

2017-09-19

FRA beteckning
20 400:3589/17:2

Justitiedepartementet
Grundlagsenheten
103 33 Stockholm

Er handläggare
Ia Hamlin

Ert datum
2017-06-19

Er beteckning
Ju2017/05495/L6

FRA handläggare
Maria Malmberg Pyke

FRA föreg. datum

FRA föreg. beteckning

Remittering av betänkandet En ny kamerabevakningslag (SOU 2017:55)

Försvarets radioanstalt (FRA) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på betänkandet.

Sammanfattning

FRA ställer sig positiv till förslaget om en ny gemensam lag för all kameraövervakning (se nedan 9.1).

FRA har i yttrande över dataskyddsutredningens betänkande Ny dataskyddslag (SOU 2017:39) framfört bl.a. följande synpunkter, vilka även är aktuella i förhållande till kamerabevakningslagen.

- Det bör framgå direkt av 1 kap. 2 § dataskyddslagen att incidentrapportering enligt artikel 33 dataskyddsförordningen och information till registrerade om sådan incident enligt artikel 34 dataskyddsförordningen inte ska gälla, om rapporteringsskyldighet följer av 10 a § säkerhetsskyddsförordningen (1996:633) (se nedan 10.1).
- Information till registrerade om personuppgiftsincidenter enligt artikel 34 dataskyddsförordningen ska inte krävas om uppgifterna avseende incidenten omfattas av sekretess (se nedan 10.1).

FRA

- FRA ifrågasätter förslaget att sanktionsavgifter ska få tas ut av myndigheter (se nedan 10.1).

FRA instämmer i utredningens bedömning att undantag från tillståndkravet och upplysningskravet ska finnas kvar (se nedan 11.8 och 12.2).

FRA ifrågasätter att bestämmelser om sanktionsavgifter görs tillämpliga på myndigheter (se nedan 15.2).

FRA:s synpunkter följer betänkandets disposition.

9.1 En ny lag

FRA ställer sig positiv till förslaget att införa en ny gemensam lag för all kameraövervakning.

10.1 Lagens inledande bestämmelser om syfte m.m.

Förhållandet till andra bestämmelser

Mot bakgrund av att dataskyddslagen föreslås bli gällande i tillämpliga delar vill FRA lyfta fram de synpunkter som FRA har lämnat i sitt remissyttrande över Ny dataskyddslag (SOU 2017:39) och som är av relevans i detta sammanhang.¹ Synpunkterna framgår nedan.

Sammanfattning

Följande bör framgå direkt av 1 kap. 2 § dataskyddslagen.²

[...]

- b) Att incidentrapportering enligt artikel 33 dataskyddsförordningen och information till registrerade om sådan incident enligt artikel 34 dataskyddsförordningen inte ska gälla om rapporteringsskyldighet följer av 10 a § säkerhetskyddsförordningen (1996:633) (se nedan 6.4.2).*

¹ Ju2017/04264/L6, FRA:s dnr 20 400:3498/17:2

² Förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning.

För verksamhet som dataskyddsförordningen ska gälla bör följande begränsning införas i dataskyddslagen.

- Information till registrerade om personuppgiftsincidenter enligt artikel 34 dataskyddsförordningen ska inte krävas om uppgifterna avseende incidenten omfattas av sekretess (se nedan 13.4.1).

FRA ifrågasätter förslaget att sanktionsavgifter ska få tas ut av myndigheter (se nedan 18.5.3).

[...]

6.4.2 Ska förordningens bestämmelser göras gällande utanför deras tillämpningsområde? (s. 91 ff.)

[...]

b) Artikel 33 och artikel 34 bör inte gälla incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633), vilket bör framgå direkt av dataskyddslagen.³

Enligt artikel 33 dataskyddsförordningen ska personuppgiftsincidenter rapporteras till tillsynsmyndigheten.

Det håller på att växa fram ett flertal parallella system för rapportering av incidenter i it-system.

- Idag ska myndigheter rapportera it-incidenter enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen).
- Motsvarande bestämmelser om rapportering av personuppgiftsincidenter i dataskyddsförordningen finns i förslag till brottsdatalog avseende brottsbekämpande myndigheters verksamhet.⁴
- Vidare föreslås incidentrapporteringsplikt för leverantörer av samhällsviktiga och digitala tjänster i samband med införandet av EU:s NIS-direktiv.⁵

³ Jämför vad som anges i 3 kap. 9 § förslag till brottsdataförordning i betänkandet Brottsdatalog (SOU 2017:29).

⁴ Se betänkandet Brottsdatalog (SOU 2017:29).

⁵ Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensamt nivå på säkerhet i nätverks- och informationssystem i hela unionen. Se betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36).

De skyldigheter att rapportera incidenter som kommer följa av de olika författningarna kommer delvis att överlappa varandra. En och samma incident kan komma att rapporteras enligt flera olika lagar och till olika tillsynsmyndigheter.⁶ Denna ordning är inte lätt att överblicka.

För FRA:s del är det viktigt att rapportering enligt nämnda författningar och författningsförslag inte ska ske för det fall rapporteringsskyldighet föreligger enligt 10 a § säkerhetsskyddsförordningen. Detta förhållande har reglerats eller kommer att regleras i de författningar som redovisas i det följande.

Rapporteringsskyldigheten enligt krisberedskapsförordningen omfattar inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen. Detsamma föreslås gälla enligt betänkandet Ny brottsdatalog (SOU 2017:29), s. 331 f., vari följande anges.

En personuppgiftsincident uppfyller kriterierna för en it-incident. Det innebär att de flesta behöriga myndigheter kommer att behöva anmäla sådana incidenter enligt två olika förfaranden och till olika myndigheter. It-incidenter som kan antas påverka säkerheten för hemliga uppgifter som rör Sveriges säkerhet ska dock enbart anmälas enligt säkerhetsskyddsförordningen. Behovet av att skydda sådan information anses vara så viktigt att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av den. Även om den rapporteringen har ett annat syfte än rapporteringen av personuppgiftsincidenter, anser utredningen att behovet av skydd för uppgifter som rör Sveriges säkerhet väger tyngre än behovet av att skydda enskilda från eventuella intrång i den personliga integriteten. Eftersom nationell säkerhet ligger utanför direktivets tillämpningsområde anser utredningen att sådana personuppgiftsincidenter som ska anmälas enligt 10 a § säkerhetsskyddsförordningen inte bör anmälas till tillsynsmyndigheten.

Även i betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster SOU (2017:36), s. 87, anges att incidentrapportering enligt den föreslagna s.k. NIS-lagen inte ska tillämpas på sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

⁶ Incidenter enligt krisberedskapsförordningen och den föreslagna lagen om vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster ska rapporteras till Myndigheten för samhällsskydd och beredskap. I nu aktuellt betänkande och betänkandet Brottsdatalog framgår att personuppgiftsincidenter rapporteras till Datainspektionen.

Något sådant undantag som anges ovan finns dock inte i förslaget till dataskyddslag.

Incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen gäller Sveriges säkerhet och omfattas inte av unionsrätten. I linje med vad som gäller idag och som föreslås i de ovan nämnda betänkandena bör inte artikel 33 dataskyddsförordningen gälla för det fall en personuppgiftsincident ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

Av samma skäl bör inte heller artikel 34 dataskyddsförordningen om information till en registrerad vid en personuppgiftsincident gälla incidenter som ska rapporteras enligt nämnda bestämmelse i säkerhetsskyddsförordningen.

Mot denna bakgrund bör det av 1 kap. 2 § förslag till dataskyddslag framgå att artikel 33 och 34 inte ska gälla personuppgiftsincidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

13.4.1 Sekretess och tystnadsplikt ska gå före informationsplikten (s. 204)

För verksamhet som dataskyddsförordningen ska gälla bör information till registrerade om personuppgiftsincidenter enligt artikel 34 dataskyddsförordningen inte krävas om uppgifterna avseende incidenten omfattas av sekretess. En begränsning med detta innehåll bör, med stöd av artikel 23 dataskyddsförordningen införas i dataskyddslagen.

Dataskyddsförordningen kommer att gälla en mängd verksamheter av varierande slag. Information om en personuppgiftsincident skulle kunna röja uppgifter som omfattas av sekretess. Därför bör det införas en bestämmelse som begränsar information till den registrerade på samma sätt som föreslås gälla artiklarna 13-15 i dataskyddsförordningen enligt 5 kap. 1 § dataskyddslagen.⁷

⁷ Jfr även den föreslagna begränsningen av information till registrerade vid personuppgiftsincident i 3 kap. 11 § brottsdatalagen, se SOU 2017, s. 337.

18.5 Sanktionsavgifter inom offentlig sektor

18.5.3 Överväganden och förslag (s. 287 ff.)

FRA ifrågasätter om det är lämpligt att sanktionsavgifter ska kunna tas ut av myndigheter. Motsvarande fråga har tidigare behandlats i betänkandet Myndighetsdatalag (SOU 2015:39). I betänkandet (s. 631) anges att det följer av allmänna rättsgrundsatser att vite inte bör användas som sanktionsmedel mellan statliga myndigheter. Vidare påtalas att myndigheters behandling av personuppgifter sker i en verksamhet som i allmänhet inte förekommer utanför det allmänna och som omgärdas av helt andra krav och regler än vad som annars är fallet. I betänkandet anges att det inte finns några bärande skäl för att i alla delar ha samma sanktionsmöjligheter mot både myndigheter och enskilda. Konklusionen i betänkandet, s. 631, är följande.

Det finns [...] inget sådant starkt vägande skäl som talar för att myndigheters behandling av personuppgifter utgör ett sådant undantagsfall att man bör avvika från den allmänna rättsgrundsatsen att staten inte kan rikta viten mot sig själv.

Sanktionsavgifter är ett effektivt rättsmedel att komma till rätta med överträdelser hos enskilda, t.ex. privata bolag, som enligt förslaget till ny dataskyddslag inte längre riskerar ådömas straff för att bryta mot dataskyddsförordningen. För ansvariga vid statliga myndigheter kan dock alltjämt tjänstemannaansvar utkrävas. Därutöver har den registrerade möjlighet att utkräva skadestånd av myndigheter vid överträdelser av dataskyddsförordningen. Regeringen har också möjlighet att ställa krav på myndigheter genom allmänna direktiv och förordningar för att komma tillrätta med överträdelser.

Mot bakgrund av det ovan angivna ifrågasätter FRA förslaget att tillsynsmyndighet ska få ta ut sanktionsavgifter av myndigheter.

11.8 Särskilda undantag från tillståndskravet

FRA instämmer i utredningens bedömning att undantag från kravet på tillstånd även fortsättningsvis ska finnas när bevakningen sker för att skydda vissa byggnader, anläggningar eller områden som har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet.

12.2 Undantag från upplysningskravet

Bevakning av skyddsobjekt

FRA instämmer även i utredningens bedömning att det undantag från upplysningskravet som finns i kameraövervakningslagen, och som motsvarar undantaget från tillståndskravet, ska behållas i den nya kamerabevakningslagen.

15.2 Tillsynsmyndighetens befogenheter, sanktioner, rättsmedel och skadestånd

Befogenheter och sanktioner vid kamerabevakning

Med hänvisning till de synpunkter som FRA har lämnat i sitt remissyttrande över Ny dataskyddslag (SOU 2017:39) ifrågasätter FRA att den föreslagna bestämmelsen, så vitt avser sanktionsavgifter, ska gälla för myndigheter (se ovan under 10.1). Det bör uttryckligen framgå att bestämmelser om sanktionsavgifter inte ska tillämpas gällande myndigheter. Det sista stycket i bestämmelsen bör som en följd av det utgå.

I detta ärende har generaldirektören Dag Hartelius beslutat. I den slutliga handläggningen har också deltagit överdirektören Charlotta Gustafsson, chefsjuristen Michaela Dráb, planeringschefen Johan Dahlstedt, kontorschefen Helene Bergquist Frederiksen samt juristen Maria Malmberg Pyke (avd V/Rätts), tillika föredragande.

Försvarets radioanstalt

Dag Hartelius

Maria Malmberg Pyke

FRASändlista*För kännedom*

Försvarsdepartementet/Sund

Försvarsdepartementet/Rättssekretariatet

Internt FRA

GD

ÖD

Chefsjuristen

C Plan

Informationschefen

Säkerhetsskyddschefen

AC

KC Rätts (Avd V/Rättskontoret)