2017-09-11

Konsekvens-bedömning avseende dataskydd

Krav enligt art. 35 dataskyddsförordningen

Dataskyddsförordningen (GDPR) kommer att gälla som lag i alla EU:s medlemsländer från och med den 25 maj 2018. Förordningen kommer att ersätta personuppgiftslagen (1998:204), PuL, och vara direkt tillämplig i Sverige. Dataskyddsförordningen gäller alla som behandlar personuppgifter i sin verksamhet, oavsett om det är en statlig eller privat aktör oaktat organisationens storlek.

I dataskyddsförordningen har ett nytt krav införts som innebär att personuppgiftsansvarige ska genomföra en konsekvensbedömning avseende dataskydd i de fall riskfylld personuppgiftsbehandling utförs.

Allmänt

Enligt artikel 24 i dataskyddsförordningen har den personuppgiftsansvarige ett grundläggande ansvar att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säker behandling av personuppgifter.

I artikel 35 anges vidare att konsekvensbedömning (så kallad DPIA-analys, Data Protection Impact Assessment) för skydd av personuppgifter ska genomföras om en personuppgiftsbehandling ”sannolikt kan leda till en hög risk för fysiska personers rättigheter och friheter”.

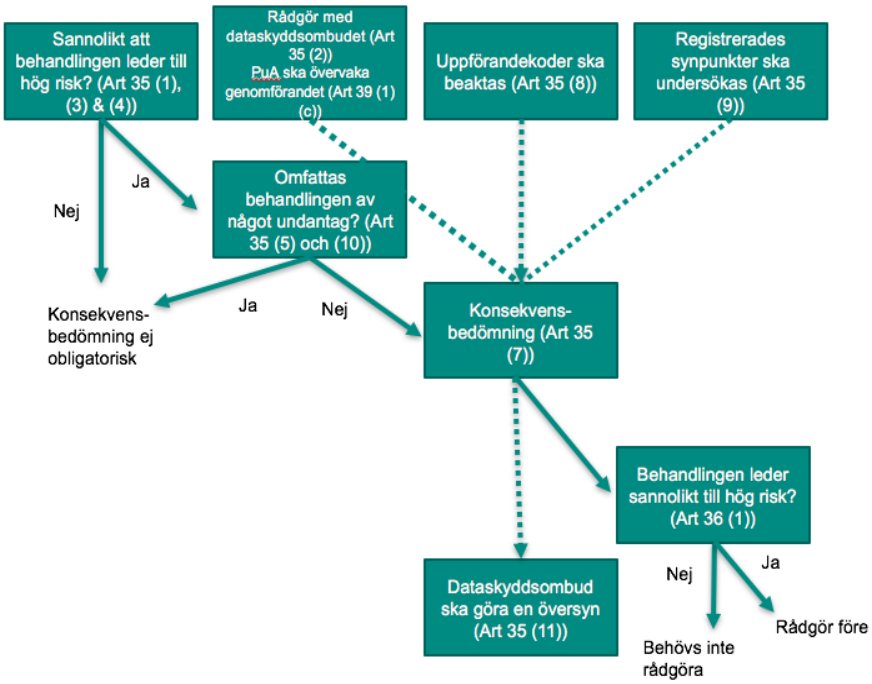
Underlåtenhet att genomföra en konsekvensbedömning när det är obligatoriskt enligt dataskyddsförordningen kan resultera i en sanktionsavgift för den personuppgiftsansvarige.

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

Artikel 29-gruppen[1] rekommenderar att en konsekvensbedömning genomförs även i situationer som inte omfattas av artikel 35.

När en konsekvensbedömning ska genomföras

Nedan följer en enkel illustration av de grundläggande principer som gäller för när en konsekvensbedömning bör göras.



Konsekvensbedömning ska genomföras när personuppgiftsbehandlingen *”sannolikt kan leda till hög risk för fysiska personers rättigheter och friheter”*:[2]

I artikel 35 (3) anges ett antal exempel på när en personuppgiftsbehandling kan leda till sådan hög risk. Denna lista är emellertid inte uttömmande, utan det kan finnas ytterligare behandlingar som behöver analyseras. Artikel 29-gruppen har därför tagit fram ett antal kriterier som bör beaktas. Dessa kriterier redovisas nedan.

En konsekvensbedömning kan genomföras för en enskild personuppgiftsbehandling eller omfatta en serie liknande personuppgiftsbehandlingar som medför likartade höga risker. Detta kan exempelvis vara när liknande teknik används för att samla in samma typ av data för samma

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

[1] Se ”Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ”likely to result in a high risk” for the purposes of Regulation 2016/679”, 4 april 2017

[2] Artikel 35 (1) tillsammans med Artikel 35 (3) samt 35 (4)

ändamål, till exempel kan en järnvägsaktör som installerar övervakningskameror på alla tågstationer, göra en konsekvensbedömning gällande samtliga personuppgiftsbehandlingar.

Enligt artikel 29-gruppen ska hänsyn tas till följande kriterier vid bedömningen av huruvida en konsekvensbedömning bör genomföras eller inte, det vill säga om personuppgiftsbehandlingen avser:

- Utvärdering eller bedömning av den registrerade inklusive profilering; kan exempelvis vara den registrerades arbetsprestationer, ekonomiska faktorer, hälsa, personliga preferenser eller intressen, beteendemönster och så vidare (till exempel när en bank screenar sina kunder mot en kredit-databas).
- Automatisk behandling på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer; till exempel när behandlingen kan leda till uteslutning eller diskriminering av en individ. (Artikel 29-gruppen har för avsikt att publicera en vägledning avseende denna punkt).
- Systematisk övervakning; behandling som syftar till att observera, bevaka eller kontrollera olika personobjekt.
- Känslig data; avser de särskilda kategorier som definieras i artikel 9 (till exempel politisk åsikt eller religion) eller uppgifter som rör lagöverträdelser. Avser även data som typiskt sett anses höja risken för individers rättigheter och friheter, till exempel ekonomiska uppgifter eller geografisk plats. Om uppgifterna gjorts offentliga av den registrerade eller en tredje part kan detta ha betydelse.
- Behandling i stor omfattning; stor omfattning definieras inte i dataskyddsförordningen, men viss ledning kan hämtas i skäl 91. Enligt artikel 29-gruppen ska följande beaktas vid avgörande om behandlingen ska anses vara i stor omfattning:
    - Antalet registrerade som omfattas av behandlingen
    - Volymen av data och omfattningen av dataposter som behandlas
    - Behandlingens tid och varaktighet
    - Den geografiska spridningen av behandlingen
- Data som matchas eller kombineras i flera datakällor; till exempel datasammansättning som ett resultat av två separata personuppgiftsbehandlingar som gjorts i olika syften och/eller av olika personuppgiftsansvariga på ett sätt som överstiger den registrerades rimliga förväntningar.
- Data som rör sårbara fysiska personer; detta gäller främst registrerade som på grund av sin ställning inte

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

anses ha samma förmåga att samtycka eller motsätta sig behandling av personuppgifter, till exempel barn, äldre, patienter.

- Innovativ användning eller användning av tekniska/organisatoriska lösningar; till exempel fingeravtryck och ansikts-scanning. Vägledning avseende användning av ny teknik kan hämtas i skäl 89 och 91 dataskyddsförordningen.
- Dataöverföring till tredje land; till exempel vid användning av vissa molntjänster.
- När behandlingen hindrar individer att utöva sina rättigheter alternativt använda sig av ett kontrakt eller tjänst; till exempel när en personuppgiftsbehandling utförs på allmän plats och den registrerade inte har möjlighet att undvika, eller som på något sätt begränsar tillgång till en tjänst eller ingående av avtal.

En genomgång av de olika kriterierna ska genomföras för att utreda huruvida en konsekvensbedömning bör utföras eller inte. Artikel 29-gruppen anser att man som huvudregel bör göra en konsekvensbedömning när minst två av ovan nämnda kriterier är uppfyllda. Om den personuppgiftsansvarige väljer att inte genomföra en konsekvensbedömning trots att minst två kriterier uppfylls ska beslutet till detta motiveras och dokumenteras.

Hur en konsekvensbedömning bör genomföras

Konsekvensbedömningen ska genomföras före behandlingen av personuppgifter sker och ska uppdateras kontinuerligt för att säkerställa regeluppfyllnad. Konsekvensbedömningen är således inte en engångsföreteelse.

Vid begäran ska konsekvensbedömningen kunna redovisas till Datainspektionen.

Personuppgiftsansvarige ansvarar för att konsekvensbedömningen genomförs, men kan dock utse någon annan lämplig person, internt eller externt, för själva utförandet. Denna kan exempelvis utföras av dataskyddsombudet[3].

Om ett dataskyddsombud har utsetts ska den personuppgiftsansvarige rådfråga denne vid genomförande av en konsekvensbedömning samt dokumentera det som sker under bedömningen.

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

[3] För mer information om dataskyddsombudet hänvisas till PM om dataskyddsombud 170807

Det finns inget lagkrav på att konsekvensanalysen ska publiceras. Artikel 29-gruppen menar dock att det kan finnas andra skäl till varför hela eller delar av konsekvensbedömningen bör publiceras, bland annat för att agera transparent gentemot den registrerade.

Datainspektionen ska informeras i följande fall:

- När det föreligger en hög risk med personuppgiftsbehandlingen
- När riskerna utgör sådant hot att en skada kan leda till förödande konsekvenser för den registrerade, det är tydligt att risken kan uppstå samt när skadan inte kan repareras
- När den personuppgiftsansvarige inte ensam kan åtgärda risken
- När nationell lag kräver detta för utförande av vissa tjänster som utförs i det allmännas intresse.

Kravet på genomförande av konsekvensbedömning gäller behandlingar som är initierade efter den 25 maj 2018. Artikel 29-gruppen rekommenderar dock att redan innan maj påbörja arbetet med konsekvensbedömningar.

Vad konsekvensbedömningen ska innehålla

Konsekvensbedömningen ska enligt dataskyddsförordningen minst innehålla:

- Beskrivning av planerad personuppgiftsbehandling/ar samt ändamålet med behandlingarna
- Bedömning av nödvändighet och proportionalitet
- Bedömning av identifierade risker mot de registrerades rättigheter och friheter
- Åtgärder för att hantera risker
- Vidtagna åtgärder för att möta lagkraven

Undantag från kravet på konsekvensbedömning

Konsekvensbedömning är inte obligatorisk i följande fall:

- När personuppgiftsbehandlingen inte innebär en risk för registrerads rättigheter eller friheter
- När en konsekvensbedömning redan har gjorts för liknande behandling och kan appliceras på förevarande personuppgiftsbehandling

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se

- När behandlingen har en rättslig grund och det har stadgats att en konsekvensbedömning inte är nödvändig
- När konsekvensbedömningen inte ansetts obligatorisk av tillsynsmyndigheten.

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
Stockholm.se