Beslut om förteckning enligt artikel 35.4 i EU:s allmänna dataskyddsförordning 2016/679

Beslut

Datainspektionen beslutar i enlighet med artikel 35.4 i EU:s allmänna dataskyddsförordning (dataskyddsförordningen) bilagda förteckning över personuppgiftsbehandling som omfattas av krav på konsekvensbedömning avseende dataskydd.

Förteckningen kompletterar och specificerar artikel 35.1 och är avsedd att närmare exemplifiera när förutsättningarna i den bestämmelsen kan anses vara uppfyllda. Förteckningen är inte avsedd att på ett uttömmande sätt ange när en konsekvensbedömning måste göras. Förteckningen avser behandling av personuppgifter oavsett om behandlingen sker enbart i Sverige eller är gränsöverskridande.

Förteckningen ska publiceras på Datainspektionens webbplats.

Bakgrund

Enligt artikel 35.1 i dataskyddsförordningen ska en konsekvensbedömning avseende dataskydd göras innan en typ av personuppgiftsbehandling inleds om behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Enligt artikel 35.4 ska tillsynsmyndigheten upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på sådan konsekvensbedömning. Förteckningen ska översändas till den Europeiska dataskyddsstyrelsen (EDPB). Om förteckningen innefattar gränsöverskridande behandling av personuppgifter ska EDPB först yttra sig över utkastet till förteckning innan den antas av tillsynsmyndigheten.

Datainspektionen skickade den 11 juli 2018 över ett utkast till EDPB i enlighet med det förfarande som styrelsen beslutat om. Syftet med förfarandet är att få till stånd en enhetlig tillämpning av artikel 35.1 i dataskyddsförordningen. EDPB har yttrat sig över Datainspektionens (och flera andra nationella dataskyddsmyndigheters) utkast den 2 oktober 2018. I yttrandet över Datainspektionens utkast anförde EDPB två synpunkter som båda avsåg ett behov av förtydligande om att förteckningen, i sin helhet respektive i ett specifikt exempel, grundar sig på de riktlinjer som Artikel 29-gruppen tidigare tagit fram avseende konsekvensbedömning.[1] EDPB hade inte i övrigt några invändningar mot utkastet till förteckning men betonade generellt att de förteckningar som ges in till EDPB för yttrande ska tolkas som att de närmare specificerar artikel 35.1 och att de inte kan vara uttömmande.

Datainspektionen har ändrat utkastet till förteckning i enlighet med EDPB:s synpunkter om tydligare hänvisning till Artikel 29-gruppens riktlinjer och har meddelat EDPB att man avser att följa deras yttrande.

Datainspektionen har också i juli 2018 skickat utkastet till förteckning på remiss till ett antal organisationer i Sverige för synpunkter. En lista över remissinstanser finns med som bilaga till beslutet. De synpunkter som kommit in redovisas nedan.

Beredning av ärendet

Den förteckning som Datainspektionen tagit fram hänvisar till de kriterier som Artikel 29-gruppen redovisat i sina riktlinjer om konsekvensbedömning (WP 248 rev. 01). I förteckningen anges att en konsekvensbedömning ska göras om personuppgiftsbehandlingen uppfyller minst två av de kriterierna. Som ett tillägg till förteckningen finns också uppräknat ett antal exempel när två av kriterierna kan anses vara uppfyllda.

Datainspektionen har, efter att EDPB yttrat sig över utkastet, svarat att man avser att rätta sig efter EDPB:s synpunkter och har därefter vidtagit nödvändiga ändringar. Inom ramen för EDPB:s yttrande har Datainspektionen också vidtagit några ändringar efter synpunkter som inkommit i den remissomgång som redovisas nedan.

I den nationella remissomgången avseende Datainspektionens utkast till förteckning har 27 remissinstanser svarat, varav 14 har haft synpunkter på

[1] 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, senast reviderade och antagna den 4 oktober 2017, WP 248 rev. 01

utkastet. De synpunkter som kommit in kan fördelas inom olika områden enligt vad som anges nedan.

Förteckningens rättsliga status och förhållandet till Artikel 29-gruppens riktlinjer
Några remissinstanser, däribland Advokatsamfundet, Post- och telestyrelsen och Transportstyrelsen, har efterlyst klargörande av förteckningens rättsliga status och vad som ska gälla om det finns en diskrepans mellan förordningens krav på konsekvensbedömning i artikel 35.1 och Datainspektionens förteckning eller Artikel 29-gruppens riktlinjer. Sveriges Kommuner och Landsting har avstyrkt förslaget huvudsakligen på grund av att förteckningen är för otydlig och att de olika kriterierna är för vida.

Datainspektionen vill i detta sammanhang förtydliga att en konsekvensbedömning alltid ska göras om en viss typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Det följer direkt av artikel 35.1 i dataskyddsförordningen. Den förteckning som ska tas fram enligt artikel 35.4 kompletterar och specificerar förordningens bestämmelser men den tar inte över bestämmelsen i artikel 35.1 och den kan inte vara uttömmande. Det har också EDPB uttalat i de yttranden som man lämnat över olika dataskyddmyndigheters förteckningar. En konsekvensbedömning kan därför behöva göras inför en behandling som sannolikt innebär en hög risk trots att bara ett kriterium bedöms föreligga. På motsvarande sätt kan den personuppgiftsansvarige göra bedömningen att behandlingen i det specifika fallet sannolikt inte leder till en hög risk även om två eller flera av kriterierna är uppfyllda. I ett sådant fall bör dock den personuppgiftsansvarige motivera och dokumentera skälet till att en konsekvensbedömning inte bedömts nödvändig. Datainspektionen har infört formuleringar som är avsedda att förtydliga detta i förteckningen.

För att bemöta synpunkterna om otydlighet i förhållandet mellan Artikel 29-gruppens kriterier och de exempel som räknas upp i förteckningen, har Datainspektionen lagt till en tydligare hänvisning till Artikel 29-gruppens riktlinjer och ett uttryckligt uttalande om att de exempel som räknas upp är avsedda att komplettera och specificera vägledningen. Vid varje exempel har förts in en hänvisning till vilka kriterier som kan anses uppfyllda i respektive situation, också det för att förtydliga och förklara kopplingen mellan Artikel 29-gruppens riktlinjer och Datainspektionens förteckning.

Formulering av de olika kriterierna
Några remissinstanser har haft synpunkter på formuleringen av de olika kriterierna. Till exempel har Lantmäteriet, Transportstyrelsen och Svenska Bankföreningen framfört synpunkter om att punkt 6 (samkörning av register

m.m.) mer korrekt bör avspegla Artikel 29-gruppens riktlinjer och bör specificeras, till exempel genom att det bör framgå att det är den registrerades *rimliga* förväntningar som avses. Datainspektionen har därför formulerat om texten i denna del. Svenska Bankföreningen, Bisnode, SKL och Transportstyrelsen har anfört att det behöver förtydligas vad som menas med behandling ”i stor omfattning” i punkt 5. I yttranden över de utkast som innehållit en närmare definition av begreppet, till exempel genom att ange ett visst antal registrerade, har EDPB ansett att de faktorer som Artikel 29-gruppen tagit fram i sina riktlinjer kring tolkning av begreppet är tillräckliga och att någon hänvisning till andra faktorer inte ska göras. Datainspektionen har därför avstått från att närmare försöka definiera begreppet ”i stor omfattning” i förteckningen utöver hänvisning till Artikel 29-gruppens riktlinjer.

Formulering av de olika exemplen
Svenska Bankföreningen och Finansinspektionen har beträffande exemplet som avser bankers och försäkringsbolags kontroll mot sanktionslistor framfört att sådana kontroller utgör en rättslig skyldighet och att det därför kan ifrågasättas om en konsekvensbedömning regelmässigt ska krävas. Datainspektionen anser att frågan om huruvida en konsekvensbedömning ska krävas i detta fall måste bedömas både utifrån den rättsliga skyldigheten att göra sådana kontroller och utifrån det sätt på vilket kontrollen utförs och vilken slags personuppgiftsbehandling det innebär. Det är därför inte lämpligt att ange ett exempel som går ut på att konsekvensbedömning regelmässigt krävs vid kontroll mot sanktionslistor. Exemplet ska därför tas bort. Kravet på konsekvensbedömning kan i vissa fall ändå följa direkt av förordningen och av de kriterier som anges i förteckningen. En enkel kontroll mot en sanktionslista av någon som har en rättslig skyldighet att göra en sådan kontroll bör inte kräva konsekvensbedömning medan en mer komplicerad samkörning av olika register kan kräva en sådan bedömning.

Undantag för lagreglerad personuppgiftsbehandling i artikel 35.10
Svenskt Näringsliv, Bisnode och Lantmäteriet har efterlyst en närmare redogörelse för förhållandet till artikel 35.10. I denna artikel finns ett undantag från kravet på konsekvensbedömning för sådan personuppgiftsbehandling som grundar sig på nationell rätt eller EU-rätt. Undantaget gäller endast i den mån den nationella rätten eller EU-rätten reglerar den specifika behandlingsåtgärden eller serien av åtgärder och då en konsekvensbedömning avseende dataskydd har gjorts i samband med att lagstiftningen beslutades. Datainspektionen har i förteckningen tagit in en hänvisning till denna undantagsbestämmelse. När det gäller kreditupplysningsverksamhet har framförts att sådan verksamhet skulle kunna falla under undantaget i 35.10. För att undantaget ska vara aktuellt

krävs dock att inte bara verksamheten utan även själva personuppgiftsbehandlingen är reglerad. Den personuppgiftsbehandling som sker i kreditupplysningsverksamhet är till viss del reglerad i kreditupplysningslagen (1973:1173) men det anges uttryckligen att bestämmelserna kompletterar EU:s allmänna dataskyddsförordning. Förordningen gäller alltså fortfarande, vid sidan av kreditupplysningslagen, för den personuppgiftsbehandling som sker i kreditupplysningsverksamhet. Mot bakgrund av den omfattande behandling av personuppgifter som kreditupplysningsverksamhet kan innebära bedömer Datainspektionen att kreditupplysningslagen inte reglerar de specifika behandlingsåtgärder som kan uppstå i kreditupplysningsverksamhet på det sätt som krävs enligt artikel 35.10. Datainspektionen har därför valt att behålla detta som ett exempel utifrån de kriterier som Artikel 29-gruppen tagit fram.

Behov av ytterligare exempel på situationer där konsekvensbedömning ska göras

Flera remissinstanser (Advokatsamfundet, Migrationsverket och Domstolsverket) har pekat på ytterligare situationer där kravet på konsekvensbedömning borde gälla. Datainspektionen vill i detta sammanhang betona att en konsekvensbedömning alltid ska ske innan man påbörjar en behandling eller en serie av behandlingsåtgärder om det sannolikt kan leda till en hög risk för fysiska personers fri- och rättigheter. Den nu framtagna förteckningen har inte för avsikt att på ett uttömmande sätt ange när en konsekvensbedömning ska göras och kan komma att ses över och kompletteras senare. Två remissinstanser (Svenskt Näringsliv och Transportstyrelsen) har också pekat på behovet av att ta fram förteckningar där konsekvensbedömningar inte krävs enligt artikel 35.5. Någon sådan förteckning är inte aktuell för närvarande men kan komma att övervägas senare.

Skäl för beslutet

Datainspektionen har tagit fram ett utkast till förteckning över när en konsekvensbedömning enligt artikel 35.1 dataskyddsförordningen krävs och berett denna enligt ovan. Utkastet har underställts EDPB i enlighet med artikel 64.1 (a) i förordningen och de synpunkter som EDPB har framfört har tagits om hand.

Datainspektionen kan därmed besluta den bilagda förteckningen.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Elisabeth Jilderyd. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom deltagit.

Lena Lindgren Schelin

Elisabeth Jilderyd