Försäkringskassan

RÄTTSLIGT STÄLLNINGSTAGANDE

Beslutsdatum
2021-10-29

Vår beteckning
Dnr FK 2021/010931

Serienummer
2021:10

Konsekvensbedömning enligt artikel 35 EU:s dataskyddsförordning – behov av ställningstagande i olika frågor

Försäkringskassans ställningstaganden

Innan en behandling av personuppgifter påbörjas ska den personuppgiftsansvarige överväga om en konsekvensbedömning enligt artikel 35 i EU:s dataskyddsförordning (nedan dataskyddsförordningen)[1] behövs. Detsamma gäller för pågående behandlingar för vilka övervägande om konsekvensbedömningar inte har gjorts tidigare, eller för de fall en pågående behandling eller riskerna med en sådan ändras.

Övervägandet består av en inledande[2] riskanalys som ska svara på om behandlingen sannolikt leder till en hög risk för enskildas fri- och rättigheter.[3]

Begreppet *hög risk* i artikel 35 dataskyddsförordningen ska enligt Försäkringskassan förstås som en hög tröskel, antingen genom att skadan är mer trolig, mer allvarlig eller en kombination av de båda. Hög risk kan röra sig om en isolerad risk som i sig bedöms som hög, eller flera risker som tillsammans bedöms vara höga.

När en riskanalys genomförs, inom ramen för övervägandet om en konsekvens-bedömning behöver genomföras, ska hänsyn tas till de tekniska och organisatoriska säkerhetsåtgärder som kan komma att reducera eller eliminera de identifierade riskerna.

En behandling av personuppgifter ska sannolikt anses leda till hög risk om det bedöms föreligga en tämligen stor risk för att behandlingen leder till höga risker.

Undantaget från att göra konsekvensbedömningar i artikel 35.10 dataskydds-förordningen ska inte tillämpas i de fall behandlingen av personuppgifterna stöder sig på 114 kap. socialförsäkringsbalken (SFB).

Bakgrund och överväganden

Dataskyddsförordningen lägger ett stort ansvar på den personuppgiftsansvarige för de personuppgifter denne behandlar. Den s.k. riskbaserade metoden, som löper som en röd tråd genom dataskyddsförordningen, är central när det gäller den personuppgifts-ansvariges behandling av personuppgifter.

---

[1] 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)
[2] Skilj från den mer fördjupade riskanalysen som sker i konsekvensbedömningen.
[3] Se Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02): https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:sv:PDF

Den riskbaserade metoden innebär att den personuppgiftsansvarige har ansvar för att utvärdera de risker som en viss personuppgiftsbehandling innebär samt att därefter vidta lämpliga åtgärder som på ett godtagbart sätt tillförsäkrar individers friheter och rättigheter. Metoden utgör kärnan i principen om ansvarsskyldighet, vilken framgår av bl.a. artikel 5.2.

Principen om ansvarsskyldighet får genomslag genom artikel 24, där den personuppgiftsansvariges generella ansvar fastställs. I artikeln anges att den personuppgiftsansvarige är skyldig att implementera lämpliga tekniska och organisatoriska åtgärder i syfte att kunna säkerställa och visa upp att behandlingen uppfyller kraven i dataskyddsförordningen. Den allmänna skyldigheten att implementera lämpliga tekniska och organisatoriska åtgärder följs av artiklar av mer praktisk karaktär. Dessa har också koppling till behandlingens risker. Frågan är då vad som kan sägas utgöra risk.

Rent allmänt kan begreppet risk ses som en funktion av sannolikheten för att en viss händelse inträffar och konsekvensen av att denna händelse inträffar. I dataskydds-förordningen finns ingen entydig och uttrycklig definition av vad som inryms i begreppet risk. Där delas risken in i olika svårighetsgrader, vilket också kommer till uttryck i de olika artiklarna. Exempelvis tar artikel 35 dataskyddsförordningen sikte på hög risk.

Bestämmelser om säkerhet i samband med behandlingen av personuppgifter är också kopplade till den identifierade risken. Dessa skyldigheter är kopplade till en av de grundläggande principerna för personuppgiftsbehandling[4]. Artikel 32 stadgar en generell skyldighet att säkerställa att personuppgifter behandlas på ett säkert sätt.[5]

Behovet av klargörande

I artikel 35 dataskyddsförordningen ställs krav på att den personuppgiftsansvarige genomför en konsekvensbedömning för sådana personuppgiftsbehandlingar som *sannolikt leder till hög risk* för fysiska personers rättigheter och friheter[6]. Varken dataskyddsförordningen, Integritetsskyddsmyndigheten (IMY) eller praxis ger någon tydlig ledning i fråga om hur en personuppgiftsansvarig ska förfara för att avgöra behovet av en konsekvensbedömning. Det behöver därför klargöras hur Försäkringskassan i sin verksamhet ska förhålla sig till nämnda artikel.

Det behöver skapas en större medvetenhet om dataskydd och risker med person-uppgiftsbehandling i Försäkringskassans verksamhet, vilket bl.a. inbegriper kunskap om när en konsekvensbedömning behöver göras och vad en sådan ska omfatta.

Försäkringskassan kan bli föremål för sanktionsavgift om en konsekvensbedömning inte utförs när det behövs eller om en sådan utförs på ett felaktigt sätt.

---

[4] Se artikel 5.1 f dataskyddsförordningen rörande principen om integritet och konfidentialitet

[5] I artikeln anges att den personuppgiftsansvarige, och i tillämpliga fall även personuppgiftsbiträdet, med hänsyn till den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter, ska vidta tekniska och organisatoriska säkerhetsåtgärder för att säkerställa den säkerhetsnivå som är lämplig för den aktuella behandlingen. I korthet handlar detta om att ju högre risken är desto starkare skyddsåtgärder krävs.

[6] Se även skäl 84 dataskyddsförordningen.

När ska en konsekvensbedömning göras?

För att en personuppgiftsansvarig ska kunna avgöra vilka skyldigheter som träffar en viss behandling måste en bedömning inledningsvis göras av vilka risker den aktuella behandlingen innebär. En sådan bedömning görs genom en riskanalys. Genom den inledande riskanalysen ska den personuppgiftsansvarige först bedöma om det överhuvudtaget föreligger en risk, och i nästa steg, nivån av den identifierade risken.

Nivån av risken bedöms utifrån graden av sannolikhet och allvar. I skäl 75 dataskyddsförordningen preciseras vilka händelser som kan innebära skada för de registrerade, och som därför utgör en risk för deras friheter och rättigheter.

Behandlingar som sannolikt innebär en hög risk medför särskilda skyldigheter för den personuppgiftsansvarige. Ett sådant exempel är skyldigheten att enligt artikel 35 dataskyddsförordningen utföra konsekvensbedömningar.

Av ordalydelsen i artikel 35.1 och skäl 76 dataskyddsförordningen får anses följa att det krävs en riskbedömning (riskanalys) för att avgöra om en konsekvensbedömning behöver göras. En konsekvensbedömning ska inte göras slentrianmässigt, utan enbart i de fall en behandling sannolikt leder till hög risk för enskildas rättigheter och friheter. Om en personuppgiftsansvarig, i detta fall Försäkringskassan, mer regelmässigt tvingas göra konsekvensbedömningar skulle det leda till en betungande resursavsättning. Det kan enligt vår bedömning inte anses vara i enlighet med lagstiftarens intentioner.

Enligt Försäkringskassan bör stor vikt läggas på en inledande riskanalys för att överväga om en konsekvensbedömning behöver göras. I övervägandet görs bedömningen om det sannolikt föreligger en hög risk för enskildas fri- och rättigheter. Ett övervägande om konsekvensbedömning ska göras innan en behandling påbörjas, om en pågående behandling ändras och för en pågående behandling där ett övervägande om konsekvensbedömning inte tidigare har genomförts.

Vad är skillnaden mellan den inledande riskanalysen och en konsekvensbedömning?

En konsekvensbedömning innebär en mer fördjupad riskbedömning jämfört med den inledande riskanalysen som görs i övervägandet. Konsekvensbedömning är en pågående process som omfattar en redogörelse för, och bestämmande av, lämpliga åtgärder i syfte att minimera risker. En konsekvensbedömnings syfte är alltså, till skillnad från den inledande riskanalysen, att på ett djupare plan bedöma om en hög risk verkligen föreligger för en viss behandling och hur risken ska hanteras. För att förenkla kan man säga att övervägandet handlar om att identifiera riskerna och bedöma hur sannolikt det är för att dessa ska inträffa, medan konsekvensbedömningen handlar om att hantera de risker som redan har identifierats under övervägandet.

Den inledande riskanalysen i övervägandet

Den inledande riskanalysen, som syftar till att bedöma om en konsekvensbedömning behöver göras, måste ta sin utgångspunkt i personuppgiftshanteringen. Enligt Försäkringskassan ska fokus ligga på att dels inventera de olika risker som kan

uppkomma, dels bedöma de potentiella skador individen kan utsättas för. I riskanalysen ska såväl materiella som immateriella skador beaktas.[7]

Den behandlingen av personuppgifter som riskanalysen tar sikte på är den totala behandlingen som kan överblickas. Det är svårt att sätta exakta gränser för detta, utan det får avgöras från fall till fall. Handlar det om ett nytt it-stöd får man inkludera all den hantering av personuppgifter som kommer att ske i stödet. Det kan exempelvis röra enskilda försäkrade och medarbetare. Behandling av personuppgifter behöver t.ex. ske för att bedöma och besluta om rätten till en förmån. Det som också kan komma att ingå i analysen är på vilket sätt personuppgifter lämnas ut.

Vad innebär hög risk?

När det gäller bedömningen av hög risk ger varken dataskyddsförordningen eller IMY någon vägledning för den personuppgiftsansvarige. Viss ledning kan dock ges av brittiska Information Commissioner´s Office (ICO) som publicerat information i frågan.[8]

För att bedöma om något innebär en hög risk är det enligt ICO klart att man måste beakta både sannolikheten och allvarligheten för eventuella skador på individer. Risk innebär enligt ICO en mer än avlägsen risk för skada, medan hög risk innebär en hög tröskel, antingen för att skadan är mer trolig, eller för att den potentiella skadan är mer allvarlig, eller en kombination av de två. Att bedöma potentialen för risk i den meningen är en del av konsekvensbedömningens uppgift.

ICO:s resonemang om hur risknivån ska bedömas är enligt Försäkringskassan rimligt. Att märka är att *en* risk, bland alla andra risker, kan vara särskilt hög. Den risken bör då bli utslagsgivande för om hög risk föreligger. För att konstatera att det kan föreligga hög risk måste man även ta hänsyn till det totala antalet risker med behandlingen. Flera mindre risker, som i sig kanske inte är höga, kan tillsammans i en sammantagen bedömning leda till en hög risk.

Vid bedömning av hög risk krävs en slags gradering, förslagsvis i form av olika nivåer; låg, medel eller hög risk.[9] Detta blir ett särskilt bedömningssteg i övervägandet.

När är det *sannolikt* att det föreligger en hög risk?

Efter att ha konstaterat att det föreligger en hög risk för en viss personuppgiftsbehandling handlar nästa steg om att bedöma hur sannolikt det är att den höga risken inträffar.

Av skäl 76 dataskyddsförordningen följer att hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art,

[7] Skäl 75 dataskyddsförordningen.

[8] Den 31 december 2020 trädde Storbritannien ut ur EU. Med tanke på att ICO:s guidelines publicerades när landet fortfarande var en medlemsstat, och då tolkningen som följer av dokumentationen fortfarande bör vara relevant trots utträdet, anser vi att materialet är att anse som en användbar källa. Se https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when1

[9] Dessa nivåer kan sägas motsvara de risknivåer som dataskyddsförordningens artiklar rörande risk ger uttryck för.

omfattning, sammanhang och ändamål. Däremot ges ingen ledning avseende hur den personuppgiftsansvariges bedömning av sannolikheten ska gå till i praktiken.

Sannolikhet är ett mått på hur troligt det är att en viss händelse inträffar.[10] Viss ledning kan ges av hur beviskravet ”sannolikt” bedöms inom juridiken. Enligt Diesen kan sannolikt jämföras med termen sannolika skäl, vilket han menar motsvarar 75 procents sannolikhet.[11] Det räcker alltså inte, ur den synvinkeln, att ett scenario verkar vara något troligare än ett annat för att nå upp till beviskravet sannolikt.

Enligt Försäkringskassan ska därför en behandling *sannolikt* anses leda till hög risk om det bedöms föreligga en tämligen stor risk för att behandlingen leder till höga risker. I praktiken blir det fråga om en uppskattning av den personuppgiftsansvarige om det är sannolikt att behandlingen leder till en hög risk, utifrån omständigheterna i det enskilda fallet.

Betydelsen av säkerhetsåtgärder i riskanalysen

Frågan är vidare om och i vilken mån säkerhetsåtgärder ska beaktas inom ramen för bedömningen om det är sannolikt att hög risk föreligger för en viss behandling.[12] Det kan handla om säkerhetsåtgärder som redan finns på plats eller som är direkt möjliga att införa. Om säkerhetsåtgärder ska beaktas i övervägandet framgår inte direkt av artikel 35 dataskyddsförordningen eller tillhörande skäl.

Enligt IMY kan dock frånvaro av säkerhetsåtgärder innebära hög risk för enskildas fri- och rättigheter.[13] Omvänt borde då gälla att tillgängliga säkerhetsåtgärder kan föra med sig att det inte längre är sannolikt att behandlingen leder till en hög risk för enskildas fri- och rättigheter, vilket skulle innebära att kravet på en konsekvensbedömning faller bort. Om åtgärder kan vägas in redan i övervägandet, kan det enligt Försäkringskassan få en avgörande betydelse för om en konsekvensbedömning ska göras eller inte.

Enligt Försäkringskassan ska man därför i övervägandet ta hänsyn till och bedöma vilka säkerhetsåtgärder som kan tänkas reducera eller eliminera de identifierade riskerna. Eftersom Försäkringskassan förfogar över ett flertal olika säkerhetsåtgärder skulle ett beaktande av dessa sannolikt leda till att ett mindre antal konsekvens-bedömningar behöver göras. I det fall osäkerhet råder i detta hänseende ska en konsekvensbedömning dock alltid göras.

Undantag från att göra en konsekvensbedömning

I artikel 35.10 dataskyddsförordnigen finns ett undantag som innebär att en personuppgiftsansvarig i vissa situationer inte behöver genomföra en konsekvens-bedömning, om denne inte anser det vara nödvändigt. Detta gäller när:

---

[10] Se vidare på Wikipedia, https://sv.wikipedia.org/wiki/Sannolikhetv för fördjupad information om sannolikhet i teorin

[11] Diesen, Christian, Bevis. 7, Bevisprövning i förvaltningsmål, 1. uppl., Norstedts juridik, Stockholm, 2003

[12] Det kan vara fråga om både tekniska och organisatoriska åtgärder. Säkerhetsåtgärder på personuppgiftsnivå är t.ex. åtkomstbegränsning, kryptering och pseudonymisering. På systemnivå kan det handla om säkerhetskopiering, kontroll av hårdvara, etc. Organisatoriska åtgärder består vanligtvis i processer och rutiner.

[13] Se vidare på IMY:s webbplats, https://www.imy.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/vem-maste-gora-en-konsekvensbedomning/

- behandlingen enligt artikel 6.1 c eller e har en rättslig grund i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, och den rätten reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder i fråga och
- en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund.

Regeringen har i samband med lagstiftningsarbetet inför införandet av dataskyddsförordningen uttalat att det inte är nödvändigt att den personuppgiftsansvarige gör ytterligare konsekvensbedömningar i de fall behandlingen av personuppgifter har stöd i befintliga registerförfattningar.[14]

Försäkringskassan anser att man inte kan stödja sig på regeringens uttalande när det gäller frågan om en konsekvensbedömning ska göras i fall då behandlingen vilar på bestämmelserna i 114 kap. SFB. Den lagstiftningen är föråldrad och i vissa delar svårtillämpad, vilket gör att bestämmelserna i en del fall kan behöva tolkas. Lagstiftaren har av naturliga skäl inte haft överblick över eller redogjort för val av tekniska lösningar. Dessutom sker behandlingar över tid med ny teknik. Risker kan lätt uppstå, exempelvis när redan insamlade uppgifter behandlas för nya ändamål eller att de används i en ny kontext.

Sammanfattningsvis kan Försäkringskassan inte tillämpa undantaget i artikel 35.10 dataskyddsförordningen när en personuppgiftsbehandling sker med stöd av 114 kap. SFB. Det måste alltså även i dessa fall göras en inledande riskanalys.

Aktuella bestämmelser, rättspraxis m.m.

Författningar

Artikel 5, 24, 32 och 35 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).

Europiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)

Förarbeten m.m.

Skäl 75,76 och 84 dataskyddsförordningen.

Anpassningar av registerförfattningar på arbetsmarknadsområdet till EU:s dataskyddsförordning, Regeringens lagrådsremiss, 11 januari 2018

[14] Se Lagrådsremissen Anpassningar av registerförfattningar på arbetsmarknadsområdet till EU:s dataskyddsförordning, s. 32

Myndighetspublikationer

Information Commissioner´s Office, *Guide to the General Data Protection Regulations (GDPR), Data Protection Impact Assessments* - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when1

Integritetsskyddsmyndighetens officiella webbplats, http://www.imy.se

Doktrin

Diesen, Christian, *Bevis. 7, Bevisprövning i förvaltningsmål*, 1. uppl., Norstedts juridik, Stockholm, 2003

Mänskliga rättigheter, diskriminering, jämställdhet och barnrätt

Det rättsliga ställningstagandet bedöms inte påverka något perspektiv inom dessa områden.

Mikael Westberg

Martina Palmgren