismorganisationer

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter som ansvarar för dess offentliga nationella register av erkända dataaltruismorganisationer.

De behöriga myndigheterna för registrering av dataaltruismorganisationer ska uppfylla de krav som anges i artikel 26.

2. Varje medlemsstat ska underrätta kommissionen om identiteten på sina behöriga myndigheter för registrering av dataaltruismorganisationers identitet senast den 24 september 2023. Varje medlemsstat ska även underrätta kommissionen om alla eventuella senare ändringar av dessa behöriga myndigheters identitet

3. Den behöriga myndigheten för registrering av dataaltruismorganisationer i en medlemsstat ska utföra sina uppgifter i samarbete med den relevanta dataskyddsmyndigheten, när dessa uppgifter rör behandlingen av personuppgifter, och med relevanta sektorsmyndigheterna i den medlemsstaten.

#### Artikel 24

##### Övervakning av efterlevnaden

1. De behöriga myndigheterna för registrering av dataaltruismorganisationer ska övervaka och utöva tillsyn över att erkända dataaltruismorganisationer uppfyller de krav som fastställs i detta kapitel. Den behöriga myndigheten för registrering av dataaltruismorganisationer får även övervaka och utöva tillsyn över sådana erkända dataaltruismorganisationers efterlevnad på grundval av en begäran från en fysisk eller juridisk person.

2. De behöriga myndigheterna för registrering av dataaltruismorganisationer ska ha befogenhet att från erkända dataaltruismorganisationer begära sådan information som är nödvändig för att kontrollera att kraven i detta kapitel följs. Varje begäran om information ska stå i proportion till uppgiftens utförande och innehålla en motivering.

3. I de fall då den behöriga myndigheten för registrering av dataaltruismorganisationer finner att en erkänd dataaltruismorganisation inte uppfyller ett eller flera av kraven i detta kapitel ska den meddela den erkända dataaltruismorganisationen dessa iakttagelser och ge den möjlighet att yttra sig, inom 30 dagar efter mottagandet av meddelandet.

4. Den behöriga myndigheten för registrering av dataaltruismorganisationer ska ha befogenhet att kräva att den överträdelse som avses i punkt 3 upphör, antingen omedelbart eller inom en rimlig tidsperiod, och ska vidta ändamålsenliga och proportionella åtgärder för att säkerställa efterlevnaden.

5. Om en erkänd dataaltruismorganisation inte uppfyller ett eller flera krav i detta kapitel ens efter att den i enlighet med punkt 3 har underrättats av den behöriga myndigheten för registrering av dataaltruismorganisationer, ska den erkända dataaltruismorganisationen

- a) förlora sin rätt att använda beteckningen "dataaltruismorganisation som är erkänd i unionen" i sin skriftliga och muntliga kommunikation,
- b) avlägsnas från det relevanta offentliga nationella registret över erkända dataaltruismorganisationer och det offentliga unionsregistret över erkända dataaltruismorganisationer.

Ett beslut om att återkalla rätten att använda beteckningen "dataaltruismorganisation om är erkänd i unionen" enligt första stycket led a ska offentliggöras av den behöriga myndigheten för registrering av dataaltruismorganisationer.

6. Om en enhet som registreras i det offentliga nationella registret över erkända dataaltruismorganisationer har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i en medlemsstat, men är aktiv i andra medlemsstater, ska den behöriga myndigheten för registrering av dataaltruismorganisationer i den medlemsstat där det huvudsakliga verksamhetsstället är beläget eller där den rättsliga företrädaren är lokaliserad och de behöriga myndigheterna för registrering av dataaltruismorganisationer i dessa andra medlemsstater samarbeta och bistå varandra. Detta bistånd och samarbete får omfatta informationsutbyte mellan de berörda behöriga myndigheterna för registrering av dataaltruismorganisationer för utförande av deras uppgifter inom ramen för denna förordning och motiverade begäranden om att de åtgärder som avses denna artikel ska vidtas.

Om en behörig myndighet för registrering av dataaltruismorganisationer i en medlemsstat begär bistånd från en behörig myndighet för registrering av dataaltruismorganisationer i en annan medlemsstat ska den lämna en motiverad begäran. Den behöriga myndigheten för registrering av dataaltruismorganisationer ska i fall av en sådan begäran svara på denna utan dröjsmål och inom en tidsram som står i proportion till hur brådskande begäran är.

All information som utbyts inom ramen för assistans som begärs och tillhandahålls enligt denna punkt får användas endast med avseende på det ärende för vilket den har begärts.

#### Artikel 25

#### Europeiskt formulär för samtycke till dataaltruism

1. För att främja insamling av data baserat på dataaltruism ska kommissionen anta genomförandeakter om upprättande och utarbetande av ett europeiskt formulär för samtycke till dataaltruism, efter samråd med Europeiska dataskyddsstyrelsen och med beaktande av rådgivning från Europeiska datainnovationsstyrelsen samt med vederbörligt deltagande av berörda parter. Detta formulär ska göra det möjligt att erhålla samtycke eller tillstånd i alla medlemsstater och i ett enhetligt format. Dessa genomförandeakter ska antas i enlighet med det rådgivande förfarande som avses i artikel 33.2.

2. Det europeiska formuläret för samtycke till dataaltruism ska baseras på moduler, så att det kan anpassas till enskilda sektorer och olika syften.

3. När personuppgifter tillhandahålls ska det europeiska formuläret för samtycke till dataaltruism säkerställa att de registrerade kan ge och dra tillbaka sitt samtycke till en specifik databehandlingsoperation i enlighet med kraven i förordning (EU) 2016/679.

4. Formuläret ska tillhandahållas på ett sådant sätt att det kan tryckas på papper, är lättförståeligt och även finns i elektronisk, maskinläsbar form.

## KAPITEL V

**Behöriga myndigheter och förfarandebestämmelser**

## Artikel 26

**Krav på behöriga myndigheter**

1. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer ska vara juridiskt åtskilda från, och funktionellt oberoende av, alla leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer. Funktionerna för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer får utföras av samma myndighet. Medlemsstaterna får antingen inrätta en eller flera nya myndigheter eller förlita sig på befintliga myndigheter.
2. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer ska utföra sina uppgifter på ett opartiskt, transparent, konsekvent och tillförlitligt sätt och utan dröjsmål. När de utför sina uppgifter ska de skydda rättvis konkurrens och icke-diskriminering.
3. De ledande befattningshavarna och personalen som ansvarar för att utföra de berörda uppgifterna hos de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer får inte vara personer som utformar, tillverkar, tillhandahåller, installerar, köper in, äger, använder eller underhåller de tjänster som de bedömer, och inte heller vara auktoriserade företrädare eller ombud för någon av dessa parter. Detta ska dock inte hindra en användning av bedömda tjänster som är nödvändig för verksamheten vid de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer eller en användning av sådana tjänster för personliga ändamål.
4. De ledande befattningshavarna och personalen vid de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer får inte delta i någon verksamhet som kan påverka deras objektivitet och integritet i samband med de bedömningar av verksamhet som de anförtrots att göra.
5. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer ska ha tillräckliga ekonomiska resurser och personalresurser till sitt förfogande för att utföra de uppgifter som de anförtrots, inbegripet de nödvändiga tekniska kunskaperna och resurserna.
6. De behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer i en medlemsstat ska, på motiverad begäran och utan dröjsmål, förse kommissionen och de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer från andra medlemsstater med den information som dessa behöver för att utföra sina uppgifter enligt denna förordning. Om en behörig myndighet för dataförmedlingstjänster eller en behörig myndighet för registrering av dataaltruismorganisationer anser att den begärda informationen är konfidentiell i enlighet med unionsrätten och nationell rätt om affärshemligheter och tystnadsplikt, ska kommissionen och andra berörda behöriga myndigheter för dataförmedlingstjänster eller behöriga myndigheter för registrering av dataaltruismorganisationer säkerställa sådan konfidentiell behandling.

## Artikel 27

**Rätt att lämna in klagomål**

1. Fysiska och juridiska personer ska, avseende frågor som omfattas av tillämpningsområdet för denna förordning, ha rätt att inkomma med klagomål, individuellt eller i relevanta fall kollektivt, till den berörda behöriga myndigheten för dataförmedlingstjänster mot en leverantör av dataförmedlingstjänster eller till den behöriga myndigheten för registrering av dataaltruismorganisationer mot en erkänd dataaltruismorganisation.

2. Den behöriga myndigheten för dataförmedlingstjänster eller den behöriga myndigheten för registrering av dataaltruismorganisationer till vilket klagomålet har lämnats in ska underrätta den klagande om

- a) hur förfarandet fortskrider och vilket beslut som fattats, och
- b) rättsmedel enligt artikel 28.

#### Artikel 28

### Rätten till ett effektivt rättsmedel

1. Utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol, ska berörda fysiska och juridiska personer ha rätt till effektiva rättsmedel avseende rättsligt bindande beslut som avses i artikel 14 och som fattats av de behöriga myndigheterna för dataförmedlingstjänster i samband med hantering, övervakning och kontroll av efterlevnaden av anmälningsordningen för leverantörer av dataförmedlingstjänster och rättsligt bindande beslut som avses i artiklarna 19 och 24 som fattats av de behöriga myndigheterna för registrering av dataaltruismorganisationer i samband med övervakningen av erkända dataaltruismorganisationer.

2. Förfaranden enligt denna artikel ska inledas vid domstolarna i den medlemsstat där den behöriga myndigheten för dataförmedlingstjänster eller den behöriga myndigheten för registrering av dataaltruismorganisationer som rättsmedlen avser är belägen, antingen individuellt eller, i förekommande fall kollektivt, av företrädare för en eller flera fysiska eller juridiska personer.

3. Om en behörig myndighet för dataförmedlingstjänster eller en behörig myndighet för registrering av dataaltruismorganisationer underlåter att vidta åtgärder med avseende på ett klagomål ska berörda fysiska och juridiska personer, i enlighet med nationell rätt, antingen ha rätt till ett effektivt rättsmedel eller tillgång till omprövning av en opartisk myndighet som besitter lämplig sakkunskap.

#### KAPITEL VI

### Europeiska datainnovationsstyrelsen

#### Artikel 29

### Europeiska datainnovationsstyrelsen

1. Kommissionen ska inrätta en europeisk datainnovationsstyrelse i form av en expertgrupp som består av företrädare för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer i alla medlemsstater, Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, Enisa, kommissionen, EU-företrädaren för små och medelstora företag eller en företrädare utsedd av nätverket av företrädare för små och medelstora företag och andra företrädare för relevanta organ inom enskilda sektorer samt organ med specifik sakkunskap. I sin utnämning av enskilda experter ska kommissionen sträva efter att uppnå jämn könsfördelning och geografisk balans bland medlemmarna av expertgruppen.

2. Europeiska datainnovationsstyrelsen ska bestå av minst följande tre undergrupper:

- a) en undergrupp bestående av de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registrering av dataaltruismorganisationer, som är avsedd att utföra uppgifterna enligt artikel 30 a, c, j och k,
- b) en undergrupp för tekniska diskussioner om standardisering, portabilitet och interoperabilitet i enlighet med artikel 30 f och g,

- c) en undergrupp för deltagande av berörda parter bestående av relevanta företrädare från näringslivet, forskningsvärlden, den akademiska världen, civilsamhället, standardiseringsorganisationer, berörda gemensamma europeiska dataområden och andra berörda intressenter och tredje parter som ger råd till Europeiska datainnovationsstyrelsen om uppgifter i enlighet med artikel 30 d, e, f, g och h.
3. Kommissionen ska vara ordförande vid Europeiska datainnovationsstyrelsens sammanträden.
4. Europeiska datainnovationsstyrelsen ska bistås av ett sekretariat som tillhandahålls av kommissionen.

#### Artikel 30

#### Europeiska datainnovationsstyrelsens uppgifter

Europeiska datainnovationsstyrelsen ska ha följande uppgifter:

- a) Att rådge och bistå kommissionen när det gäller utarbetandet av en konsekvent praxis för offentliga myndigheter och behöriga organ enligt 7.1 vid behandlingen av ansökningar om vidareutnyttjande av de kategorier av data som avses i artikel 3.1.
- b) Att rådge och bistå kommissionen när det gäller utvecklingen av en enhetlig praxis för dataatruism i hela unionen.
- c) Att rådge och bistå kommissionen när det gäller utarbetandet av en konsekvent praxis för de behöriga myndigheterna för dataförmedlingstjänster och de behöriga myndigheterna för registreringen av dataatruismorganisationer vad gäller tillämpningen av krav för leverantörer av dataförmedlingstjänster och erkända dataatruismorganisationer.
- d) Att rådge och bistå kommissionen när det gäller utarbetandet av konsekventa riktlinjer för hur man inom ramen för denna förordning bäst ska skydda kommersiellt känsliga data som inte är personuppgifter, särskilt företagshemligheter, men även icke-personuppgifter med immaterialrättsligt skyddat innehåll, mot olaglig åtkomst med risker för stöld av immateriella rättigheter eller industrispionage.
- e) Att rådge och bistå kommissionen när det gäller utarbetandet av konsekventa riktlinjer för cybersäkerhetskrav vid utbyte och lagring av data.
- f) Att rådge kommissionen, särskilt med hänsyn till bidrag från standardiseringsorganisationer, om prioriteringsordningen för sektorsövergripande standarder som ska användas och utvecklas för dataanvändning och sektorsövergripande datadelning mellan framväxande gemensamma europeiska dataområden, sektorsövergripande jämförelse och utbyte av bästa praxis när det gäller sektorskrav avseende säkerhet samt förfaranden för tillgång, med beaktande av sektorsspecifik standardiseringsverksamhet, framför allt för att klarlägga och särskilja vilka standarder och praxisformer som är sektorsövergripande och vilka som är sektorsspecifika.
- g) Att bistå kommissionen, särskilt med hänsyn till bidrag från standardiseringsorganisationer, med att ta itu med fragmenteringen av den inre marknaden och av dataekonomin på den inre marknaden genom att förbättra den gränsövergripande, sektorsövergripande interoperabiliteten för data och datadelningstjänster mellan olika sektorer och områden, baserat på befintliga europeiska, internationella eller nationella standarder, bland annat med syftet att uppmuntra inrättandet av gemensamma europeiska dataområden.
- h) Att föreslå riktlinjer för gemensamma europeiska dataområden, nämligen ändamåls- eller sektorsspecifika eller sektorövergripande interoperabla ramar med allmänna standarder och praxisformer för delning eller gemensam behandling av data bl.a. för utveckling av nya produkter och tjänster, vetenskaplig forskning eller civilsamhällsinitiativ, sådana allmänna standarder och praxisformer tar hänsyn till befintliga standarder, följer konkurrensreglerna och säkerställer icke-diskriminerande tillgång för alla deltagare, för att underlätta datadelning i unionen och utnyttja potentialen i befintliga och framtida dataområden, som bland annat tar upp
- i) sektorsövergripande standarder som ska användas och utvecklas för dataanvändning och sektorsövergripande datadelning, sektorsövergripande jämförelse och utbyte av bästa praxis när det gäller sektorskrav avseende säkerhet samt förfaranden för tillgång, med beaktande av sektorsspecifik standardiseringsverksamhet, framför allt för att klarlägga och särskilja vilka standarder och praxisformer som är sektorsövergripande och vilka som är sektorsspecifika,
- ii) krav för att motverka hinder för marknadstillträde och för att undvika inläsningseffekter, i syfte att säkerställa rättvis konkurrens och interoperabilitet,

- iii) tillräckligt skydd för lagliga dataöverföringar till tredjeländer, däribland skyddsåtgärder mot överföringar som är förbjudna enligt unionsrätten,
  - iv) tillräcklig och icke-diskriminerande representation av berörda parter i förvaltningen av gemensamma europeiska dataområden,
  - v) efterlevnad av cybersäkerhetskrav i enlighet med unionsrätten.
- i) Att underlätta samarbetet mellan medlemsstaterna om fastställandet av harmoniserade villkor som möjliggör vidareutnyttjande av de kategorier av data som avses i artikel 3.1 och som innehas av offentliga myndigheter överallt på den inre marknaden.
  - j) Att underlätta samarbetet mellan behöriga myndigheter för dataförmedlingstjänster och behöriga myndigheter för registrering av dataaltruismorganisationer, genom kapacitetsuppbyggnad och informationsutbyte, i synnerhet genom att fastställa metoder för ett effektivt utbyte av information som rör förfarandet för anmälan av leverantörer av dataförmedlingstjänster och registreringen och övervakningen av erkända dataaltruismorganisationer, inbegripet samordning avseende fastställande av avgifter eller sanktioner, samt underlätta samarbetet mellan behöriga myndigheter för dataförmedlingstjänster och behöriga myndigheter för registrering av dataaltruismorganisationer avseende internationell tillgång till och överföring av data.
  - k) Att rådge och bistå kommissionen när det gäller utvärderingen av huruvida de genomförandeakter som avses i artikel 5.11 och 5.12 ska antas.
  - l) Att rådge och bistå kommissionen när det gäller utarbetande av det europeiska formuläret för samtycke till dataaltruism i enlighet med artikel 25.1.
  - m) Att rådge kommissionen om förbättring av det internationella regelverket för icke-personuppgifter, inbegripet standardisering.

#### KAPITEL VII

#### *internationell tillgång och överföring*

#### Artikel 31

#### **Internationell tillgång och överföring**

1. Den offentliga myndighet, den fysiska eller juridiska person som beviljats rätt att vidareutnyttja data i enlighet med kapitel II, leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen ska vidta alla rimliga tekniska, rättsliga och organisatoriska åtgärder, inbegripet kontraktsmässiga arrangemang, för att förhindra internationell överföring av eller statlig tillgång till icke-personuppgifter som innehas i unionen, om en sådan överföring eller tillgång skulle strida mot unionsrätten eller den nationella rätten i den berörda medlemsstaten, utan att detta påverkar punkt 2 eller 3.
2. Beslut eller domar från en domstol i ett tredje land och beslut från förvaltningsmyndigheter i ett tredjeland där det krävs att en offentlig myndighet, en fysisk eller juridisk person som beviljas rätten att vidareutnyttja data i enlighet med kapitel II, en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation överför icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning från unionen eller ger tillgång till sådana icke-personuppgifter som innehas i unionen får endast erkännas eller genomföras på något som helst sätt om det grundar sig på en internationell överenskommelse, såsom ett fördrag om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen, eller ett sådant avtal mellan det begärande tredjelandet och en medlemsstat.
3. I de fall då, i avsaknad av en internationell överenskommelse som avses i punkt 2 i denna artikel, en offentlig myndighet, en fysisk eller juridisk person som i enlighet med kapitel II beviljats rättigheten att vidareutnyttja data, en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation är adressat för ett beslut eller en dom från en domstol i ett tredje land eller ett beslut från en förvaltningsmyndighet i ett tredjeland om att överföra icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning från unionen eller ge tillgång till sådana icke-personuppgifter som innehas i unionen, och efterlevnaden av ett sådant beslut skulle riskera att medföra att adressaten bryter mot unionsrätten eller den nationella rätten i den berörda medlemsstaten, ska tredjelandsmyndighetens överföring av eller tillgång till sådana data endast äga rum om:
  - a) tredjelandets system kräver att skälen till och proportionaliteten hos sådana beslut eller domar ska fastställas, och föreskriver att sådana beslut eller domar är av specifik art, exempelvis genom att det fastställs en tillräckligt stark koppling till vissa misstänkta personer eller till överträdelse,



- b) adressatens motiverade invändning är föremål för en granskning av en behörig domstol i tredjelandet, och
- c) den behöriga domstol i tredjelandet som utfärdar beslutet eller domen eller granskar en förvaltningsmyndighets beslut enligt det tredjelandets rätt har befogenhet att ta vederbörlig hänsyn till de relevanta rättsliga intressena för leverantören av de data som skyddas av unionsrätten eller den nationella rätten i den berörda medlemsstaten.
4. Om de villkor som fastställs i punkterna 2 och 3 är uppfyllda ska den offentliga myndigheten, den fysiska eller juridiska person som beviljats rätt att vidareutnyttja data i enlighet med kapitel II, leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen tillhandahålla den minimimängd data som är tillåten till följd av en begäran, baserat på en rimlig tolkning av denna begäran.
5. Den offentliga myndigheten, den fysiska eller juridiska person som i enlighet med kapitel II beviljats rättigheten att vidareutnyttja data, leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen ska underrätta datainnehavaren om förekomsten av en begäran från en förvaltningsmyndighet i ett tredjeland om att få tillgång till dess data, innan den tillmötesgår den begäran, förutom då denna begäran avser brottsbekämpande ändamål och så länge som detta är nödvändigt för att skydda brottsbekämpningens effektivitet.

#### KAPITEL VIII

#### **Delegering och kommittéförfarande**

##### Artikel 32

#### **Utövande av delegeringen**

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Den befogenhet att anta delegerade akter som avses i artiklarna 5.13 och 22.1 ges till kommissionen tills vidare från och med den 23 juni 2022.
3. Den delegering av befogenhet som avses i artiklarna 5.13 och 22.1 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artikel 5.13 eller 22.1 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

##### Artikel 33

#### **Kommittéförfarande**

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 4 i förordning (EU) nr 182/2011 tillämpas.
3. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

#### KAPITEL IX

#### Slut- och övergångsbestämmelser

#### Artikel 34

#### Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av skyldigheterna om överföring av icke-personuppgifter till tredjeländer enligt artiklarna 5.14 och 31, anmälningsskyldigheten för leverantörer av dataförmedlingstjänster enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 och villkoren för registrering som erkänd dataaltruismorganisation enligt artiklarna 18, 20, 21 och 22 och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska i sina regler om sanktioner ta hänsyn till Europeiska datainnovationsstyrelsens rekommendationer. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 24 september 2023 samt utan dröjsmål eventuella ändringar som berör dem.
2. Medlemsstaterna ska i lämpliga fall beakta följande icke-uttömmande och vägledande kriterier för utdömmande av sanktioner för leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer vid överträdelser av denna förordning:
  - a) Överträdelsens art, allvar, omfattning och varaktighet.
  - b) Eventuella åtgärder som leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen vidtagit för att begränsa eller avhjälpa den skada som överträdelsen har orsakat.
  - c) Eventuella tidigare överträdelser som leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen har gjort sig skyldig till.
  - d) De ekonomiska vinster som leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen gjort eller de förluster som de undvikit till följd av överträdelsen, i den mån sådana vinster eller förluster på ett tillförlitligt sätt kan fastställas.
  - e) Eventuella andra försvårande eller förmildrande omständigheter som är tillämpliga på ärendet.

#### Artikel 35

#### Utvärdering och översyn

Kommissionen ska senast den 24 september 2025 genomföra en utvärdering av denna förordning och lämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. Rapporten ska vid behov åtföljas av lagstiftningsförslag.

I rapporten ska särskilt följande bedömas:

- a) Tillämpningen av och funktionssättet för de regler om sanktioner som medlemsstaterna fastställt i enlighet med artikel 34.
- b) I vilken utsträckning de rättsliga företrädarna för leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer som inte är etablerade i unionen efterlever denna förordning, och i vilken utsträckning de sanktioner som åläggs är verkställbara på dessa leverantörer och organisationer.
- c) Vilken typ av dataaltruismorganisationer som registrerats i enlighet med kapitel IV, samt en översikt av för vilka mål av allmänt intresse datadelning förekommer, för att tydliga kriterier för detta ska kunna fastställas.

Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta den rapporten.

Artikel 36

**Ändring av förordning (EU) 2018/1724**

I tabellen i bilaga II till förordning (EU) 2018/1724 ska posten "Starta företag och bedriva affärsverksamhet" ersättas med följande:

Livshändelser	Förfaranden	Förväntat resultat med förbehåll för den behöriga myndighetens bedömning av ansökan i enlighet med nationell rätt, där så är relevant
Starta företag och bedriva affärsverksamhet	Anmälan av affärsverksamhet, tillstånd för affärsverksamhet, ändring av affärsverksamhet och avslutande av affärsverksamhet utan insolvens- eller likvidationsförfaranden, undantaget inledande registrering av affärsverksamhet i företagsregistret och undantaget förfaranden för bildande eller senare anmälan av bolag i den mening som avses i artikel 54 andra stycket i EUF-fördraget	Bekräftelse på mottagande av anmälan eller ändring av – eller av ansökan om tillstånd för – affärsverksamhet
	Registrera en arbetsgivare (en fysisk person) i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Registrera anställda i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Lämna in en bolagsskattedeklaration	Bekräftelse på mottagande av deklarationen
	Meddela socialförsäkringssystemet när en anställds kontrakt avslutas, dock ej förfaranden för kollektivt avslutande av anställningskontrakt	Bekräftelse på mottagande av meddelandet
	Betala sociala avgifter för anställda	Kvitto eller annan form av bekräftelse på betalningen av sociala avgifter för anställda
	Anmälan som leverantör av dataförmedlingstjänster	Bekräftelse på mottagande av anmälan
	Registrering som dataaltruismorganisation som är erkänd i unionen	Bekräftelse av registreringen

Artikel 37

**Övergångsbestämmelser**

Enheter som tillhandahåller de dataförmedlingstjänster som avses i artikel 10 den 23 juni 2022 ska fullgöra de skyldigheter som fastställs i kapitel III senast den 24 september 2025.

Artikel 38

**Ikraftträdande och tillämpning**

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 24 september 2023.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 30 maj 2022.

På Europaparlamentets vägnar  
R. METSOLA  
Ordförande

På rådets vägnar  
B. LE MAIRE  
Ordförande

---

# Sammanfattning av promemorian

## Genomförande av EU:s dataförvaltningsförordning (Ds 2023:24)

I promemorian lämnas förslag till genomförande av och komplettering till förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltningsförordning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan dataförvaltningsförordningen. Bestämmelserna i EU-förordningen ska börja tillämpas den 24 september 2023.

Dataförvaltningsförordningen omfattar villkor för vidareutnyttjande av vissa typer av skyddade data från offentliga myndigheter, en ram för anmälan av och tillsyn över tillhandahållande av dataförmedlingstjänster, ett ramverk för frivillig registrering av och tillsyn över dataaltruismorganisationer samt inrättande av en europeisk datainnovationsstyrelse.

Det föreslås att förordningen genomförs genom en ny lag samt genom tillägg till lagen om offentliga sektorns tillgängliggörande av data för vidareutnyttjande.

Enligt dataförvaltningsförordningen ska en eller flera myndigheter utses till behöriga organ. Dessa ska bistå andra myndigheter som ska bevilja eller vägra tillgång till vissa kategorier av skyddade data för vidareutnyttjande. Myndigheten för digital förvaltning och Statistiska centralbyrån föreslås bli behöriga organ. Myndigheten för digital förvaltning ska vara huvudansvarig för uppgiften och också ha till uppgift att främja tillgängliggörande av skyddade data.

En gemensam informationspunkt ska inrättas enligt dataförvaltningsförordningen. Myndigheten för digital förvaltning föreslås tillhandahålla den gemensamma informationspunkten.

I dataförvaltningsförordningen finns det ramverk för leverantörer av dataförmedlingstjänster och för dataaltruismorganisationer. Post- och telestyrelsen föreslås bli s.k. behörig myndighet för dessa. Uppgiften innebär att myndigheten ska ta emot anmälningar och ansökningar från dessa aktörer samt utöva tillsyn över dem.

Medlemsstaterna ska införa sanktioner för överträdelse av vissa artiklar i dataförvaltningsförordningen. Post- och telestyrelsen ska kunna besluta om en erinran mot leverantörer av dataförmedlingstjänster och dataaltruismorganisationer. Sanktionsavgift ska kunna beslutas för vissa överträdelse som leverantörer av dataförmedlingstjänster begår. Sanktionsavgift ska också kunna beslutas för överträdelse som vidareutnyttjare gör sig skyldiga till vid vissa tredjelandsöverföringar. Myndigheter som tillgängliggör vissa kategorier av skyddade data för vidareutnyttjande ska anmäla till tillsynsmyndigheten för dataförmedlingstjänster om de får kännedom om sådana överträdelse som kan leda till en sanktionsavgift.

Lagförslagen ska träda i kraft den 1 januari 2024.

## Promemorians lagförslag

### Förslag till lag med kompletterande bestämmelser till EU:s dataförvaltningsförordning

Härigenom föreskrivs följande.

#### **Inledande bestämmelse**

**1 §** Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan EU:s dataförvaltningsförordning.

Ord och uttryck i lagen har samma betydelse som i EU:s dataförvaltningsförordning.

#### **Tillsynsmyndighet**

**2 §** Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet enligt denna lag. Den myndighet som är tillsynsmyndighet enligt denna lag är behörig myndighet för dataförmedlingstjänster enligt artikel 13 EU:s dataförvaltningsförordning och behörig myndighet för registrering av dataaltruismorganisationer enligt artikel 23 EU:s dataförvaltningsförordning.

#### **Informationsutbyte**

**3 §** De myndigheter regeringen bestämmer ska på begäran lämna tillsynsmyndigheten de uppgifter som den behöver för att kunna utföra sitt tillsynsuppdrag enligt EU:s dataförvaltningsförordning.

Tillsynsmyndigheten ska på begäran lämna de uppgifter som andra myndigheter som regeringen bestämmer behöver för att kunna utföra tillsynsuppdrag enligt annan författning.

#### **Erinran**

**4 §** Tillsynsmyndigheten får meddela en erinran till en leverantör av dataförmedlingstjänster som bryter mot anmälningsskyldigheten enligt artikel 11, villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12 eller villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Tillsynsmyndigheten får meddela en erinran till en erkänd dataaltruismorganisation som bryter mot villkoren för registrering som erkänd dataaltruismorganisation i artiklarna 18, 20, 21 och 22 eller villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

**5 §** Tillsynsmyndigheten får förena förelägganden enligt artikel 14 EU:s dataförvaltningsförordning med vite.

### **Sanktionsavgift**

**6 §** Tillsynsmyndigheten får ta ut en sanktionsavgift av en leverantör av en dataförmedlingstjänst vid överträdelser av

- anmälningsskyldigheten för leverantören av dataförmedlingstjänster enligt artikel 11,
- villkoren för tillhandahållande av dataförmedlingstjänster enligt artikel 12, eller
- villkoren för överföring av andra uppgifter än personuppgifter till tredjeland enligt artikel 31 EU:s dataförvaltningsförordning.

Tillsynsmyndigheten får ta ut en sanktionsavgift av en vidareutnyttjare för överträdelser av artikel 5.14 i EU:s dataförvaltningsförordning.

**7 §** En sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

När avgiftens storlek bestäms ska särskild hänsyn tas till

3. överträdelsens art, allvar, omfattning och varaktighet,
4. eventuella åtgärder som leverantören av dataförmedlingstjänster eller vidareutnyttjaren vidtagit för att begränsa eller avhjälpa den skada som överträdelserna har orsakat,
5. tidigare överträdelser som leverantören av dataförmedlingstjänster eller vidareutnyttjaren har gjort sig skyldig till,
6. de ekonomiska vinster som leverantören av dataförmedlingstjänster eller vidareutnyttjaren gjort eller de förluster som de undvikit till följd av överträdelserna, och
7. andra försvårande eller förmildrande omständigheter.

Tillsynsmyndigheten får avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelserna är ringa eller ursäktliga eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

**8 §** En sanktionsavgift får inte beslutas om överträdelserna omfattas av ett föreläggande som har förenats med vite och överträdelserna ligger till grund för en ansökan om utdömmande av vitet.

**9 §** En sanktionsavgift får inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom två år från den dag då överträdelserna ägde rum.

Ett beslut om sanktionsavgift ska delges.

**10 §** En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften fick laga kraft eller inom den längre tid som anges i beslutet.

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.

En sanktionsavgift tillfaller staten.

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

### **Avgifter**

**12 §** Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om skyldighet för leverantörer av dataförmedlingstjänster som omfattas av anmälningsskyldighet enligt artikel 11 EU:s dataförvaltningsförordning att betala avgift för tillsynsmyndighetens verksamhet enligt EU:s dataförvaltningsförordning och denna lag

### **Överklagande**

**13 §** Tillsynsmyndighetens beslut enligt artikel 14, 19 och 24 EU:s dataförvaltningsförordning eller enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

Denna lag träder i kraft den 1 januari 2024.



# Förslag till lag om ändring i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data

Bilaga 3

Härigenom föreskrivs i fråga om lag (2022:818) om den offentliga sektorns tillgängliggörande av data

*dels* att 1 kap. 2, 3, 4, 8 och 10 §§, 4 kap. 1 § samt 5 kap. 1 § ska ha följande lydelse,

*dels* att det ska införas sex nya paragrafer, 1 kap. 1 a § och 7 a §, 2 kap. 5 a och 6 a §§, 3 kap. 1 a § och 4 kap. 2 a §, och närmast före 2 kap. 6 a § en ny rubrik av följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

## 1 kap.

### 1 a §

*Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten), nedan EU:s dataförvaltningsförordning.*

### 2 §

Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data eller som begränsar en sådan rätt.

Denna lag påverkar inte tillämpningen av bestämmelser i någon annan lag eller förordning som ger någon rätt att få tillgång till data *eller skyddade data* eller som begränsar en sådan rätt.

### 3 §

Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data än i denna lag, ska de kraven tillämpas.

Om det i någon annan lag eller i en förordning finns mer långtgående krav i fråga om tillgängliggörande av data *eller skyddade data* än i denna lag, ska de kraven tillämpas.

### 4 §

I lagen avses med

*begäran om tillgängliggörande av data för vidareutnyttjande*: en begäran om att data ska göras tillgängliga för vidareutnyttjande i enlighet med denna lag,

*begäran om tillgängliggörande av data för vidareutnyttjande*: en begäran om att data *eller skyddade data* ska göras tillgängliga för vidareutnyttjande i enlighet med

*bulknedladdning*: nedladdning av en avgränsad datamängd,

*data*: information i digitalt format oberoende av medium,

*dynamiska data*: data som uppdateras ofta eller i realtid för att vara aktuella och relevanta att vidareutnyttja,

*forskningsdata*: data som till någon del är offentligt finansierade, som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet och som görs direkt tillgängliga för vidareutnyttjande genom en dataplattform som är allmänt åtkomlig,

*gränssnitt*: en regeluppsättning för dynamiskt datautbyte mellan programvaror,

*maskinläsbart format*: ett filformat som är strukturerat på ett sådant sätt att det enkelt kan läsas av ett datorprogram,

*offentligt företag*: ett företag som en eller flera myndigheter har ett bestämmande inflytande över och som är verksamt

- inom de sektorer som framgår av 2 kap. 1 § och 5–8 §§ lagen (2016:1146) om upphandling inom försörjningssektorerna,

- som ett kollektivtrafikföretag enligt Europaparlamentets och rådets förordning (EG) nr 1370/2007 av den 23 oktober 2007 om kollektivtrafik på järnväg och väg och om upphävande av rådets förordning (EEG) nr 1191/69 och (EEG) nr 1107/70,

- som ett lufttrafikföretag som har allmän trafikplikt enligt artikel 16 i Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen, eller

- som ett rederi inom gemenskapen som uppfyller förpliktelser vid allmän trafik enligt artikel 4 i rådets förordning (EEG) nr 3577/92 av den 7 december 1992 om tillämpning av principen om frihet att tillhandahålla tjänster på sjötransportområdet inom medlemsstaterna (cabotage),

*offentligt styrt organ*: ett sådant organ som avses i 1 kap. 18 § lagen (2016:1145) om offentlig upphandling eller en sammanslutning av sådana organ,

*skyddade data*: sådana kategorier av skyddade data som avses i artikel 3.1 EU:s dataförvaltningsförordning.

*vidareutnyttjande*: bearbetning av data från den offentliga sektorn för valfritt ändamål,

*värdefull datamängd*: data som förtecknas i en genomförandeakt som har meddelats med stöd av artikel 14.1 i öppna data-direktivet,

*öppna data-direktivet*: Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

## 7 a §

*Bestämmelserna om vidareutnyttjande av skyddade data ska endast tillämpas av myndigheter, dock inte av kulturinstitutioner och utbildningsinstitutioner.*

## 8 §

Lagen ska tillämpas

1. när någon som har rätt att få tillgång till data enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,

2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, *eller*

3. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.

Trots första stycket ska lagen inte tillämpas

1. när data, i andra fall än som avses i första stycket 3, lämnas

a) mellan statliga och kommunala myndigheter,

b) från ett organ som enligt 1 kap. 5 § andra stycket jämställs med en myndighet eller ett offentligt företag till en statlig eller kommunal myndighet, *eller*

2. när en statlig eller kommunal myndighet tillhandahåller data i en konkurrensutsatt verksamhet.

1. när någon som har rätt att få tillgång till data *eller skyddade data* enligt någon annan lag eller förordning framställer en begäran om tillgängliggörande av data för vidareutnyttjande,

2. när en myndighet eller ett offentligt företag på eget initiativ tillgängliggör data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas,

3. när en myndighet på eget initiativ tillgängliggör *skyddade data som omfattas av lagen i syfte att de ska kunna vidareutnyttjas, eller*

4. när data lämnas till en statlig eller kommunal myndighet som ska använda dem i en konkurrensutsatt verksamhet som avser tillhandahållande av data.

## 10 §

Lagen gäller inte för data som

1. omfattas av en sådan ensamrätt som följer av patentlagen (1967:837), mönsterskyddslagen (1970:485), lagen (1992:1685) om skydd för kretsmönster för halvledarprodukter, växtförädlarrättslagen (1997:306), varumärkeslagen (2010:1877) eller lagen (2018:1653) om företagsnamn,

2. tredje man innehar rätt till enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk,

3. utgörs av datorprogram, *eller*

4. utgörs av logotyper, heraldiska vapen eller insignier.

*Första stycket ska inte tillämpas avseende sådana kategorier av skyddade data som framgår av artikel 3.1 c i EU:s dataförvaltningsförordning.*

## **2 kap.**

### *5 a §*

*En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska ställa upp villkor för vidareutnyttjandet i enlighet med artikel 5 i EU:s dataförvaltningsförordning.*

*En myndighet som tillgängliggör konfidentiella data till en vidareutnyttjare som avser att överföra dem till tredje land i enlighet med artikel 5.10 i EU:s dataförvaltningsförordning är skyldig att anmäla de överträdelser av artikel 5.14 som myndigheten får kännedom om till tillsynsmyndigheten enligt lag (2023:000) med kompletterande bestämmelser till EU:s dataförvaltningsförordning.*

### **Förteckning över skyddade data som görs tillgängliga**

### *6 a §*

*Den myndighet som regeringen bestämmer ska tillhandahålla en gemensam informationspunkt enligt artikel 8 i EU:s dataförvaltningsförordning.*

*En myndighet som tillgängliggör skyddade data för vidareutnyttjande ska informera den myndighet som tillhandahåller den gemensamma informationspunkten om sådana data och villkoren för vidareutnyttjande av dessa.*

## **3 kap.**

### *1 a §*

*En myndighet som innehar skyddade data får endast ge någon en exklusiv rätt att vidareutnyttja dessa data i den mån det är tillåtet enligt artikel 4 i EU:s dataförvaltningsförordning.*

**4 kap.**

## 1 §

En myndighet eller ett offentligt företag som har rätt att ta ut en avgift för att tillgängliggöra data för vidareutnyttjande får inte beräkna den till ett högre belopp än vad som följer av 2–6 §§.

En myndighet eller ett offentligt företag som har rätt att ta ut en avgift för att tillgängliggöra data *eller skyddade data* för vidareutnyttjande får inte beräkna den till ett högre belopp än vad som följer av 2–6 §§.

## 2 a §

*Vid tillgängliggörande av skyddade data får en avgift, utöver vad som följer av 2 § första stycket första meningen, också täcka sådana kostnader som framgår av artikel 6.5 i EU:s dataförvaltningsförordning.*

**5 kap.**

## 1 §

En myndighet ska inom fyra veckor avgöra ett ärende till följd av en begäran om tillgängliggörande av data för vidareutnyttjande.

*Om en sådan begäran avser skyddade data ska ärendet avgöras inom åtta veckor.*

Tidsfristen får förlängas med ytterligare fyra veckor, om en begäran är omfattande eller komplicerad. Myndigheten ska underrätta sökanden om förlängningen och redovisa skälen för den senast tre veckor från den dag då begäran kom in.

---

Denna lag träder i kraft den 1 januari 2024.

## Förteckning över remissinstanserna

Efter remiss har yttranden kommit in från Arbetsförmedlingen, Bolagsverket, E-hälsomyndigheten, Folkhälsomyndigheten, Försvarmakten, Försvarets materielverk, Försvarets radioanstalt, Förvaltningsrätten i Luleå, Förvaltningsrätten i Stockholm, Försäkringskassan, Gagnefs kommun, Göteborgs kommun, Integritetsskyddsmyndigheten, Justitiekanslern, Järfälla kommun, Kammarrätten i Jönköping, Kommerskollegium, Konkurrensverket, Konsumentverket, Kungliga biblioteket, Kungliga tekniska högskolan, Lantmäteriet, Läkemiddelsverket, Malmö kommun, Myndigheten för digital förvaltning, Myndigheten för samhällsskydd och beredskap, Nacka kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Post och telestyrelsen, Regelrådet, Region Blekinge, Region Skåne, Region Stockholm, Region Östergötland, Skatteverket, Socialstyrelsen, Statistiska centralbyrån, Stockholms kommun, Svenskt näringsliv, Sveriges advokatsamfund, Sveriges kommuner och regioner, Sveriges meteorologiska och hydrologiska institut, Sveriges universitets- och högskoleförbund, Säkerhetspolisen, TechSverige, Teknikföretagen, Verket för innovationssystem, Vetenskapsrådet, Växjö kommun och Åklagarmyndigheten.

Följande remissinstanser har inte svarat eller angett att de avstår från att lämna några synpunkter: Bodens kommun, Båstads kommun, CGI Sverige AB, Chalmers tekniska högskola AB, Civic Tech Sweden, Dun & Bradstreet Sverige AB, Ekerö kommun, Falköpings kommun, Google Sverige, Grums kommun, Gävle kommun, InfoTrader i Ronneby AB, Internetstiftelsen, Jönköpings kommun, Kristianstads kommun, Kävlinge kommun, Köpings kommun, Leksands kommun, Lidköpings kommun, Lunds kommun, Malå kommun, Mariestads kommun, Meta Sverige, Metria AB, MyData Sverige, Mönsterås kommun, Näringslivets regelnämnd, Piteå kommun, Research Institutes of Sweden (RISE), Riksdagens ombudsmän, Rättighetsalliansen, Sollefteå kommun, Svenljunga kommun, Svenska institutet för standarder, Tibro kommun, Tillväxtanalys, Tillväxtverket, Trosa kommun, UC AB och Åre kommun.