Förteckning enligt artikel 35.4 i Dataskyddsförordningen

Av artikel 35.1 i dataskyddsförordningen följer att den personuppgiftsansvarige ska utföra en konsekvensbedömning om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Konsekvensbedömningen ska som huvudregel utföras innan en behandling påbörjas.

Den personuppgiftsansvarige måste alltid göra en självständig bedömning av den planerade behandlingen för att avgöra om en konsekvensbedömning är nödvändig i det enskilda fallet.

Skyldigheten enligt artikel 36 att samråda med Datainspektionen har koppling till skyldigheten att göra en konsekvensbedömning enligt artikel 35. Det bör dock observeras att skyldigheten att begära förhandssamråd hos Datainspektionen endast gäller om konsekvensbedömningen visar att behandlingen skulle leda till en hög risk och denna risk inte kan avhjälpas genom att den personuppgiftsansvarige vidtar lämpliga åtgärder för att minska risken.

I artikel 35.3 anges vissa situationer när en konsekvensbedömning krävs. Därutöver ska tillsynsmyndigheten enligt artikel 35.4 upprätta och offentliggöra en förteckning över behandlingar som kräver en sådan bedömning.

Datainspektionen har, med ledning av riktlinjer från Artikel 29-arbetsgruppen och de kriterier som gruppen tagit fram[1], antagit nedanstående förteckning över när en konsekvensbedömning ska göras.

En konsekvensbedömning ska göras om minst två av de nedanstående punkterna finns med i den planerade behandlingen. I slutet av förteckningen anges också några exempel på när minst två av kriterierna ska anses föreligga och en konsekvensbedömning alltså måste göras. Förteckningen återger de kriterier som Artikel 29-gruppen tagit fram i sin vägledning och innehåller exempel som är avsedda att komplettera och specificera vägledningen.

Förteckningen är dock inte uttömmande och kan komma att uppdateras och kompletteras med fler exempel framöver. Förteckningen gäller oavsett om det är fråga om personuppgiftsbehandling enbart i Sverige eller behandling av personuppgifter som är att anse som gränsöverskridande enligt definitionen i dataskyddsförordningen artikel 4.23.

Det krävs inte någon konsekvensbedömning för behandlingar som har kontrollerats av en tillsynsmyndighet eller ett dataskyddsombud i enlighet med artikel 20 i direktiv 95/46/EG och vars genomförande inte har ändrats sedan föregående kontroll. Som en god praxis bör dock en konsekvensbedömning ses över kontinuerligt och utvärderas regelbundet.

Om en behandling enligt artikel 6.1 c eller e har en rättslig grund i EU-rätten eller svensk lag, om denna lagstiftning reglerar den specifika behandlingsåtgärden och om en konsekvensbedömning har genomförts som en del av fastställandet av denna rättsliga grund, krävs som utgångspunkt inte någon ytterligare konsekvensbedömning enligt artikel 35.10. En bedömning som görs under utarbetandet av lagstiftningen kan dock behöva ses över om den antagna lagstiftningen skiljer sig från förslaget på sätt som påverkar integriteten och frågor som rör uppgiftsskydd.

[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.
 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Förteckning över när en konsekvensbedömning ska göras enligt artikel 35(4)

Utöver de situationer som anges i artikel 35.3, och med beaktande av undantaget i artikel 35.10, ska en konsekvensbedömning avseende dataskydd göras om den planerade behandlingen uppfyller minst två av följande kriterier:

1. utvärderar eller poängsätter människor, till exempel ett företag som erbjuder genetiska tester till konsumenter för att bedöma och förutse risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare
2. behandlar personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade
3. systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer
4. behandlar känsliga personuppgifter enligt artikel 9[2] eller uppgifter som är av mycket personlig karaktär, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter
5. behandlar personuppgifter i stor omfattning
6. kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man samkör register
7. behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter
8. använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT)
9. behandlar personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

Att utföra en konsekvensbedömning är obligatoriskt endast om behandlingen ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1, illustrerat av artikel 35.3 och kompletterat av artikel 35.4) En

[2] Med känsliga uppgifter avses enligt artikel 9 bland annat biometriska uppgifter som behandlas för att entydigt identifiera en fysisk person.

behandling kan uppfylla två eller flera av ovanstående kriterier men den personuppgiftsansvarige kan ändå göra bedömningen att den ”sannolikt inte leder till en hög risk”. I sådana situationer bör den personuppgiftsansvarige motivera och dokumentera anledningarna till att en konsekvensbedömning inte utförs och inkludera dataskyddsombudets synpunkter.

Exempel på behandlingar som kräver att konsekvensbedömning utförs (notera att det inte är en uttömmande uppräkning)

Inom arbetslivet

- En arbetsgivare övervakar systematiskt hur de anställda använder internet och e-post (kriterium 3 och 7).

- En arbetsgivare inför ett inpasseringssystem för anställda som innefattar behandling av biometriska uppgifter i syfte att identifiera en viss fysisk person, t.ex. fingeravtrycksavläsning (kriterium 3, 7 och 8).
- En organisation inför ett gemensamt system i vilket det är möjligt att anmäla missförhållanden på arbetsplatsen – ett s.k. visselblåsarsystem (kriterium 4 och 7)
- Rekryteringsföretag som inrättar kandidat- eller kompetensdatabaser. (kriterium 1 och 4)
- Verksamheter som utför bakgrundskontroller inför rekryteringar. (kriterium 1,4 och 6)

Marknadsföring

- Ett företag använder kunders lokaliseringsuppgifter, som till exempel inhämtas via en mobilapp, i syfte att rikta marknadsföring till kunden eller planera sina marknadsföringsstrategier (kriterium 3 och 4.)
- Ett företag inhämtar uppgifter från sociala medier för att profilera fysiska personer och därefter rikta marknadsföring till vissa utvalda grupper. (kriterium 1 och 3)
- En sökmotor på internet samlar in uppgifter om enskilda som använder tjänsten för att skapa kundprofiler och rikta marknadsföring (kriterium 1 och 3).

Känsliga personuppgifter

- Verksamheter som erbjuder genetiska tester till människor för att bedöma och förutse risker för sjukdomar eller hälsotillstånd eller ge besked om etniskt ursprung. (kriterium 1 och 4)
- Vårdgivares behandling av personuppgifter om patienter i annat än ringa omfattning. Exempel på ringa omfattning är när en läkare är ensam verksamhetsutövare och behandlar uppgifter om sina

patienter. (kriterium 4, 5 och 7)
- Behandling, innefattande lagring i arkiveringssyfte, av pseudonymiserade känsliga personuppgifter som rör registrerade från forskningsprojekt eller kliniska prövningar. (kriterium 4 och 7).
- Verksamheter som samlar in och lagrar känsliga personuppgifter som ska utgöra underlag för urval för framtida forskningsändamål. (kriterium 4 och 7)

Övrigt privat sektor
- En bank eller annat kreditinstitut som fattar automatiserade beslut som avser om en kredit ska beviljas eller inte (kriterium 1, 2 och 9)
- Ett företag behandlar ekonomiska uppgifter om fysiska personer i stor omfattning för att kunna lämna ut dessa till andra aktörer för kreditupplysningsändamål (kreditupplysningsverksamhet). (kriterium 4 och 9)
- Ett företag som tillhandahåller en plattform för kommunikation (sociala medier) - riktad till allmänheten och där användarna själva kan publicera text, bild eller ljud – och samlar in detaljerade uppgifter om användningen av tjänsten. (kriterium 3 och 5)
- Ett företag som i stor omfattning behandlar uppgifter om kunders tidigare misskötsamhet (en s.k. svart lista) i syfte att avgöra om personen ska få återkomma som kund eller inte. (kriterium 4, 5 och 9)

Offentlig sektor
- En kommun samlar in personuppgifter innefattande bland annat lokaliseringsuppgifter i syfte att använda dessa vid exempelvis stads- och trafikplanering. (kriterium 3, 4 och 5)
- Behandling av barns personuppgifter i skolverksamhet, om det är ett större antal registrerade. (kriterium 5 och 7)
- En kommun som behandlar personuppgifter i social omsorg, om det är ett större antal registrerade. (kriterium 4, 5 och 7)
- En myndighet som, enskilt eller tillsammans med andra personuppgiftsansvariga, genom digitala plattformar ger service till befolkningen, vilket leder till storskalig personuppgiftsbehandling. (kriterium 4, 5 och 8)

Teknik
- Ett företag som tillhandahåller internetuppkopplade produkter för konsumenters bostäder (smarta hem-produkter), till exempel för att kunna fjärrstyra uppvärmning, belysning eller ljuduppspelning, samlar in detaljerade uppgifter om hur kunderna använder tjänsterna (kriterium 3, 4 och 8)
- Verksamheter inom social omsorg som använder välfärdsteknik, t.ex.

robotar eller kamerabevakning, i människors boenden. (kriterium 3, 4 och 8)

- Verksamheter som använder ett system för intelligent videoanalys för att skilja ut bilar och automatiskt känna igen registreringsskyltar i syfte att övervaka körbeteendet på motorvägar. (kriterium 3, 4 och 8)
- Ett parkeringsbolag som använder kamerabevakning som kan skilja ut registreringsnummer i syfte att debitera parkeringsavgifter. (kriterium 3 och 8)
- Verksamheter som samlar in personuppgifter, innefattande bland annat lokaliseringsuppgifter, som uppkommer genom användning av smarta bilar, t.ex. för att utveckla tekniken. (kriterium 3, 4 och 8)
- Installation av smarta elmätare hos elabonnenter för att kunna ta fram, överföra och analysera uppgifter som rör konsumenter på en detaljerad nivå. (kriterium 3 och 8)
- Verksamheter som gör stora ändringar i sin tekniska infrastruktur och som behandlar personuppgifter inom exempelvis hälso- och sjukvård eller social omsorg. (kriterium 4, 7 och 8)