IMY. Integritetsskydds myndigheten

Vägledning vid konsekvensbedömning

Rättsligt tolkningsstöd

Bilaga till *En praktisk guide*

Februari 2025

IMY. Vägledning vid konsekvensbedömning – Rättsligt tolkningsstöd
Har du frågor om innehållet kontakta Integritetsskyddsmyndigheten,
telefon 08-657 61 00, e-post imy@imy.se,
eller besök www.imy.se

Innehåll

1. Ansvaret för konsekvens-bedömningen

Den *personuppgiftsansvarige*[1] har det yttersta ansvaret för att kraven i dataskydds-förordningen[2] och annan dataskyddslagstiftning uppfylls. Det följer av principen om ansvarsskyldighet som kommer till uttryck i artikel 5.2 i dataskyddsförordningen. I ansvaret ingår även att genomföra lämpliga tekniska och organisatoriska åtgärder samt att säkerställa en säkerhetsnivå som är lämplig i förhållande till behandlingens risk för fysiska personers rättigheter och friheter.

Den personuppgiftsansvarige ska säkerställa att en konsekvensbedömning avseende dataskydd genomförs när det är obligatoriskt, och att den genomförs och följs upp på ett godtagbart sätt. Den eller de personer som i praktiken utför själva konsekvens-bedömningen, eller eventuella åtgärder med anledning av den, kan vara personer inom eller utom organisationen.

Eventuella *personuppgiftsbiträden*[3] ska bistå den personuppgiftsansvarige med att se till att skyldigheten att genomföra konsekvensbedömning enligt artikel 35 i dataskydds-förordningen fullgörs, med hänsyn till typen av behandling och den information som personuppgiftsbiträdet har tillgång till.[4] Ansvaret för personuppgiftsbiträdet ska vara reglerat i personuppgiftsbiträdesavtalet.

Den personuppgiftsansvarige ansvar även för att säkerställa att *dataskyddsombudet*, om ett sådant finns, får korrekt och tillräcklig information om behandlingen och processen för att kunna utföra sina uppgifter enligt dataskyddsförordningen.

Fördjupad information
Avsnitt 6. Dataskyddsombudets roll i konsekvensbedömningen

1 Enligt artikel 4.7 i dataskyddsförordningen är en personuppgiftsansvarig en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
2 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).
3 Enligt artikel 4.8 i dataskyddsförordningen är ett personuppgiftsbiträde en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
4 Artikel 28.3 f i dataskyddsförordningen.

2. Metod och dokumentation

Det finns vissa uttryckliga krav som den personuppgiftsansvarige måste uppfylla under arbetet med en konsekvensbedömning och vissa minimikrav på innehållet i den.[5] Det finns dock ingen bestämd metod för hur en konsekvensbedömning ska genomföras. Det är därför upp till den personuppgiftsansvarige att välja en metod som uppfyller kraven enligt dataskyddsförordningen, utifrån exempelvis vilken typ av behandling som är aktuell och vilken verksamhet som utför behandlingen.

Europeiska dataskyddsstyrelsen (EDPB) har uttalat att det gällande konsekvensbedömningars ”exakta struktur och form” finns en flexibilitet, men att en konsekvensbedömning alltid (oberoende av form) ska vara en genuin riskbedömning som gör det möjligt för personuppgiftsansvariga att vidta åtgärder för att hantera riskerna.[6] EDPB har i bilaga 2 till sina riktlinjer om konsekvensbedömning tagit fram kriterier som kan användas av personuppgiftsansvariga för att bedöma om en konsekvensbedömning, eller en metod för att utföra en konsekvensbedömning, är tillräcklig för att uppfylla dataskyddsförordningens krav. EDPB anser att den metod som väljs bör överensstämma med dessa kriterier.[7] IMY:s vägledning vid konsekvensbedömning och förslag på tillvägagångssätt överensstämmer med kraven i dataskyddsförordningen och med EDPB:s kriterier. Sådant metodstöd som har tagits fram i enlighet med branschpraxis kan också vara användbart för att anpassa konsekvensbedömningen till verksamhetens branschspecifika särdrag.

Det finns inga bestämda krav på hur detaljerad dokumentationen av konsekvensbedömningen ska vara. Dokumentationen måste anpassas utifrån aktuella omständigheter, exempelvis den aktuella behandlingen, organisationens resurser och befintliga processer. Enligt principen om ansvarsskyldighet ska den personuppgiftsansvarige kunna visa att dataskyddsförordningen efterlevs. Det innebär att konsekvensbedömningen ska dokumenteras på ett godtagbart sätt. Dokumentationen bör utföras på ett sätt som möjliggör för tillsynsmyndigheten att kontrollera att minimikraven enligt artikel 35 i dataskyddsförordningen har uppfyllts och att övriga bestämmelser, som är aktuella inom ramen för den enskilda konsekvensbedömningen, följs.

5 Jfr artikel 35.2, 7–9 i dataskyddsförordningen. Skäl 90 till dataskyddsförordningen.
6 Artikel 29-arbetsgruppens *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 (WP 248, rev. 01), s. 19.
7 Jfr WP 248, s. 22.

3. Artikel 35 i dataskydds-förordningen

Bestämmelserna om konsekvensbedömning avseende dataskydd finns i artikel 35 i dataskyddsförordningen. Nedan återges artikeln i sin helhet.

Artikel 35 Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

2. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.

3. En konsekvensbedömning avseende dataskydd som avses i punkt 1 ska särskilt krävas i följande fall:

   a) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

   b) Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10.

   c) Systematisk övervakning av en allmän plats i stor omfattning.

4. Tillsynsmyndigheten ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd i enlighet med punkt 1. Tillsynsmyndigheten ska översända dessa förteckningar till den styrelse som avses i artikel 68.

5. Tillsynsmyndigheten får också upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som inte kräver någon konsekvensbedömning avseende dataskydd. Tillsynsmyndigheten ska översända dessa förteckningar till styrelsen.

6. Innan de förteckningar som avses i punkterna 4 och 5 antas ska den behöriga tillsynsmyndigheten tillämpa den mekanism för enhetlighet som avses i artikel 63 om en sådan förteckning inbegriper behandling som rör erbjudandet av varor eller tjänster till registrerade, eller övervakning av deras beteende i flera medlemsstater, eller som väsentligt kan påverka den fria rörligheten för personuppgifter i unionen.

7. Bedömningen ska innehålla åtminstone

   a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,

   b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,

   c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och

   d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

8. De berörda personuppgiftsansvarigas eller personuppgiftsbiträdenas efterlevnad av godkända uppförandekoder enligt artikel 40 ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av de behandlingar som utförs av dessa personuppgiftsansvariga eller personuppgiftsbiträden, framför allt när det gäller att ta fram en konsekvensbedömning avseende dataskydd.

9. Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.

10. Om behandling enligt artikel 6.1 c eller e har en rättslig grund i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, reglerar den rätten 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, ska punkterna 1–7 inte gälla, om inte medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen.

11. Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Skälen till artikel 35 i dataskyddsförordningen

Skälen till dataskyddsförordningen är viktiga vid tolkningen av förordningens bestämmelser. De skäl till dataskyddsförordningen som särskilt berör konsekvensbedömningar är skälen 89−94.

(89) Direktiv 95/46/EG föreskrev en allmän skyldighet att anmäla behandling av personuppgifter till tillsynsmyndigheterna. Denna skyldighet medförde administrativa och ekonomiska bördor, men förbättrade inte alltid personuppgiftsskyddet. Sådana övergripande och allmänna anmälningsskyldigheter bör därför avskaffas och ersättas av effektiva förfaranden och mekanismer som i stället inriktas på de typer av behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa behandlingar kan vara sådana som särskilt inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller som blir nödvändiga på grund av den tid som har förflutit sedan den ursprungliga behandlingen.

(90) I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftskyddet och visa att denna förordning efterlevs.

(91) Detta bör särskilt vara tillämpligt på storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå, vilket skulle kunna påverka ett stort antal registrerade och sannolikt kommer att innebära en hög risk, exempelvis till följd av uppgifternas känsliga natur, där i enlighet med den uppnådda nivån av teknisk kunskap en ny teknik används storskaligt, samt på annan behandling som innebär en hög risk för registrerades rättigheter och friheter, framför allt när denna behandling gör det svårare för de registrerade att utöva sina rättigheter. En konsekvensbedömning avseende dataskydd bör också göras, där personuppgifter behandlas i syfte att fatta beslut om specifika fysiska personer efter en systematisk och omfattande bedömning av fysiska personers personliga aspekter på grundval av profilering av dessa uppgifter eller efter behandling av särskilda kategorier

av personuppgifter, biometriska uppgifter eller uppgifter om fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder. Likaså krävs en konsekvensbedömning avseende dataskydd för övervakning av allmän plats i stor omfattning, särskilt vid användning av optisk-elektroniska anordningar, eller för all annan behandling där den behöriga tillsynsmyndigheten anser att behandlingen sannolikt kommer att innebära en hög risk för de registrerades rättigheter och friheter, framför allt på grund av att den hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal eller på grund av att den systematiskt genomförs i stor omfattning. Behandling av personuppgifter bör inte anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud. I dessa fall bör en konsekvensbedömning avseende dataskydd inte vara obligatorisk.

(92) Ibland kan det vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform eller när flera personuppgiftsansvariga planerar att införa en gemensam tillämpnings- eller behandlingsmiljö för en hel bransch eller ett helt segment eller för en allmänt utnyttjad horisontell verksamhet.

(93) Medlemsstaterna kan anse det nödvändigt att genomföra en sådan bedömning före behandlingen i samband med antagandet av medlemsstaters nationella rätt som ligger till grund för utförandet av myndighetens eller det offentliga organets uppgifter och reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder.

(94) Om det av en konsekvensbedömning avseende dataskydd framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader, bör samråd hållas med tillsynsmyndigheten innan behandlingen inleds. En sådan hög risk kommer sannolikt att orsakas av vissa typer av behandling samt av en viss omfattning och frekvens för behandlingen, vilket även kan leda till skador för eller kränkningar av fysiska personers rättigheter och friheter. Tillsynsmyndigheten bör inom en fastställd tid svara på en begäran om samråd. Ett uteblivet svar från tillsynsmyndigheten inom denna tid bör dock inte hindra ett eventuellt ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning, inbegripet befogenheten att förbjuda behandling. Som en del av denna samrådsprocess får resultatet av en konsekvensbedömning avseende dataskydd som utförs med avseende på behandlingen i fråga överlämnas till tillsynsmyndigheten, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.

Läs mer:
De skäl till dataskyddsförordningen som särskilt berör risk är skälen 75–77

4. Stöd i att bedöma om en konsekvens-bedömning ska genomföras

4.1 Tolka artikel 35.1 i dataskyddsförordningen

Artikel 35.1 i dataskyddsförordningen innehåller en bestämmelse om *när* den personuppgiftsansansvarige ska utföra en konsekvensbedömning. Det går dock inte att tolka artikeln enbart utifrån ordalydelsen. Den EU-rättsliga tolkningsmetoden innebär att bestämmelser även ska tolkas bl.a. utifrån de mål som eftersträvas med dem och det sammanhang där de ingår, och att begrepp ofta ska ges en självständig och enhetlig tolkning inom hela unionen.[8] Nedan utvecklas IMY:s tolkning av bestämmelsen i artikel 35.1 i dataskyddsförordningen.

En typ av behandling

Vid bedömningen av om en behandling är en sådan *typ av behandling* som omfattas av kravet på konsekvensbedömning ska personuppgiftsansvariga utgå från de faktorer som framgår av artikel 35.1, punkterna i artikel 35.3 och kriterierna i IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen.

Att det är *typen av behandling* som är i fokus innebär att fler behandlingar blir föremål för konsekvensbedömning än om det hade varit den faktiska planerade behandlingen som var avgörande för bedömningen. Detta eftersom det saknar betydelse (för skyldigheten att göra en konsekvensbedömning) att den personuppgiftsansvarige har bestämt att flera riskreducerande och effektiva åtgärder ska implementeras för en viss behandling. Med andra ord: Om en planerad behandling är en sådan *typ av behandling* som innebär att en konsekvensbedömning ska genomföras så saknar det betydelse att behandlingen, efter att olika åtgärder utförts, i praktiken sannolikt inte kommer att leda till en hög risk. De åtgärder som kan reducera eller eliminera de identifierade riskerna för den specifika planerade behandlingen ska beaktas först när konsekvensbedömningen faktiskt genomförs.[9] Om kravet i artikel 35.1 i dataskyddsförordningen hade tagit sikte på den faktiska behandlingen skulle många högriskbehandlingar aldrig bli föremål för en konsekvensbedömning. Höga risker skulle då i högre utsträckning förbises.

Denna tolkning av begreppet *typ av behandling* bygger på bestämmelsens syfte och sammanhang i enlighet med den EU-rättsliga tolkningsmetoden. Ett av syftena med kravet att genomföra en konsekvensbedömning är att behandlingar som typiskt sett kan leda till höga risker ska bli föremål för riskreducerande åtgärder. Om omständigheter som ska beaktas och dokumenteras under själva konsekvensbedömningen beaktas redan vid frågan om konsekvensbedömningen är nödvändig skulle möjligheterna till efterhandskontroll minska. När det gäller bestämmelsens sammanhang kan konstateras att både artikel 35.4 och 35.5 innehåller begreppet ”behandlingsverksamhet” (på engelska: ”processing operation”) och inte ”en behandling”. Även detta för att begreppet i artikel 35.1 inte ska likställas med den faktiska behandlingen.

De faktorer som räknas upp

IMY anser att de faktorer som räknas upp i artikel 35.1 i dataskyddsförordningen ska förstås på följande sätt.

- ***Användning av ny teknik***
  Begreppet avser användning av den senaste tekniken och tekniska kunskapen, exempelvis artificiell intelligens, maskininlärning och djupinlärning, självkörande fordon och intelligenta transportsystem, samt vissa Internet of Things-applikationer. Det kan även handla om ny och innovativ användning av befintlig teknik. Nya former

8 EU-domstolens dom den 14 december 2023, C-340/21 (Natsionalna agentsia za prihodite), EU:C:2023:986, p. 23 och där angiven rättspraxis.
9 Se för ett liknande resonemang: Ambrock J., Moritz K. (2023), Art. 35 – Data protection impact assessment, s. 692. I: Döhmann I. S., Papakonstantinou V., Hornung G., De Hert P., General Data Protection Regulation – Article-by-Article Commentary, s. 687–705.

av insamling och användning av uppgifter innebär ofta en högre risk för enskildas fri- och rättigheter. Detta eftersom de personliga och sociala konsekvenserna av att använda ny teknik kan vara okända.[10] En konsekvensbedömning hjälper personuppgiftsansvariga att förstå och hantera sådana risker.

Exempel på användning av ny teknik

Ett generativt AI-system som har tränats på stora mängder data och vars beteende inte har analyserats i större utsträckning skulle sannolikt omfattas av kriteriet *användning av ny teknik.* Ett system som använder AI-tekniker som är kända, väl beprövade och som har analyserats sedan tidigare, skulle dock kunna falla utanför kriteriet.

- ***Behandlingens art***
  Begreppet avser vilken typ av behandling det är, hur den ska gå till och vilka typer av personuppgifter som ska behandlas. Några exempel på olika behandlingstyper är kommunikation, lagring och bearbetning. Hur behandlingen ska gå till kan exempelvis handla om vilken teknik som ska användas eller hur personuppgifterna rent praktiskt ska samlas in, användas, lagras eller delas. Vilka typer av personuppgifter som behandlas inbegriper frågan om uppgifterna är känsliga eller på annat sätt integritetskänsliga och om de avser sårbara eller särskilt utsatta personer. De sistnämnda kan exempelvis vara barn, personer med nedsatt funktionsförmåga eller individer som står i beroendeställning till den personuppgiftsansvarige.

- ***Behandlingens omfattning***
  Begreppet avser vilken volym av personuppgifter det är fråga om, antalet registrerade, hur länge och hur ofta behandlingen ska pågå samt vilken geografisk omfattning den ska ha. För att klargöra behandlingens omfattning kan den personuppgiftsansvarige exempelvis fråga sig om behandlingen rör ett stort antal registrerade, om det är fråga om ett stort antal personuppgifter om varje registrerad, hur länge uppgifterna ska lagras samt hur många och vilka som kommer ha åtkomst till uppgifterna.

- ***Behandlingens sammanhang***
  Begreppet avser behandlingen i ett större perspektiv med hänsyn till olika interna och externa faktorer, exempelvis uppgifternas ursprung, den personuppgiftsansvariges relation till de enskilda personerna och i vilken utsträckning som enskilda har kontroll över sina uppgifter. Andra omständigheter som bör beaktas är om enskilda rimligen kan förvänta sig behandlingen eller om den kan uppfattas som oförutsägbar.
  Den personuppgiftsansvarige kan exempelvis fråga sig om behandlingen kommer att ske i ett särskilt förtroendefullt sammanhang där det finns förväntningar på konfidentialitet på grund av tystnadsplikt eller sekretess (som för sjukvårdspersonal, journalister, advokater, visselblåsningskanaler m.m.). I behandlingens sammanhang ingår även om det finns relevanta uppförandekoder eller andra certifieringssystem.

- ***Behandlingens ändamål***
  Begreppet avser själva anledningen till att den personuppgiftsansvarige vill genomföra behandlingen och vilken effekt den kommer att ha på enskilda. Ibland används ordet syfte istället för ändamål. För att klargöra ändamålet med behandlingen kan den personuppgiftsansvarige exempelvis fråga sig vilka som är de förväntade fördelarna med behandlingen för verksamheten eller för de registrerade. Ändamålet med behandlingen

10 Jfr WP 248, s. 12.

kan vara mer eller mindre integritetskänsligt. Om syftet med en tjänst exempelvis är att avslöja, peka ut, kontrollera eller övervaka vissa personer, eller att de registrerade ska kunna profileras på olika sätt, är behandlingens ändamål mer integritetskänsligt än om syftet är att kunna kontakta kunder för en kundnöjdhetsundersökning.

Sannolikt leder till

Sannolikt leder till innebär en uppskattning och prognos för hur troligt det är att något (en viss typ av behandling) medför eller resulterar i ett visst utfall (hög risk för fysiska personers rättigheter och friheter). I EU-domstolens praxis saknas närmare vägledning kring hur begreppet ska tolkas.

Hög risk

Trots att begreppet *risk* har en så framträdande roll i dataskyddsförordningen har det ingen uttrycklig definition i dataskyddsförordningen. Begreppet utvecklas dock i skälen 75–77 till dataskyddsförordningen. I EDPB:s riktlinjer om konsekvensbedömning har risk beskrivits som ”ett scenario som beskriver en händelse och dess uppskattade konsekvenser vad gäller allvar och sannolikhet”.[11] Vid tolkningen av begreppet ”risk” enligt dataskyddsförordningen går det även att hämta vägledning från olika internationella standarder om generell riskhantering, exempelvis ISO 3100026.[12]

Vad som krävs för att en behandling ska innebära en hög risk för enskildas fri- och rättigheter är inte heller uttryckligen definierat i förordningen. Det går dock att hämta ledning i exemplen som ges i artikel 35.3 i dataskyddsförordningen, IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen och kriterierna i EDPB:s riktlinjer om konsekvensbedömning.

Fysiska personers rättigheter och friheter

Fysiska personer är den grupp som utgör skyddsintresset, och vars rättigheter och friheter som ska beaktas. Notera att det inte står ”de registrerade”. Det är därmed inte enbart risker för de personer vars personuppgifter som kommer att behandlas som ska beaktas. Med *rättigheter och friheter* avses i första hand fysiska personer rätt till skydd för sina personuppgifter, sitt privatliv och sin integritet, men även andra grundläggande rättigheter (exempelvis yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, samvetsfrihet och religionsfrihet).[13]

IMY anser att begreppet ”rättigheter och friheter” ska ges en vidsträckt tolkning och att de flesta negativa effekter som olika fysiska, materiella eller immateriella skador har på den enskildes privatliv ska beaktas i sammanhanget.[14] Det kan handla om exempelvis stigmatisering i sociala sammanhang, sämre avtalsvillkor på osakliga grunder, manipulation som påverkar i viktiga beslut eller begränsning av kommunikation eller yttrandefrihet genom självcensur. Andra exempel är identitetsstöld, ekonomisk förlust och skadat anseende.[15]

4.2 Tolka artikel 35.3 a−c i dataskyddsförordningen

Punkterna i artikel 35.3 i dataskyddsförordningen är exempel på situationer då en behandling *sannolikt leder till en hög risk*[16] och en konsekvensbedömning alltid ska genomföras. Det är inte en uttömmande förteckning. Andra behandlingar som medför liknande höga risker som de som framgår av dessa punkter ska också föregås av en konsekvensbedömning.

11 WP 248, s. 7.
12 Jfr WP 248, s. 5 not 9 och s. 19.
13 Jfr WP 248, s. 7.
14 Jfr skäl 75 i dataskyddsförordningen.
15 Jfr skäl 75 i dataskyddsförordningen.
16 WP 248, s. 9 f.

Punkterna i artikel 35.3 i dataskyddsförordningen syftar till att säkerställa en enhetlig tolkning av de situationer i vilka en konsekvensbedömning är obligatorisk.[17] Att punkterna utgör exempel innebär dock inte att skyldigheten att genomföra en konsekvensbedömning är frivillig i dessa fall. Om den planerade behandlingen faller under något av exemplen så är den personuppgiftsansvarige skyldig att genomföra en konsekvensbedömning.

Systematisk (punkt a och c)

Dataskyddsförordningen innehåller ingen definition av ordet *systematisk*. Enligt EDPB ska dock en *systematisk behandling* förstås som en behandling:

- som sker enligt ett system,
- som är på förhand arrangerad, organiserad eller metodisk,
- som sker enligt en allmän plan för uppgiftsinsamling, och/eller
- som utförs som ett led i en strategi.[18]

Automatisk behandling (punkt a)

I punkt a hänvisas till bedömningar och beslut som ”grundar sig” på *automatisk behandling*, snarare än ”enbart” automatisk behandling. Det innebär att det inte behöver vara fråga om ett ”helt automatiserat” beslut i den mening som avses i artikel 22 i dataskydds-förordningen för att bestämmelsen ska vara tillämpbar.[19]

Rättsliga följder (punkt a)

Exempel på sådana *rättsliga följder* som avses i punkt a är uppsägning av ett avtal, avslag på en lagstadgad social förmån eller inreseförbud i ett land. Exempel på ”sådant som på liknande sätt i betydande grad påverkar fysiska personer” är beslut som påverkar någons tillgång till hälso- och sjukvård, anställningsmöjlighet eller tillgång till utbildning.[20]

I stor omfattning (punkt b och c)

Vad gäller begreppet i *stor omfattning* finns inga uttalade tröskelvärden. EDPB rekommenderar dock att följande faktorer beaktas särskilt vid bedömningen av om behandlingen utförs i stor omfattning.

- antalet berörda personer (antingen som ett särskilt antal eller som en andel av den aktuella populationen)
- mängden data och/eller antalet typer av uppgifter som behandlas
- behandlingens varaktighet
- behandlingens geografiska omfattning.[21]

I skäl 91 till dataskyddsförordningen anges att skyldigheten att genomföra en konsekvensbedömning särskilt bör tillämpas på storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå. Behandling av personuppgifter bör dock inte anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud. I EDPB:s riktlinjer om dataskydds-ombud betonas att det finns en stor gråzon mellan de ytterligheter som nämns i skäl 91.[22]

17 WP 248, s. 5.
18 Artikel 29-arbetsgruppens *Riktlinjer om dataskyddsombud* (WP 243, rev 01), s. 11. EDPB har ställt sig bakom riktlinjerna, Endorsement 1/2018.
19 Artikel 29-arbetsgruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679 (WP 251, rev 01), s. 31.
20 WP 251, s. 22 f.
21 WP 248, s. 11 och WP 243, s. 10.
22 WP 243, not 14.

Personuppgiftsansvariga måste vara beredda på att kunna motivera sin bedömning i detta avseende. Det är därför viktigt att göra en väl underbyggd uppskattning av den mängd personuppgifter som ska behandlas.

Systematisk övervakning (punkt c)

Kamerabevakning som innebär personuppgiftbehandling är typiskt sett att anse som en systematisk övervakning av människor.[23] Ett annat exempel är sådan övervakning som kan ske genom positioneringssystem.

En allmän plats (punkt c)

Av EDPB:s riktlinjer om konsekvensbedömning framgår att begreppet en allmän plats ska ges en vid innebörd och inkludera alla platser som är tillgängliga för allmänheten, exempelvis torg, köpcentra, gator, marknader, tågstationer och offentliga bibliotek.[24] Vidare har det i den juridiska litteraturen − med hänvisning till EU-domstolens Ryneš-dom[25] − uttalats att begreppet förmodligen har en EU-gemensam innebörd.[26] Av Ryneš-domen framgår att privatundantaget ska tolkas restriktivt och att områden i anslutning till en privatpersons bostad som delvis omfattar en allmän väg och ingången till en privatbostad mitt emot, är områden dit allmänheten har tillträde. Detta talar sammantaget för att begreppet har en vid innebörd.

4.3 EDPB:s kriterier och IMY:s förteckning enligt artikel 35.4

EDPB:s riktlinjer om konsekvensbedömning

Europeiska dataskyddsstyrelsen (EDPB) inrättades i samband med att dataskyddsförordningen trädde i kraft år 2018. EDPB består av företrädare för EU-medlemsstaternas tillsynsmyndigheter och den Europeiska datatillsynsmannen (EDPS). EDPB har en i dataskyddsförordningen fastställd uppgift att se till att förordningen tillämpas enhetligt genom att utfärda riktlinjer, rekommendationer och bästa praxis.[27] EDPB:s riktlinjer är inte rättsligt bindande.[28]

EDPB ersatte Artikel 29-arbetsgruppen (Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter), som var inrättad genom artikel 29 i dataskyddsdirektivet[29]. Artikel 29-arbetsgruppen antog år 2017 *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* (WP 248 rev. 01). EDPB har genom beslut ställt sig bakom dessa riktlinjer.[30] Riktlinjerna har betydelse som vägledning om konsekvensbedömningar, och utgör ett stöd både i personuppgiftsansvarigas arbete med att uppfylla förordningens krav och i tillsynsmyndigheternas verksamhet. Riktlinjerna har även varit en av huvudkällorna till denna vägledning.

23 Jfr definitionen av ”systematisk” i WP 243, s. 11 och hänvisning i WP 248, s. 10.
24 WP 248, not på s. 11.
25 EU-domstolens dom den 11 december 2014, C-212/13 (Ryneš) EU:C:2014:2428, p. 29.
26 Öman S., *Dataskyddsförordningen (GDPR) m.m. – En Kommentar. Kommentaren till artikel 35.3 c.*
27 Artikel 70 i dataskyddsförordningen.
28 HFD har begärt ett förhandsavgörande från EU-domstolen som innefattar frågan om vilken rättslig tyngd EDPB:s uttalanden ska ges vid tolkningen av dataskyddsförordningen. Högsta förvaltningsdomstolens beslutade den 13 juni 2024 att inhämta förhandsavgörande i mål nr 870-23 (IMY:s ärende, dnr IMY-2023-1305).
29 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
30 EDPB, Endorsement 1/2018.

Riktlinjerna innehåller de kriterier som enligt EDPB ska beaktas vid bedömningen av om en typ av behandling kräver en konsekvensbedömning. Syftet med dessa kriterier är att ge konkreta exempel på typer av behandlingar som kräver konsekvensbedömning på grund av sin ”inneboende höga risk”.[31]

Läs mer

EDPB:s 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

IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen

Som tillsynsmyndighet ansvarar IMY bl.a. för att verkställa tillämpningen av dataskyddsförordningen och bidra till en enhetlig tillämpning av dataskyddsreglerna inom EU. I detta ingår att i enlighet med artikel 35.4 i dataskyddsförordningen, upprätta och föra en förteckning över de slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning. IMY har fattat beslut[32] om att upprätta och offentliggöra en sådan förteckning.[33] IMY:s förteckning bygger på kriterierna i EDPB:s riktlinjer om konsekvensbedömning.

Syftet med de nationella förteckningarna enligt artikel 35.4 i dataskyddsförordningen är inte att ersätta bestämmelsen i artikel 35.1 i dataskyddsförordningen, utan att komplettera de exempel som ges i artikel 35.3 i dataskyddsförordningen.[34] Genom att ytterligare specificera vad som kan utgöra ”hög risk”, och ge exempel på behandlingar som kräver att en konsekvensbedömning genomförs, ger IMY:s förteckning ett stöd vid tolkningen av begreppet.

Som huvudregel ska personuppgiftsansvariga genomföra en konsekvensbedömning om en planerad behandling uppfyller minst två av kriterierna i förteckningen. I förteckningen finns ett antal exempel på behandlingar som uppfyller minst två kriterier och där en konsekvensbedömning ska genomföras. Det är viktigt att vara medveten om att förteckningen inte är uttömmande och att en konsekvensbedömning kan behöva genomföras i ett enskilt fall även om bara ett av kriterierna i förteckningen är uppfyllt.

I vissa fall kan en behandling uppfylla två eller flera av kriterierna, eller vara närliggande ett av exemplen, men den personuppgiftsansvarige gör ändå bedömningen att den *sannolikt inte leder till en hög risk*. Den personuppgiftsansvarige bör i sådana fall alltid utförligt motivera och dokumentera skälen för detta, och inkludera eventuella synpunkter från dataskyddsombudet (om ett sådant finns).[35]

Läs mer:

IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen
IMY:s beslut om förteckning enligt artikel 35.4 i dataskyddsförordningen

31 WP 248, s. 10.
32 IMY:s dnr DI-2018-13200.
33 IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen.
34 Det kan noteras att bestämmelsen i artikel 35.1 står över de nationella förteckningarna enligt artikel 35.4 i rättskällehierarkin.
35 IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen.

Kriterierna i IMY:s förteckning enligt artikel 35.4 och EDPB:s riktlinjer

För att underlätta jämförelse anges respektive kriterium parallellt nedan.

IMY:s Förteckning över när en konsekvensbedömning ska göras enligt artikel 35.4 En konsekvensbedömning ska göras om den planerade behandlingen uppfyller minst två av följande kriterier:	**Kriterier som enligt EDPB ska beaktas vid bedömningen av om en behandling *sannolikt leder till en hög risk***
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	**1. Utvärdering eller poängsättning, inbegripet profilering** och förutsägelse, särskilt ”aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar” (skälen 71 och 91). Exempel på detta kan innefatta finansinstitut som granskar sina kunder mot en databas för kreditupplysning eller mot en databas för bekämpning av penningtvätt och finansiering av terrorism, eller ett bioteknikföretag som erbjuder genetiska tester direkt till konsumenter för att bedöma och förutse risker för sjukdomar/hälsorisker, eller ett företag som utvecklar profiler för beteende eller marknadsföring som grundas på användning av eller navigering på dess webbplats.
2. behandlar personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade	**2. Automatiskt beslutsfattande med rättsliga eller liknande betydande följder:** behandling som har i syfte att fatta beslut om registrerade som har ”rättsliga följder för fysiska personer” eller ”på liknande sätt i betydande grad påverkar fysiska personer” (artikel 35.3 a). Till exempel kan behandlingen leda till utestängning eller diskriminering av enskilda. Behandling som har liten eller ingen påverkan på enskilda uppfyller inte detta särskilda kriterium.
3. systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer	**3. Systematisk övervakning:** behandling som används för att observera, övervaka eller kontrollera registrerade, inbegripet uppgifter som har samlats in genom nätverk eller ”[s]ystematisk övervakning av en allmän plats” (artikel 35.3 c). Denna typ av övervakning är ett kriterium eftersom personuppgifter kan samlas in i situationer där de registrerade kanske inte är medvetna om vem som samlar in deras uppgifter eller hur de kommer att användas. Dessutom kan det vara omöjligt för enskilda att undvika att bli föremål för sådan behandling på allmän plats (eller allmänt tillgängliga platser).

Tabellen fortsätter på nästa sida.

IMY:s Förteckning över när en konsekvensbedömning ska göras enligt artikel 35.4 En konsekvensbedömning ska göras om den planerade behandlingen uppfyller minst två av följande kriterier:	**Kriterier som enligt EDPB ska beaktas vid bedömningen av om en behandling *sannolikt leder till en hög risk***
4. behandlar känsliga personuppgifter enligt artikel 9 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	**4. Känsliga uppgifter eller uppgifter av mycket personlig karaktär:** detta omfattar särskilda kategorier av personuppgifter såsom de definieras i artikel 9 (till exempel information om enskildas politiska åsikter) liksom personuppgifter som gäller fällande domar i brottmål och brott såsom de definieras i artikel 10. Ett exempel kan vara ett allmänt sjukhus som lagrar patienternas journaler eller en privatdetektiv som sparar uppgifter om gärningsmän. Utöver dessa bestämmelser i förordningen kan vissa kategorier av uppgifter anses öka den eventuella risken för enskildas rättigheter och friheter. Sådana personuppgifter anses vara känsliga (såsom detta begrepp normalt förstås), eftersom de är kopplade till verksamhet som har samband med hushållet och privat verksamhet (såsom elektronisk kommunikation vars konfidentialitet ska skyddas), eller eftersom de påverkar utövandet av en grundläggande rättighet (såsom lokaliseringsuppgifter vars insamling medför att den fria rörligheten ifrågasätts) eller eftersom åsidosättandet av dessa rättigheter entydigt får allvarliga konsekvenser för den registrerades dagliga liv (såsom finansiella uppgifter som kan användas för betalningsbedrägeri). I detta avseende kan det ha betydelse om uppgifterna redan har offentliggjorts av den registrerade eller av tredje man. Det faktum att personuppgifterna har offentliggjorts kan beaktas som en faktor vid bedömningen av om uppgifterna förväntades användas vidare för särskilda ändamål. Detta kriterium kan även omfatta uppgifter såsom personliga dokument, e-postmeddelanden, dagböcker, kommentarer från läsplattor som är utrustade med kommentarfunktioner och mycket personlig information i applikationer som registrerar aktiviteter.

Tabellen fortsätter på nästa sida.

IMY:s Förteckning över när en konsekvensbedömning ska göras enligt artikel 35.4 En konsekvensbedömning ska göras om den planerade behandlingen uppfyller minst två av följande kriterier:	**Kriterier som enligt EDPB ska beaktas vid bedömningen av om en behandling *sannolikt leder till en hög risk***
5. behandlar personuppgifter i stor omfattning	**5. Uppgifter som behandlas i stor omfattning:** I förordningen definieras inte vad som avses med stor omfattning, även om viss vägledning ges i skäl 91. Arbetsgruppen rekommenderar i vart fall att följande faktorer beaktas särskilt vid bedömningen av huruvida behandlingen utförs i stor omfattning: a. Antalet registrerade som berörs, antingen som ett särskilt antal eller som en andel av den aktuella populationen. b. Mängden uppgifter och/eller variationen av hanterade dataelement. c. Databehandlingens varaktighet eller beständighet. d. Behandlingens geografiska 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	**6. Matchande eller kombinerande uppgiftsserier,** som till exempel kommer från två eller flera behandlingar av uppgifter som utförs i olika syften och/eller av olika personuppgiftsansvariga på ett sätt som överstiger den registrerades rimliga förväntningar.
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	**7. Uppgifter som rör sårbara registrerade** (skäl 75): behandling av denna typ av uppgifter är ett kriterium på grund av en ökad maktobalans mellan de registrerade och den personuppgiftsansvarige, vilket innebär att det kan vara svårt för enskilda att på ett enkelt sätt lämna samtycke eller motsätta sig behandling av sina uppgifter eller utöva sina rättigheter. Sårbara registrerade kan omfatta barn (de kan anses inte vara i stånd att medvetet och med eftertanke motsätta sig eller lämna samtycke till behandling av sina uppgifter), anställda, mer sårbara befolkningsgrupper som behöver socialt skydd (psykiskt sjuka personer, asylsökande, äldre personer, patienter osv.), samt i vart fall situationer där en obalans kan fastställas vad gäller förhållandet mellan den registrerade och den personuppgiftsansvarige.

Tabellen fortsätter på nästa sida.

IMY:s Förteckning över när en konsekvensbedömning ska göras enligt artikel 35.4 En konsekvensbedömning ska göras om den planerade behandlingen uppfyller minst två av följande kriterier:	**Kriterier som enligt EDPB ska beaktas vid bedömningen av om en behandling *sannolikt leder till en hög risk***
8. använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT)	**8. Innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar,** såsom en kombination av fingeravtryck och ansiktsigenkänning för förbättrad fysisk åtkomstkontroll osv. I förordningen klargörs (artikel 35.1 och skälen 89 och 91) att användningen av ny teknik, definierad ”i enlighet med den uppnådda nivån av teknisk kunskap” (skäl 91), kan innebära att det behövs en konsekvensbedömning. Detta beror på att användningen av sådan teknik kan omfatta nya former av insamling och användning av uppgifter, eventuellt med hög risk för enskildas rättigheter och friheter. De personliga och sociala konsekvenserna av användningen av ny teknik kan vara okända. En konsekvensbedömning hjälper den personuppgiftsansvarige att förstå och hantera sådana risker. Till exempel kan vissa ”sakernas internet”-applikationer få betydande konsekvenser för enskildas dagliga liv och integritet och således kräva en konsekvensbedömning.
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.	**9. Om behandlingen i sig ”hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal”** (artikel 22 och skäl 91). Detta omfattar behandlingar som syftar till att medge, ändra eller neka registrerade tillgång till en tjänst eller att ingå ett avtal. Ett exempel på detta är när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

Exempel på behandlingar som kräver att konsekvensbedömning utförs som framgår av IMY:s förteckning enligt artikel 35.4

Nedan anges de exempel som framgår av IMY:s förteckningen. Det är viktigt att vara medveten om att det inte är en uttömmande uppräkning på respektive område.

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 missköt-samhet (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 lokaliserings-uppgifter 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 registre-ringsnummer i syfte att debitera parkeringsavgifter (kriterium 3 och 8).

- Verksamheter som samlar in personuppgifter, innefattande bland annat lokalise-ringsuppgifter, 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).

4.4 Ingen skyldighet att genomföra en konsekvensbedömning

Inte en sådan typ av behandling som sannolikt leder till hög risk

Det är endast om en typ av behandling ”sannolikt leder till en hög risk för fysiska personers fri- och rättigheter” som det finns en skyldighet att genomföra en konsekvensbedömning.[36] I andra fall saknas sådan skyldighet. Personuppgiftsansvariga är skyldiga att kontinuerligt bedöma risker som uppkommer vid deras behandlingar av personuppgifter för att uppmärksamma om en behandling övergår i att bli en sådan ”typ av behandling” som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.[37]

IMY får enligt artikel 35.5 i dataskyddsförordningen upprätta och offentliggöra en nationell förteckning över ”det slags behandlingsverksamheter” som inte kräver någon konsekvensbedömning. Ett antal nationella tillsynsmyndigheter har tagit fram en sådan förteckning, bl.a. franska CNIL[38] och spanska AEPD[39].

IMY har gjort vissa uttalanden om när det inte finns skyldighet att genomföra en konsekvensbedömning. I beslutet om IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen framgår bl.a. att en konsekvensbedömning inte regelmässigt krävs vid kontroll mot en sanktionslista av en personuppgiftsansvarig som har en rättslig skyldighet att göra en sådan. En enkel kontroll mot en sanktionslista bör inte kräva en konsekvensbedömning, medan en mer komplicerad samkörning av olika register bör göra det.[40] Det framgår även av IMY:s förteckning att en vårdgivares behandling av personuppgifter om patienter i ringa omfattning (såsom när en läkare är ensam verksamhetsutövare och behandlar uppgifter om sina patienter) inte behöver bli föremål för en konsekvensbedömning.[41]

Mycket lik en annan behandling för vilken konsekvensbedömning genomförts

En personuppgiftsansvarig planerar flera liknande behandlingar

Av artikel 35.1 i dataskyddsförordningen framgår att en enda konsekvensbedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker. Det innebär att en konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra i fråga om art, omfattning, sammanhang, ändamål och risker.[42] En personuppgiftsansvarig som planerar flera liknande behandlingar behöver därför inte alltid upprätta en helt ny konsekvensbedömning för varje planerad personuppgiftsbehandling. Exempelvis kan en redan genomförd konsekvensbedömning användas som referens i den nya konsekvensbedömningen. Skälet till detta är givetvis att det ofta saknas behov att analysera situationer (som kan medföra hög risk för fysiska personers rättigheter och friheter) när en sådan situation redan har analyserats.[43] Den personuppgiftsansvarige måste dock kunna motivera att den planerade behandlingens art, omfattning, sammanhang, ändamål och risker har tillräckliga likheter med den tidigare behandlingen. Enligt IMY:s mening krävs det att behandlingarna är mycket lika varandra för att förutsättningarna ska vara uppfyllda.

36 Jfr artikel 35.1 i dataskyddsförordningen.
37 WP 248, s. 7.
38 Commission Nationale de l’Informatique et des Libertés (CNIL), Analyse d’impact relative à la protection des données: publication d’une liste des traitements pour lesquels une analyse n’est pas requise, den 9 oktober 2019, https://www.cnil.fr/fr/liste-traitements-aipd-non-requise (hämtat den 17 januari 2025).
39 Agencia Española Protección Datos (AEPD), Indicative list of the typers of data that do not require a data protection impact assessment under art 35.5 GDPR, https://www.aepd.es/documento/listadpia-35-5-ingles.pdf, (hämtat den 17 januari 2025).
40 IMY:s Beslut om förteckning enligt artikel 35.4 i EU:s allmänna dataskyddsförordning 2016/679, dnr DI-2018-13200, s. 4.
41 Exempel i IMY:s förteckning enligt artikel 35.4.
42 WP 248, s. 8.
43 WP 248, s. 8.

Flera personuppgiftsansvariga planerar flera liknande behandlingar

Artikel 35.1 i dataskyddsförordningen innebär också att flera personuppgiftsansvariga som planerar liknande behandlingar kan genomföra en gemensam konsekvensbedömning om behandlingarna liknar varandra i fråga om art, omfattning, sammanhang, ändamål och risker.[44] Exempelvis bör bolag som inom ramen för en branschorganisation planerar att skapa en gemensam plattform för behandling av personuppgifter kunna genomföra en gemensam konsekvensbedömning – förutsatt att bolagens respektive behandlingar och dess risker är tillräckligt lika. Även statliga myndigheter som planerar att införa ett gemensamt IT-system som tillhandahålls av samma leverantör bör i regel kunna genomföra en gemensam konsekvensbedömning – förutsatt att de planerade behandlingarna innebär samma risknivå.

Om flera personuppgiftsansvariga genomför en gemensam konsekvensbedömning bör det framgå skriftligen vilken av de personuppgiftsansvariga som är ansvarig för de olika åtgärder som har vidtagits för att skydda enskildas rättigheter och friheter. Det är viktigt att vara medveten om att oavsett hur ansvaret för säkerhetsåtgärderna fördelas måste respektive personuppgiftsansvarig säkerställa att det genomförs en godtagbar konsekvensbedömning för den egna personuppgiftsbehandlingen. Det innebär bl.a. att den personuppgiftsansvarige ska kunna motivera att dataskyddsförordningens krav har uppfyllts genom att en gemensam konsekvensbedömning har genomförts.[45]

En personuppgiftsansvarig kompletterar en konsekvensbedömning

En personuppgiftsansvarig som köper in en teknisk produkt (exempelvis en maskinvara eller programvara) bör även – i den mån det är lämpligt – kunna hänvisa till den konsekvensbedömning som har genomförts av organisationen som har tillhandahållit produkten, om en sådan finns. Den personuppgiftsansvarige är dock ansvarig för att genomföra sin egen konsekvensbedömning för den särskilda användningen av produkten i fråga.[46]

Om flera personuppgiftsansvariga genomför en gemensam konsekvensbedömning för ett gemensamt system, men en av de personuppgiftsansvariga har en tilläggsmodul eller en egen utveckling av systemet, kan den sistnämnda behöva komplettera den gemensamma konsekvensbedömningen med en konsekvensbedömning för den egna behandlingen. Det gäller förstås enbart om det egna tillägget innebär en behandling som omfattas av kravet på konsekvensbedömning, och särskilt om det innebär högre risker än det övriga systemet. Den personuppgiftsansvarige behöver även då kunna motivera att dataskyddsförordningens krav är uppfyllda genom användandet av en tidigare genomförd, eller en gemensam, konsekvensbedömning.

En allmän konsekvensbedömning har genomförts

Lagstiftaren kan inom ramen för ett författningsarbete genomföra en allmän konsekvensbedömning för att underlätta för de berörda personuppgiftsansvariga, exempelvis de myndigheter eller andra aktörer som får arbetsuppgifter enligt den nya lagstiftningen.[47] Av artikel 35.10 i dataskyddsförordningen följer att den personuppgiftsansvarige inte behöver genomföra en konsekvensbedömning om en sådan allmän konsekvensbedömning har genomförts och den planerade behandlingen har sin rättsliga grund i lagen eller förordningen.

44 WP 248, s. 8.
45 Jfr WP 248, s. 8.
46 Jfr WP 248, s. 9.
47 Artikel 35.10 i dataskyddsförordningen. Jfr skäl 93 till dataskyddsförordningen.

För att den personuppgiftsansvarige ska kunna avstå från att genomföra en konsekvensbedömning med hänvisning till en allmän konsekvensbedömning krävs att samtliga förutsättningar i artikel 35.10 i dataskyddsförordningen är uppfyllda. Det innebär att

- den rättsliga grunden för behandlingen ska vara artikel 6.1 c eller e i dataskyddsförordningen
- det ska finnas lagstiftning eller annan författning som reglerar behandlingen
- lagstiftaren ska ha genomfört en konsekvensbedömning (som en del av en allmän konsekvensbedömning) i samband med antagandet av den rättsliga grunden.

Det är dock sällan möjligt att redan i lagstiftningsärendet göra en sådan heltäckande konsekvensbedömning som dataskyddsförordningen kräver. Lagstiftaren kan lämna till den personuppgiftsansvarige att närmare bedöma vilken specifik teknisk lösning som ska användas för att genomföra uppdraget som ges i lagstiftningen. Den personuppgiftsansvarige kan därför behöva komplettera den allmänna konsekvensbedömningen med en egen konsekvensbedömning av de praktiska, tekniska och organisatoriska förutsättningarna för behandlingen.[48]

I lagstiftningsärendet kan lagstiftaren ibland redogöra för integritetsrisker och överväga hur olika skyddsåtgärder kan minimera integritetsrisker för att uppnå proportionalitet. Det innebär att den personuppgiftsansvarige i regel kan ta ledning i de generella överväganden som lagstiftaren har gjort vid genomförandet av sin kompletterande konsekvensbedömning.

48 T.ex. IMY:s remissvar den 14 september 2023 i IMY-2023-8865; prop. 2021/22:177, *Sammanhållen vård- och omsorgsdokumentation*, s. 54; SOU 2024:33, *Delad hälsodata – dubbel nytta*, s. 320 f.

5. IMY:s tillsynsbeslut

Som tillsynsmyndighet ansvarar IMY bl.a. för att övervaka tillämpningen av dataskyddsförordningen och annan dataskyddsreglering, öka allmänhetens och personuppgiftsansvarigas medvetenhet om risker och skyldigheter enligt regleringen, samt behandla klagomål.

För att säkerställa att dataskyddsförordningen efterlevs har IMY flera utredande och korrigerande befogenheter. Om personuppgiftsansvariga exempelvis inte uppfyller de krav som ställs på konsekvensbedömning kan IMY använda dessa. Det kan ske både när en personuppgiftsansvarig underlåtit att genomföra en konsekvensbedömning när detta är obligatoriskt, och när en konsekvensbedömning har genomförts på ett bristfälligt sätt.

Nedan ges referat av ett antal tillsynsbeslut där IMY har konstaterat brister i förhållande till artikel 35 i dataskyddsförordningen.

Digital skolplattform (IMY-2023-1647)

IMY:s granskning rörde Barn- och utbildningsnämndens i Östersunds kommun beslut att migrera en ny version av en befintlig digital skolplattform till en egen domän och starta upp tjänsten i kommunens egen IT-miljö. Tjänsten användes i 24 av kommunens skolor.

IMY konstaterade bl.a. följande. Förändringarna i användandet av tjänsten har resulterat i en ny personuppgiftsbehandling hos nämnden. Inför en så omfattande behandling av barns personuppgifter i skolverksamhet ska den som är personuppgiftsansvarig genomföra en konsekvensbedömning för att identifiera risker och behov av skyddsåtgärder, vilket nämnden inte hade gjort. Barnen befann sig i egenskap av elever i en utsatt position i förhållande till den personuppgiftsansvarige. Behandlingen rörde även anställda som befann sig i ett beroendeförhållande gentemot nämnden. Behandlingen innefattade dessutom till viss del återkoppling på skoluppgifter, vilket får anses utgöra en utvärdering av de registrerades prestationer.

IMY beslutade den 28 november 2023 att Barn- och utbildningsnämnden skulle betala en administrativ sanktionsavgift för överträdelse av artikel 35.1 i dataskyddsförordningen. Tillsynsbeslutet har fått laga kraft.

Läs beslutet: IMY-2023-1647

Kamerabevakning på LSS-boende (DI-2019-7782)

IMY:s granskning baserades på ett klagomål från en anhörig till en boende på ett LSS-hem som gjorde gällande att den boende olagligen kamerabevakades bl.a. i sitt sovrum.

IMY konstaterade flera brister, bl.a. att det inte hade genomförts en konsekvensbedömning.

IMY beslutade den 24 november 2020 att Gnosjö kommun – Socialutskottet skulle betala en administrativ sanktionsavgift för överträdelse av bl.a. artikel 35 i dataskyddsförordningen. Tillsynsbeslutet har fått laga kraft.

Läs beslutet: DI-2019-7782

Digital skolplattform (DI-2019-7024)

IMY:s granskning avsåg ett IT-system som användes av skolor i Stockholms stad för bl.a. elevadministration.

IMY konstaterade bl.a. annat följande. Granskningen visade att det fanns allvarliga brister i säkerheten. En konsekvensbedömning hade inte genomförts trots att det var fråga om

stora system med många barn och anställda registrerade, och med både känsliga och integritetskänsliga personuppgifter. Om Utbildningsnämnden skulle ha gjort en fullständig konsekvensbedömning så kunde de konstaterade bristerna sannolikt ha undvikits.

IMY beslutade den 23 november 2020 att Utbildningsnämnden i Stockholms stad skulle betala en administrativ sanktionsavgift för överträdelse av flera artiklar i dataskydds-förordningen samt förelade nämnden att snarast genomföra en konsekvensbedömning i enlighet med artikel 35 i dataskyddsförordningen för tre delsystem. Tillsynsbeslutet har fått laga kraft.

Läs beslutet: DI-2019-7024

Ansiktsigenkänning för närvarokontroll av elever (DI-2019-2221)

IMY:s granskning genomfördes mot bakgrund av att Gymnasienämnden i Skellefteå kommun i ett försöksprojekt på en gymnasieskola hade använt ansiktsigenkänning för att registrera elevers närvaro. Gymnasienämnden hänvisade till en ”utförd risk-bedömning” vid vilken slutsatsen dragits att det rättsliga stöd man hänvisade till, och den säkerhet behandlingen omfattades av, medförde att ingen ”särskild riskbedömning” behövde göras beträffande de känsliga personuppgifterna.

IMY konstaterade bl.a. följande. Det saknades förutsättningar för att behandla bio-metriska personuppgifter på det sätt som skett. De aktuella behandlingarna har inne-fattat ett antal faktorer som talade för att en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen skulle ha genomförts innan behandlingarna inleddes. Den ”riskbedömning” som nämnden redogjort för kunde inte anses uppfylla kraven i artikel 35 i dataskyddsförordningen. Den saknade en bedömning av de risker som förelåg för de registrerades rättigheter och friheter, liksom en redogörelse för proportionaliteten av behandlingen i förhållande till dess syften. Behandlingarna borde ha föranlett en begäran om förhandssamråd med IMY innan behandlingen inleddes, vilket innebar att behandlingarna även skett i strid med artikel 36 i dataskyddsförordningen.

IMY beslutade den 20 augusti 2019 att Gymnasienämnden i Skellefteå skulle betala en administrativ sanktionsavgift för överträdelse av bl.a. artikel 35 i dataskydds-förordningen. Tillsynsbeslutet har fått laga kraft.

Läs beslutet: DI-2019-2221

6. Dataskydds-ombudets roll i konsekvens-bedömningen

Av artikel 35.2 i dataskyddsförordningen framgår att den personuppgiftsansvarige ska rådfråga dataskyddsombudet vid genomförandet av en konsekvensbedömning. Dataskyddsförordningen reglerar inte i detalj när och på vilket sätt det ska ske, eller i övrigt hur dataskyddsombudet ska involveras i arbetet med konsekvensbedömningar.[49] Det finns därför ett visst utrymme för variation utifrån organisationens struktur, strategier för dataskydd och förutsättningar i övrigt, så länge den personuppgiftsansvarige beaktar övriga bestämmelser om dataskyddsombud.[50]

De centrala bestämmelserna om dataskyddsombudets uppgifter finns i artikel 37–39 i dataskyddsförordningen. Av artikel 39 följer att dataskyddsombudet på begäran ska ge råd till den personuppgiftsansvarige om konsekvensbedömningen och övervaka genomförandet av den. Det framgår även bl.a. att dataskyddsombudet ska fungera som kontaktpunkt för IMY om den personuppgiftsansvarige begär förhandssamråd enligt artikel 36 i dataskyddsförordningen. Dataskyddsombudets ställning framgår av artikel 38 och relevanta kvalifikationer för ett dataskyddsombud framgår av artikel 37.5. Av artikel 38.1 framgår att personuppgiftsansvariga ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Detta innefattar bl.a. arbetet med konsekvensbedömningar.

För att avgöra hur dataskyddsombudet ska eller bör involveras i konsekvensbedömningar kan den personuppgiftsansvarige hämta vägledning i EDPB:s riktlinjer om konsekvensbedömning och EDPB:s riktlinjer om dataskyddsombud.

IMY:s inställning är att dataskyddsombudet generellt sett bör involveras löpande, i flera skeden av genomförandet av konsekvensbedömningen och i samband med viktiga beslut. Det är lämpligt att dataskyddsombudet involveras så tidigt som möjligt i processen, för att exempelvis kunna ge råd om metod och minska risken för att avgränsningar blir fel.

Den personuppgiftsansvarige bör fastställa vem som ansvarar för att dataskyddsombudet involveras och bygga in kontroller i processerna för att kunna upptäcka när så inte har skett. Det är den personuppgiftsansvariges ansvar att säkerställa att dataskyddsombudet får korrekt och tillräcklig information om behandlingen och processen för att kunna utföra sitt uppdrag.

6.1 IMY anser att dataskyddsombudet bör göra följande i processen:

1. Ge råd inför en konsekvensbedömning

Den personuppgiftsansvarige bör rådfråga dataskyddsombudet innan omfattningen och avgränsningen av en konsekvensbedömning fastställs. Dataskyddsombudet bör exempelvis rådfrågas om en konsekvensbedömning ska genomföras inför en viss behandling och innan den personuppgiftsansvarige beslutar att inte genomföra en konsekvensbedömning trots att två kriterier i IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen är uppfyllda.[51] Dataskyddsombudet kan också föreslå att den personuppgiftsansvarige genomför en konsekvensbedömning för en särskild behandling.[52]

2. Ge råd kring metoden för konsekvensbedömningen

Dataskyddsombudet bör regelbundet och vid behov ge sina råd kring om metoden för konsekvensbedömningen är ändamålsenligt utformad. Med metod avses här hur konsekvensbedömningen går till, exempelvis i vilken ordning saker ska ske, vem som

49 Jfr WP 248, s. 19.
50 Jfr WP 248, s. 19.
51 Jfr WP 243, s. 20.
52 WP 248, s. 17.

ska involveras och om konsekvensbedömningen ska genomföras internt eller externt.[53] Dataskyddsombudet kan exempelvis gå igenom relevanta styr- och stöddokument, som process- och rutinbeskrivningar, mallar och vägledning. Dataskyddsombudet kan också rekommendera lämpliga åtgärder och följa upp att åtgärderna vidtas.

3. Ge råd vid riskhanteringen

IMY anser att den personuppgiftsansvarige vid behov bör rådfråga dataskyddsombudet i samband med riskbedömningen och vid bedömningen av vilka riskreducerande åtgärder som bör vidtas. Dataskyddsombudet kan exempelvis hjälpa till att utvärdera riskbedömningens kvalitet.[54] Dataskyddsombudet kan förslagsvis delta i eventuella workshops om riskhantering.

Hantering av dataskyddsombudets råd

IMY rekommenderar att dataskyddsombudet gör skillnad mellan å ena sidan allmänna råd och å andra sidan formella rekommendationer till den personuppgiftsansvarige. Vad den personuppgiftsansvarige bör göra med anledning av de råd och rekommendationer som dataskyddsombudet lämnar beror på omständigheterna i det enskilda fallet. Om dataskyddsombudet lämnar en formell rekommendation om att vidta eller avstå från en åtgärd och den personuppgiftsansvarige beslutar att inte följa den, bör den personuppgiftsansvarige dokumentera en motivering till det.[55]

4. Övervaka genomförandet av konsekvensbedömningen

Dataskyddsombudets uppgift att övervaka genomförandet av konsekvensbedömningen bör vara riskbaserad.[56] Dataskyddsombudets uppgift i detta avseende bör därmed anpassas till hur höga riskerna med behandlingen bedöms vara. För att dataskyddsombudet ska kunna utföra sin uppgift bör den som genomför konsekvensbedömningen regelbundet skicka statusrapporter om genomförandet.

5. Utvärdera resultatet av konsekvensbedömningen

Innan de riskreducerande åtgärderna genomförs och den kvarstående risken fastställs bör dataskyddsombudet utvärdera resultatet av konsekvensbedömningen. Dataskyddsombudet bör framförallt utvärdera om dokumentationen, bedömningarna och slutsatserna håller tillräckligt hög kvalitet. Dataskyddsombudet bör också hjälpa till att utvärdera om den kvarstående risken är godtagbar.

Generellt sett är lämpligt att dataskyddsombudet upprättar ett skriftligt utlåtande där det bl.a. framgår hur dataskyddsombudet har involverats i genomförandet och vilken dokumentation som ligger till grund för utlåtandet. Ett sådant utlåtande bör anpassas efter hur komplicerad konsekvensbedömningen är, hur omfattande den planerade behandlingen är och hur hög risken bedöms vara. I vissa fall kan det vara tillräckligt att dataskyddsombudet undertecknar en färdig text som har upprättats enligt en mall.[57] Dataskyddsombudets utlåtande bör dokumenteras i konsekvensbedömningen.[58]

53 Jfr WP 243, s. 20.
54 WP 248, s. 17.
55 Jfr WP 248, s. 13 och WP 243, s. 16.
56 Jfr WP 243, s. 22.
57 Jfr EU-domstolens dom den 16 februari 2023, C-349/21, HYA m.fl., EU:C:2023:102, p. 53 f.
58 WP 248, s. 13 och WP 243, s. 16.

Ett dataskyddsombud som anser att konsekvensbedömningen har brustit i någon del bör lämna en motivering som tydliggör bristen och om möjligt hur den kan avhjälpas. Dataskyddsombudet ska dock inte ta över genomförandet av konsekvensbedömningen.[59]

Nedan följer ett antal frågor som dataskyddsombudet kan ställa sig i sitt arbete med att utvärdera resultatet av konsekvensbedömningen.

Exempel på frågor att ställa vid utvärderingen

- Har dataskyddsombudet involverats tillräckligt i arbetet med konsekvensbedömningen? Har dataskyddsombudet fått korrekt och tillräcklig information för att kunna utföra sitt uppdrag?
- Är beskrivningen av behandlingen tillräckligt utförlig för att det ska vara möjligt att avgöra om principen om ändamålsbegränsning är uppfylld?
- Framstår det som att ett tillräckligt arbete genomförts vid identifiering av riskerna och som att riskvärderingen är välmotiverad?
- Är de identifierade åtgärderna lämpliga för att hantera riskerna?
- Är ansvarsfördelningen inom organisationen tydlig för att verkställa de riskreducerande åtgärderna?
- Är bedömningen av den eventuella kvarstående risken tydligt beskriven och motiverad?
- Är det tydligt vem som är ansvarig för den kvarstående risken inom organisationen?[60]
- Är bedömningen av behandlingens nödvändighet och proportionalitet tillräckligt utförligt motiverad? Är bedömningen rimlig?
- Är det tydligt när konsekvensbedömningen ska ses över och vem som ansvarar för att följa upp eventuella förändringar av riskerna?

6. Övervaka den övergripande efterlevnaden

Av dataskyddsförordningen framgår att dataskyddsombudet ska övervaka att gällande dataskyddsbestämmelser efterlevs i stort[61] och att dataskyddsombudet ska rapportera till den personuppgiftsansvariges högsta förvaltningsnivå[62]. Dataskyddsombudet bör därmed, förutom att ge råd kring enskilda konsekvensbedömningar, även övervaka organisationens arbete med konsekvensbedömningar i stort. Det kan exempelvis handla om att utreda hur många konsekvensbedömningar som genomförs, vilka delar av organisationen som genomför dem, hur lång tid det tar att genomföra dem och vilken kvalitet de har.

59 Jfr t.ex. artikel 35.2, 39.1 c och 38.6 i dataskyddsförordningen.
60 Notera att det interna ansvaret inom organisationen inte ska förväxlas med personuppgiftsansvaret enligt artikel 4.7 i dataskyddsförordningen.
61 Jfr artikel 39.1 b i dataskyddsförordningen.
62 Jfr artikel 38.3 tredje meningen i dataskyddsförordningen.

6.2 Vad dataskyddsombudet *inte* ska göra vid konsekvensbedömningen

Dataskyddsombudet ska inte genomföra konsekvensbedömningen eller ansvara för att den genomförs.[63] Dataskyddsombudet kan inte oberoende kvalitetssäkra, kontrollera eller granska något som denne själv har gjort. Det är den personuppgiftsansvarige som ansvarar för att metoden för att genomföra en konsekvensbedömning och resultatet av enskilda bedömningar är förenliga med dataskyddsförordningen.

Processen bör inte utformas så att dataskyddsombudet i praktiken tilldelas ansvar för bedömningar som visar sig vara felaktiga, exempelvis att en risk har värderats för lågt eller att behandlingen i någon del inte är nödvändig. Dataskyddsombudet har inte det slutliga ansvaret för att förhindra behandling som inte är förenlig med dataskydds-förordningen eller att se till att behandlingen anpassas till de rekommendationer som dataskyddsombudet föreslår. Det riskerar att strida mot dataskyddsombudets oberoende ställning.[64]

Den personuppgiftsansvarige bör utforma sin process för konsekvensbedömning så att ansvarsfördelningen mellan dataskyddsombudet och den personuppgiftsansvarige är tydlig för alla involverade.

63 Jfr t.ex. artikel 35.2, 39.1 c och 38.6 i dataskyddsförordningen.
64 Jfr IMY:s beslut den 27 juni 2024 i tillsynsärende IMY-2023-7980 (ang. personuppgiftsansvarigas skyldighet att se till att dataskydds-ombudets arbetsuppgifter inte leder till en intressekonflikt).

IMY. Integritetsskydds myndigheten

Detta är Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten arbetar för att skydda alla dina personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer. Det är vi som granskar att företag, myndigheter och andra aktörer följer GDPR – data-skyddsförordningen. Vi utbildar och vägleder dem som behandlar personuppgifter. Vi vill se en hållbar och integritetsvänlig digitalisering. Vi är övertygade om att det går att värna medborgarnas trygghet och samhällets säkerhet, utan omotiverad kartläggning och övervakning. Tillsammans med övriga dataskyddsmyndigheter i EU arbetar vi för att medborgarnas personuppgifter ska ha samma skydd i hela unionen. Vi arbetar även för att kreditupplysning ska bedrivas på ett korrekt sätt. Vår vision är ett tryggt informationssamhälle, där vi tillsammans värnar den personliga integriteten.

Kontakta Integritetsskyddsmyndigheten

E-post: imy@imy.se
Webb: www.imy.se
Tel: 08-657 61 00
Postadress: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm