

Rekommendation



**Rekommendation 01/2019 om utkastet till förteckning från
Europeiska datatillsynsmannen över de
behandlingsverksamheter som omfattas av kravet på en
konsekvensbedömning avseende dataskydd (artikel 39.4 i
förordning (EU) 2018/1725)**

Antagen den 10 juli 2019

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Innehållsförteckning

1	SAMMANFATTNING AV OMSTÄNDIGHETERNA	4
2	BEDÖMNING.....	4
2.1	Europeiska dataskyddsstyrelsens övergripande resonemang angående den inlämnade förteckningen	4
2.2	Analys av utkastet till förteckning	5
3	SLUTSATS.....	8

Europeiska dataskyddsstyrelsen har antagit denna rekommendation

med beaktande av artikel 70.1e i 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),

med beaktande av artikel 39.4 i 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 (nedan kallad *förordning 2018/1725*),

med beaktande av artikel 12 och artikel 22 i dess arbetsordning av den 25 maj 2018, ändrad den 23 november 2018, och

av följande skäl:

(1) Europeiska dataskyddsstyrelsens viktigaste uppgift är att se till att förordning (EU) 2016/679 tillämpas på ett enhetligt sätt i hela Europeiska ekonomiska samarbetsområdet (EES). I enlighet med artikel 70.1 i den allmänna dataskyddsförordningen ska Europeiska dataskyddsstyrelsen på begäran av en av sina ledamöter behandla frågor om tillämpningen av denna förordning och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av denna förordning. I artikel 39.6 i förordning 2018/1725 föreskrivs att Europeiska datatillsynsmannen ska begära att Europeiska dataskyddsstyrelsen, i enlighet med artikel 70.1 e i dataskyddsförordningen, undersöker utkastet till förteckningar över behandlingsverksamheter som omfattas kravet på en konsekvensbedömning avseende dataskydd i enlighet med artikel 39.4 i förordning 2018/1725. Denna skyldighet gäller i den utsträckning som förteckningen tar upp behandlingsverksamheter som en personuppgiftsansvarig, i den mening som avses i artikel 3.8 i förordning 2018/1725, utför gemensamt med en eller flera andra personuppgiftsansvariga än unionsinstitutioner och unionsorgan. Syftet med denna rekommendation är således att vara konsekvent med den hållning som tidigare intagits i förhållande till utkast till förteckningar över tillsynsmyndigheter. Dataskyddsstyrelsen strävade efter att nå konsekvens genom att för det första kräva att tillsynsmyndigheterna medtar vissa typer av behandlingsverksamheter i sina förteckningar, för det andra genom att begära att de avlägsnar vissa kriterier som dataskyddsstyrelsen inte anser nödvändigtvis innebär att behandlingen medför hög risk för de registrerade och slutligen genom att begära att tillsynsmyndigheterna ska använda vissa kriterier på ett enhetligt sätt.

(4) Den personuppgiftsansvarige är endast skyldig att göra en konsekvensbedömning avseende dataskydd i enlighet med artikel 39.1 i förordning 2018/1725 om behandlingen "sannolikt leder till en hög risk för fysiska personers rättigheter och friheter". I artikel 39.3 i förordning 2018/1725 anges vad som sannolikt leder till en hög risk. Denna är en icke uttömmande förteckning, som motsvarar ordalydelsen i artikel 35.3 i dataskyddsförordningen. Artikel 29-arbetsgruppen har i sina riktlinjer för

konsekvensbedömning¹ avseende dataskydd, som har godkänts av dataskyddsstyrelsen², angett kriterier som kan göra det lättare att avgöra när behandlingsverksamheter omfattas av kravet på en konsekvensbedömning avseende dataskydd. Enligt artikel 29-arbetsgruppens riktlinjer WP248 kan en personuppgiftsansvarig i de flesta fall anse att det krävs en konsekvensbedömning om en behandling uppfyller två kriterier, men i vissa fall kan en personuppgiftsansvarig anse att det krävs en konsekvensbedömning även om behandlingen endast uppfyller ett av dessa kriterier.

De förteckningar som den europeiska datatillsynsmannen utarbetar bidrar till samma mål, dvs. att identifiera behandlingsverksamheter som sannolikt leder till en hög risk och behandlingsverksamheter för vilka det därför krävs en konsekvensbedömning avseende dataskydd. De kriterier som har utarbetats i artikel 29-arbetsgruppens riktlinjer är relevanta.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

1 SAMMANFATTNING AV OMSTÄNDIGHETERNA

1. Europeiska datatillsynsmannen lämnade, med tillämpning av artikel 39.4 i förordning 2018/1725, in sitt utkast till förteckning till Europeiska dataskyddsstyrelsen den 18 mars 2019, och tillhandahöll en reviderad version den 21 juni 2019.
2. Det dokument som lämnades in av Europeiska datatillsynsmannen inbegrep också en del som rörde artikel 39.5 i förordning 2018/1725. I det reviderade utkastet sägs det uttryckligen att den artikel 39.5-förteckning som ingår i utkastet endast är tillämplig i situationer där unionsinstitutioner eller unionsorgan agerar personuppgiftsansvariga tillsammans med någon annan eller på egen hand. I synnerhet omfattar utkastet till artikel 39.5-förteckning behandlingsverksamheter med anknytning till unionsinstitutioner eller unionsorgan som behandlar uppgifter inom ramen för sin interna förvaltning
3. Europeiska dataskyddsstyrelsen noterar således att denna andra del av dokumentet inte omfattas av tillämpningsområdet för artikel 39.6 i förordning 2018/1725. I denna bestämmelse fastställs att skyldigheten att begära en rekommendation av Europeiska dataskyddsstyrelsen endast är tillämplig på punkter som rör behandlingsverksamheter där en personuppgiftsansvarig som omfattas av förordning 2018/1725 agerar gemensamt med en eller flera andra personuppgiftsansvariga som inte är unionsinstitutioner och unionsorgan. Europeiska dataskyddsstyrelsen kommer således inte att kommentera denna del av utkastet till dokument.

2 BEDÖMNING

2.1 Europeiska dataskyddsstyrelsens övergripande resonemang angående den inlämnade förteckningen

¹Artikel 29-arbetsgruppen, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679 (WP248 rev. 1).

²Europeiska dataskyddsstyrelsen, Godkännande 1/2018.

4. Den förteckning som har lämnats in till Europeiska dataskyddsstyrelsen tolkas som en ytterligare specifikation av artikel 39.1 i förordning 2018/1725, som ska ha företräde under alla omständigheter. Förteckningen bör dock inte betraktas som uttömmande.
5. Europeiska dataskyddsstyrelsen noterar artikel 39.10 i förordning 2018/1725, som föreskriver att det inte krävs någon konsekvensbedömning avseende dataskydd om den specifika behandlingsåtgärden eller åtgärds kombinationen i fråga har en rättslig grund i en rättsakt som antagits på grundval av fördragen och om en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning som föregick antagandet av den rättsakten. I detta fall ska artikel 30.1–6 inte vara tillämpliga, såvida inte rättsakten i fråga föreskriver annat.
6. Denna rekommendation rör generellt sett inte punkter som Europeiska datatillsynsmannen tagit upp, men som bedömts ligga utanför tillämpningsområdet för artikel 39.6 i förordning 2018/1725. Här avses punkter som inte rör en behandlingsverksamhet där en registeransvarig agerar tillsammans med en eller flera registeransvariga som inte unionsinstitutioner eller unionsorgan,. Eftersom Europeiska datatillsynsmannen har beslutat att anta en förteckning för båda typerna av behandlingsverksamheter, är denna rekommendation således tillämplig på båda kategorierna av behandlingsverksamheter.
7. Rekommendationen syftar till en anpassning till kärnan av behandlingsverksamheter, som styrelsen uppmanade alla tillsynsmyndigheter att lägga till sin förteckning, om den inte redan fanns där.
8. Detta innebär att styrelsen rekommenderar Europeiska datatillsynsmannen att kräva att en konsekvensbedömning avseende dataskydd genomförs för ett begränsat antal behandlingsverksamheter som ska definieras på ett samordnat sätt.
9. När det inte sägs något i denna rekommendation om punkter i den inlämnade förteckningen över behandlingsverksamheter som omfattas av krav på en konsekvensbedömning avseende dataskydd innebär detta att Europeiska dataskyddsstyrelsen inte uppmanar Europeiska datatillsynsmannen att vidta ytterligare åtgärder.
10. Slutligen påminner Europeiska dataskyddsstyrelsen om att det är avgörande med insyn för personuppgiftsansvariga och personuppgiftsbiträden. För att förtydliga punkterna i förteckningen rekommenderar Europeiska dataskyddsstyrelsen att man för varje typ av behandling i förteckningarna tar med en uttrycklig hänvisning till riktlinjernas kriterier. Det skulle vara ett sätt att förbättra insynen.

2.2 Analys av utkastet till förteckning

11. Med beaktande av
 - a. att det enligt artikel 39.1 i förordning 2018/1725 krävs en konsekvensbedömning avseende dataskydd när behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, och
 - b. att artikel 39.3 i förordning 2018/1725 innehåller en förteckning som inte är uttömmande över de typer av behandling som kräver en konsekvensbedömning avseende dataskydd:

utfärdar styrelsen följande rekommendationer:

KÄNSLIGA UPPGIFTER

12. I utkastet till förteckning anges "känsliga uppgifter" som ett kriterium i enlighet med följande: "Känsliga uppgifter: Uppgifter som avslöjar etniskt ursprung eller ras, politisk åsikter, religiös tro eller politisk åskådning, medlemskap i fackförening, genetiska data, biometriska data för entydig identifiering av en fysisk person, uppgifter rörande hälsa, sexualliv eller sexuell läggning, fällande brottmålsdomar eller brott och därtill knutna säkerhetsåtgärder eller uppgifter som anses känsliga av andra skäl."
13. Även om ordalydelsen i mycket liknar den i riktlinjerna för konsekvensbedömning avseende dataskydd enligt A29WP WP248rev.01, som godkänts av Europeiska dataskyddsstyrelsen, finns det en betydande skillnad. Där utkastet till förteckning använder ordalydelsen "eller anses känsliga av andra skäl", anges i riktlinjerna "uppgifter av starkt personlig karaktär"
14. Styrelsen noterar att dataskyddsförordningen inte använder termen "känsliga uppgifter" i någon av artiklarna, även om den används i två av skälen. Termen uppfattas så att den uteslutande betecknar de kategorier av uppgifter som anges i artiklarna 9 och 10 i dataskyddsförordningen. För att undvika förvirring rekommenderar styrelsen Europeiska datatillsynsmannen att ändra formuleringen "anses känsliga av andra skäl" genom att använda den exakta ordalydelsen i konsekvensbedömningen avseende dataskydd.

STORSKALIG BEHANDLING

15. Styrelsen noterar att Europeiska datatillsynsmannen hänvisar till en EU-institutions interna telefonregister som ett motexempel på storskalig behandling. Utan att det påverkar frågan om huruvida en konsekvensbedömning avseende dataskydd verkligen behövs, är det inte klart varför en EU-institutions telefonregister inte i sig skulle omfattas av begreppet "storskalig behandling", särskilt eftersom det potentiellt kan innehålla personuppgifter rörande ett stort antal individer. Europeiska dataskyddsstyrelsen erinrar om att begreppet "stor" också avser proportionen av den relevanta populationen, i enlighet med definitionen i Artikel 29-arbetsgruppens riktlinjer om dataskyddsombud, vilka antogs i december 2016, reviderades den 5 april 2017, och godkändes av Europeiska dataskyddsstyrelsen. Europeiska dataskyddsstyrelsen [rekommenderar användning av ett annat exempel](#).

DATAMÄNGDER FRÅN OLIKA DATABEHANDLINGSDATAOPERATIONER SOM MATCHAS ELLER KOMBINERAS

16. Europeiska dataskyddsstyrelsen noterar att det exempel som används för behandlingsverksamhet som inbegriper datamängder från olika databehandlingsoperationer som matchas eller kombineras kan ge upphov till tvivel om dess lagenlighet enligt förordning 2018/1725, med hänsyn till hur beskrivningen ser ut. Medan Europeiska dataskyddsstyrelsen inte är i den position och inte har den kompetens som krävs för att bedöma denna lagenlighet, rekommenderar den för tydlighetens skull att man använder ett annat exempel.

SÅRBARA REGISTRERADE

17. Styrelsen noterar att Europeiska dataskyddsombudsmannen i sitt beslut använder ett motexempel med personal vid EU:s institutioner som ställs mot de standardförfaranden som fastställs i tjänsteföreskrifterna. Styrelsen erinrar om att anställda är förtecknade som sårbara registrerade i riktlinjerna för konsekvensbedömning avseende dataskydd enligt A29WP WP248rev.01, som godkänts av Europeiska dataskyddsstyrelsen. Även om det kan hävdas att

ojämlika styrkeförhållanden mellan en arbetsgivare och en anställd är mindre påtagliga inom ramen för standardförfaranden enligt relevanta tjänsteföreskrifter, kan man inte utgå från att så alltid är fallet, särskilt när de anställda inte har något nämnvärt inflytande på innehållet i den nämnda bestämmelserna. Dessutom står det inte klart vilka förfaranden som kan anses som icke-standard, dvs fall där konsekvensbedömning avseende dataskydd kan komma att krävas, vilket kan resultera i betydande förvirring. Av dessa skäl rekommenderar styrelsen att Europeiska datatillsynsmannen ersätter det givna motexemplet med ett annat.

3 SLUTSATS

18. Styrelsen uppmanar Europeiska datatillsynsmannen att göra följande ändringar i sin förteckning:
-) Beträffande känsliga uppgifter: Styrelsen rekommenderar Europeiska datatillsynsmannen att ändra formuleringen "anses känsliga av andra skäl" genom att använda den exakta ordalydelsen i riktlinjerna i konsekvensbedömningen avseende dataskydd
 -) Beträffande uppgifter som behandlas i stor skala: Styrelsen rekommenderar Europeiska datatillsynsmannen att ändra sin förteckning genom att använda ett annat motexempel.
 -) Vad gäller datamängder från olika databehandlingsoperationer som matchas eller kombineras Styrelsen rekommenderar Europeiska datatillsynsmannen att ändra sin förteckning genom att använda ett annat exempel.
 -) Vad gäller sårbara registrerade: Styrelsen rekommenderar Europeiska datatillsynsmannen att ändra sin förteckning genom att använda ett annat motexempel.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)