Integritetsskydds myndigheten

Vägledning vid konsekvensbedömning

En praktisk guide

Februari 2025

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

Innehåll

Om vägledningen

IMY:s vägledning vid konsekvensbedömning riktar sig till verksamheter som behandlar personuppgifter enligt dataskyddsförordningen[1] och som vill ha stöd i arbetet med att genomföra konsekvensbedömningar. Syftet med vägledningen är att underlätta arbetet med konsekvensbedömningar och minska osäkerheten kring hur de olika momenten genomförs och hur regelverket ska förstås.

I ***En praktisk guide*** ger IMY sitt förslag på hur en godtagbar konsekvensbedömning kan genomföras. Den kan läsas separat eller tillsammans med de två stödmallar som IMY har tagit fram. För att underlätta planeringen av det praktiska arbetet, och för att kunna anpassa arbetssättet till den aktuella behandlingen, rekommenderar vi att ni läser guiden i sin helhet innan ni påbörjar konsekvensbedömningen. Guiden är framtagen främst för er som har liten eller ingen kunskap av konsekvensbedömningar.

I bilagan ***Rättsligt tolkningsstöd*** går IMY igenom regelverket på området och tolkningsstödet för detta. Bilagan är framtagen för er som vill ha det rättsliga tolkningsstödet samlat och fördjupad information om hur regelverket ska förstås.

IMY:s vägledning vid konsekvensbedömning

En praktisk guide
Bilagan Rättsligt tolkningsstöd

Mallar till stöd i arbetet

IMY:s mall för Bedömning av behovet av konsekvensbedömning
IMY:s mall för Konsekvensbedömning enligt dataskyddsförordningen
Excelblad Riskhantering vid konsekvensbedömning

IMY:s webbplats

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

Vår webbplats www.imy.se erbjuder översiktlig information om konsekvensbedömningar.

1. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Vad är en konsekvens-bedömning?

En konsekvensbedömning är en pågående och dokumenterad process som hjälper personuppgiftsansvariga[2] att följa dataskyddsförordningens bestämmelser vid högrisk-behandlingar. Processen ger en fördjupad förståelse för den aktuella behandlingen, vilka risker den innebär för enskildas fri- och rättigheter, och de säkerhets- och skyddsåtgärder som krävs för att minska riskerna.

En pågående och dokumenterad process

Ett syfte med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter – och framför allt deras rätt till skydd för sina personuppgifter[3]. För att enskildas rättigheter ska kunna garanteras lägger dataskyddsförordningen ett stort ansvar på dem som samlar in och behandlar personuppgifter att se till att behandlingarna följer tillämpliga bestämmelser. Det gäller i synnerhet vid så kallade *högriskbehandlingar*, dvs. sådana personuppgiftsbehandlingar som bedöms kunna leda till höga risker för enskildas fri- och rättigheter. De höga riskerna kan exempelvis bero på att känsliga personuppgifter ska behandlas, ny teknik för databehandling ska införas eller att behandlingen ska ske genom omfattande övervakning.

Det är viktigt att vara medveten om att konsekvensbedömningen är en pågående process. Det är inte en engångsaktivitet med ett tydligt avslut. Det innebär att konsekvens-bedömningen ska uppdateras och omprövas löpande.[4]

En skyldighet enligt gällande lagstiftning

Bestämmelser om konsekvensbedömning avseende dataskydd finns i artikel 35 i data-skyddsförordningen. Enligt den första punkten i artikeln ska personuppgiftsansvariga utföra en konsekvensbedömning inför sådan ”typ av behandling” som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

2 *Personuppgiftsansvarig* är 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 (se artikel 4.7 i dataskydds-förordningen). Avgörande för frågan om vem som är personuppgiftsansvarig är vem eller vilka som har bestämt varför behandlingen sker, samt utövar ett inflytande över vilka personuppgifter som samlas in och behandlas, hur länge de lagras och vem som har åtkomst. Bedömningen av vem eller vilka som är personuppgiftsansvarig för en viss behandling ska alltid utgå från de faktiska omständigheterna i det specifika fallet (se EDPB:s riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och person-uppgiftsbiträde i GDPR, version 2.1, s. 3 och 9 f.).

3 Rätten till skydd av personuppgifter framgår av artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (2012/C 326/02).

4 Artikel 35.11 i dataskyddsförordningen.

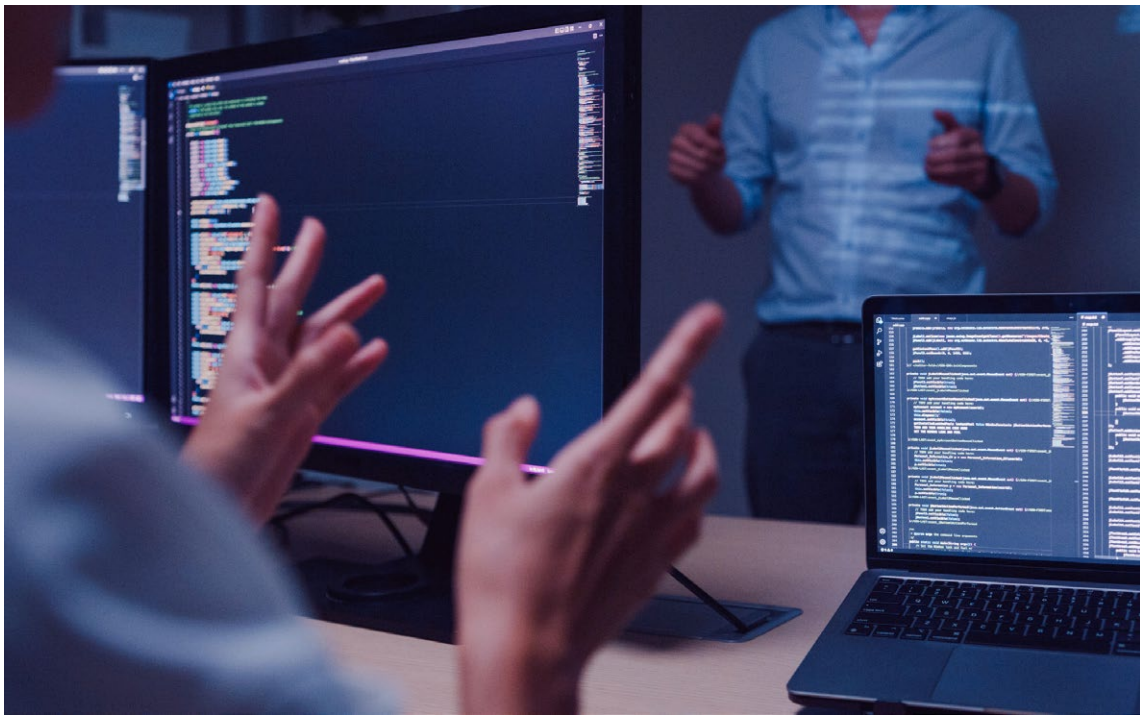
Dataskyddsförordningen kräver att personuppgiftsansvariga använder ett riskbaserat arbetssätt när de säkerställer att bestämmelserna i den följs och att de anpassar dataskyddet till behandlingens risknivå. Ju högre risk desto mer långtgående säkerhetsåtgärder, aktivt dataskyddsarbete och tätare uppföljning krävs. *Högriskbehandlingar* medför helt enkelt fler skyldigheter för personuppgiftsansvariga, och att genomföra konsekvensbedömningar är en av dessa.

Ett praktiskt verktyg för att säkerställa efterlevnad av gällande bestämmelser

Rätt genomförd är en konsekvensbedömning ett bra verktyg för personuppgiftsansvariga att bedöma risker och säkerställa att bestämmelserna i dataskyddsförordningen följs. Konsekvensbedömningen kan användas för att få ett helhetsgrepp om personuppgiftsbehandlingen och dess konsekvenser, samt minimera behandlingen så att den inte blir onödigt omfattande i förhållande till ändamålet.[5]

Konsekvensbedömningen skapar också förutsättningar för att personuppgiftsansvariga ska kunna uppfylla kravet på inbyggt dataskydd.[6] Dessutom är det utifrån konsekvensbedömningen som personuppgiftsansvariga ska avgöra om det finns en skyldighet att begära förhandssamråd med tillsynsmyndigheten.[7]

En väl utförd och dokumenterad konsekvensbedömning är en viktig del i att uppfylla principen om ansvarsskyldighet[8].



5 Jfr principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen.
6 Jfr artikel 25 i dataskyddsförordningen.
7 Jfr artikel 36 i dataskyddsförordningen. Förhandssamråd ska begäras om konsekvensbedömningen visar att behandlingen skulle leda till en hög risk, även med beaktande av de riskreducerande åtgärder som planeras.
8 *Principen om ansvarsskyldighet* innebär en skyldighet för personuppgiftsansvariga att efterleva dataskyddsförordningens bestämmelser och kommer till uttryck i artikel 5.2 i dataskyddsförordningen. Personuppgiftsansansvariga ska ansvara för att samtliga principer för behandling av personuppgifter följs och även kunna visa detta. I de personuppgiftsansvarigas ansvar ingår även att genomföra lämpliga tekniska och organisatoriska åtgärder och att säkerställa en säkerhetsnivå som är lämplig i förhållande till behandlingens risk för fysiska personers rättigheter och friheter (se artikel 32 i dataskyddsförordningen).

En konsekvensbedömning ska innehålla åtminstone:

- en systematisk beskrivning av den planerade behandlingen av personuppgifter och syftena med den
- en bedömning av behovet av behandlingen av personuppgifter och om intrånget den innebär står i proportion till syftena med den
- en bedömning av riskerna för fysiska personers rättigheter och friheter
- de åtgärder som planeras för att hantera riskerna och visa att dataskyddsförordningen följs.[9]

En konsekvensbedömning innebär att den personuppgiftsansvarige ska:

- rådfråga dataskyddsombudet (om ett sådant utsetts)[10]
- kontrollera att behandlingen är förenlig med eventuella uppförandekoder som har godkänts inom den aktuella branschen[11]
- inhämta synpunkter från de registrerade[12] eller deras företrädare, när det är lämpligt[13]
- genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen, vid behov.[14]

9 Artikel 35.7 i dataskyddsförordningen.
10 Artikel 35.2 i dataskyddsförordningen.
11 Artikel 35.8 i dataskyddsförordningen med hänvisning till artikel 40 i dataskyddsförordningen. En uppförandekod är en sorts regelbok om behandling av personuppgifter som utarbetats av och frivilligt tillämpas inom t.ex. en viss bransch eller sektor.
12 Begreppet registrerad kan definieras som den person vars personuppgifter behandlas, jfr artikel 4.1 i dataskyddsförordningen.
13 Artikel 35.9 i dataskyddsförordningen.
14 Artikel 35.11 i dataskyddsförordningen.

Om den praktiska guiden

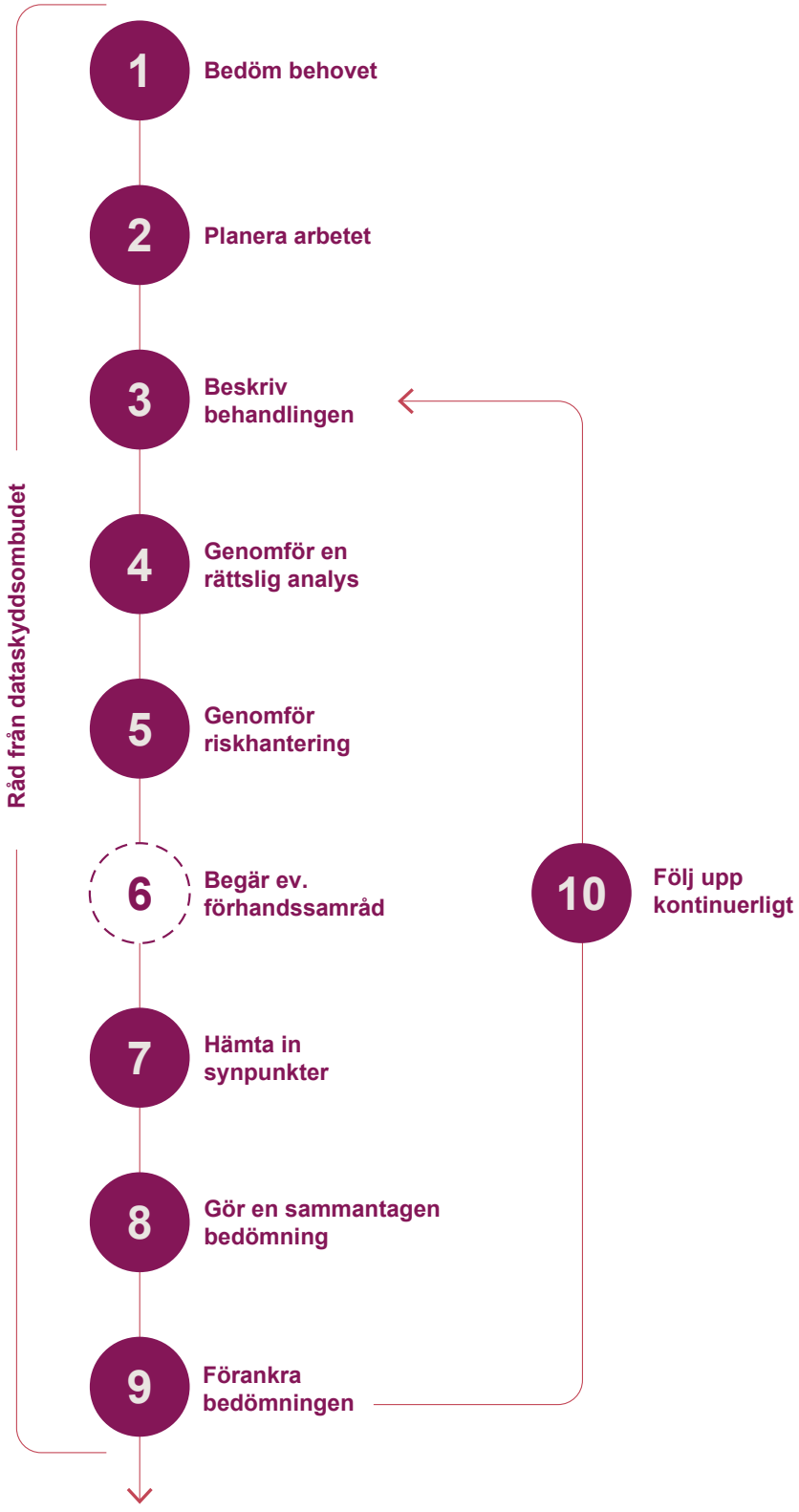
IMY:s guide till det praktiska arbetet med konsekvensbedömning utgår från de kriterier för godtagbar konsekvensbedömning som framgår av bilaga 2 till Europeiska dataskyddsstyrelsens (EDPB) riktlinjer om konsekvensbedömning[15]. Dessa kriterier tydliggör och utvecklar minimikraven enligt artikel 35 i dataskyddsförordningen.[16]

Det är naturligt att konsekvensbedömningars utformning varierar i omfattning och detaljnivå beroende på bl.a. komplexiteten av den behandling som ska bedömas och den enskilda organisationens storlek. Det tillvägagångssätt som beskrivs i IMY:s guide ska ses som en grund att utgå ifrån. Tillvägagångssättet kan behöva anpassas utifrån de resurser och kompetenser som finns tillgängliga. Stegen kan även behöva genomföras i en annan ordning än vad som beskrivs i guiden. Beroende på den aktuella behandlingen kan exempelvis synpunkter från registrerade i vissa fall behöva hämtas in i ett tidigare skede än som anges i guiden. Om den personuppgiftsansvarige har utsett ett dataskyddsombud bör detta enligt IMY:s mening rådfrågas löpande, och inte enbart i samband med att synpunkter hämtas in från berörda.

Den personuppgiftsansvarige ska dokumentera de bedömningar som görs och de beslut som fattas inom ramen för konsekvensbedömningen. Konsekvensbedömningen ska dokumenteras för att organisationen ska kunna visa att den följer dataskyddsförordningen.[17] Den personuppgiftsansvarige har dock ett utrymme att själv avgöra dokumentationens omfattning och detaljnivå.

15 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). EDPB har ställt sig bakom riktlinjerna, Endorsement 1/2018.
16 Jfr. WP 248, s. 19 och 22.
17 Artikel 5.2 i dataskyddsförordningen (principen om ansvarsskyldighet).

IMY:s förslag – en dokumenterad process i tio steg


1
Bedöm behovet
2
Planera arbetet
3
Beskriv behandlingen
4
Genomför en rättslig analys
5
Genomför riskhantering
6
Begär ev. förhandssamråd
7
Hämta in synpunkter
8
Gör en sammantagen bedömning
9
Förankra bedömningen
10
Följ upp kontinuerligt
Råd från dataskyddsombudet

Steg 1.
Bedöm behovet av att genomföra en konsekvens-bedömning

Personuppgiftsansvariga kan överväga att behandla personuppgifter av en mängd skäl, exempelvis med anledning av ett utvecklingsarbete, en ny verksamhetsprocess eller ett inköp av ett nytt verksamhetssystem. Det blir då aktuellt att bedöma om en konsekvensbedömning måste genomföras. Om den personuppgiftsansvarige har utsett ett dataskyddsombud bör detta alltid rådfrågas om behovet av att genomföra en konsekvensbedömning.

IMY har tagit fram en mall för att bedöma behovet av att genomföra en konsekvensbedömning. Mallen är framtagen för att underlätta för personuppgiftsansvariga att på ett strukturerat sätt dokumentera denna.

Mall till stöd i arbetet

IMY:s mall för Bedömning av behovet av konsekvensbedömning enligt dataskyddsförordningen

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

1.1 Skyldigheten att genomföra en konsekvensbedömning

En konsekvensbedömning ska genomföras 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.[18] Att det är *typen av behandling* som är ifråga när behovet av konsekvensbedömning ska bedömas, betyder att åtgärder som kan reducera eller eliminera risker vid den enskilda planerade behandlingen inte ska beaktas i detta steg.

Konsekvensbedömningen ska som huvudregel genomföras innan behandlingen påbörjas. En konsekvensbedömning kan dock även behöva genomföras om den personuppgiftsansvarige fattar beslut som förändrar riskerna med en behandling som redan pågår. Dvs. om den övergår i att bli en sådan *typ av behandling* som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

18 Artikel 35.1 i dataskyddsförordningen.

Stöd i att bedöma om det finns ett behov av konsekvensbedömning

Vid bedömningen av om en konsekvensbedömning är obligatorisk ska den personuppgiftsansvarige utgå från följande rättskällor:

1 Faktorerna som anges i artikel 35.1 i dataskyddsförordningen.

I artikel 35.1 nämns vissa faktorer som ska tas särskild hänsyn till när ni bedömer om en konsekvensbedömning behöver genomföras. De är

- användning av ny teknik
- behandlingens art
- behandlingens omfattning
- behandlingens sammanhang
- behandlingens ändamål.

2 Exemplen som ges i artikel 35.3 i dataskyddsförordningen.

De exempel som nämns är:

- 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.
- 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 lagöverträdelser som innefattar brott, som avses i artikel 10.
- Systematisk övervakning av en allmän plats i stor omfattning.

3 IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen.

Förteckningen kompletterar de exempel som ges i artikel 35.3 i dataskyddsförordningen och bygger på de kriterier som anges i EDPB:s riktlinjer om konsekvensbedömning.

Som huvudregel ska en konsekvensbedömning genomföras om den planerade personuppgiftsbehandlingen uppfyller minst två av de nio kriterierna i IMY:s förteckning. Förteckningen är inte uttömmande. En konsekvensbedömning kan behöva genomföras i ett enskilt fall även om bara ett av kriterierna i förteckningen är uppfyllt.

Fördjupad information

Bilagan Rättsligt tolkningsstöd: Avsnitt 4. Stöd i att bedöma om en konsekvensbedömning ska genomföras
IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

Läs mer om skyldigheten att genomföra konsekvensbedömning på enskilda områden

IMY:s webbplats IMY.se – Konsekvensbedömning – personuppgifter i arbetslivet
IMY:s webbplats IMY.se – Konsekvensbedömning inför kamerabevakning

1.2 Ingen skyldighet att genomföra en konsekvensbedömning

Den personuppgiftsansvarige är inte skyldig att genomföra en konsekvensbedömning när:

- **Det inte är fråga om en ”typ av behandling” som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.**
  Inför de flesta behandlingar av personuppgifter behöver en konsekvensbedömning inte genomföras. Personuppgiftsansvariga måste dock kontinuerligt analysera risker som uppkommer i samband med deras behandlingar för att uppmärksamma om en behandling övergår i att bli en ”typ av behandling” för vilken en konsekvensbedömning måste genomföras.

- **Det är fråga om en behandling som är mycket lik en behandling för vilken det redan har genomförts en konsekvensbedömning.**
  För att en tidigare gjord konsekvensbedömning ska kunna användas för en ny, planerad behandling krävs att behandlingarna liknar varandra i fråga om art, omfattning, sammanhang, ändamål och risker. Möjligheten att göra en konsekvensbedömning för flera behandlingar innebär också att flera olika personuppgiftsansvariga kan göra en gemensam konsekvensbedömning för olika behandlingar, så länge de planerade behandlingarna är tillräckligt lika.[19]

  Generellt sett krävs att behandlingarna är mycket lika varandra för att en enda konsekvensbedömning ska vara tillräcklig. Den personuppgiftsansvarige måste kunna motivera att den planerade behandlingen är tillräckligt lik den tidigare eller den gemensamma behandlingen.

- **Det har gjorts en allmän konsekvensbedömning i samband med författningsarbetet.**
  Lagstiftaren kan inom ramen för författningsarbetet genomföra en allmän konsekvensbedömning för att underlätta för de berörda personuppgiftsansvariga (exempelvis de myndigheter eller andra aktörer som får arbetsuppgifter enligt den nya lagstiftningen).[20] I författningsarbeten görs dock sällan en så heltäckande konsekvensbedömning som krävs enligt dataskyddsförordningen, vilket innebär att den personuppgiftsansvarige ofta måste komplettera med en egen konsekvensbedömning av de praktiska, tekniska och organisatoriska förutsättningarna för behandlingen.[21]

Fördjupad information

Bilagan Rättsligt tolkningsstöd: Avsnitt 4.4. Ingen skyldighet att genomföra en konsekvensbedömning

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

19 Jfr artikel 35.1 i dataskyddsförordningen.
20 Artikel 35.10 i dataskyddsförordningen. Jfr skäl 93 till dataskyddsförordningen.
21 Se 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.

Steg 2.
Sätt ihop en arbetsgrupp och planera arbetet

När den personuppgiftsansvarige har bedömt att en konsekvensbedömning ska genomföras är nästa steg att planera genomförandet och bestämma vilka resurser som behöver avsättas.

För större organisationer är det lämpligt att sätta ihop en arbetsgrupp som består av personer som har kunskap om:

- den information som ska behandlas (t.ex. en medarbetare som ska arbeta i den process eller med det system där uppgifterna ska behandlas)
- hur behandlingen ska utföras rent tekniskt (t.ex. en IT-tekniker)
- informationssäkerhet och riskhantering (t.ex. verksamhetens informationssäkerhetsansvariga)
- dataskyddslagstiftningen (t.ex. en dataskyddsjurist).

Mindre organisationer har sällan alla dessa kompetenser på plats, och ibland kan samma person därför behöva ha flera roller. För att säkerställa att olika perspektiv beaktas är det ofta att föredra om flera personer med olika kompetens deltar i att genomföra konsekvensbedömningen.

För att underlätta arbetet med konsekvensbedömningen bör den personuppgiftsansvarige utse en person i arbetsgruppen som är ansvarig för att samordna och driva genomförandeprocessen framåt. I många organisationer är det dataskyddsombudet som har mest kunskap om konsekvensbedömningar och tillämplig reglering. Det är dock viktigt att den personuppgiftsansvariga organisationen är införstådd med att det inte är dataskyddsombudet som ska ansvara för att utföra konsekvensbedömningen.

Redan i det inledande skedet av processen bör den personuppgiftsansvarige även identifiera vem (person och funktion) som är behörig att besluta om eller anta konsekvensbedömningen.

Därefter bör en tidplan för arbetet upprättas. Tänk på att avsätta tid för att förankra konsekvensbedömningen med ledningen och dataskyddsombudet, och − när det är lämpligt − för att hämta in de registrerades synpunkter.

Fördjupad information

Bilagan Rättsligt tolkningsstöd: Avsnitt 6. Dataskyddsombudets roll i konsekvensbedömningen

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

Steg 3.
Gör en systematisk beskrivning av person-uppgiftsbehandlingen

Att behandlingen och ändamålen med den ska beskrivas *systematiskt*[22] innebär att beskrivningen ska göras på ett grundligt och metodiskt sätt. Det är viktigt att beskrivningen av behandlingen är tydlig, och så heltäckande som möjligt, för att den personuppgiftsansvarige ska kunna skapa sig en fullständig överblick av behandlingen. Beskrivningen ska fungera som en grund för det fortsatta arbetet med konsekvensbedömningen. När ni bedömer vad som är relevant att beskriva i respektive del bör ni ha i åtanke att det är behandlingens påverkan på enskildas fri- och rättigheter som ska bedömas inom ramen för konsekvensbedömningen.

Följande bör framgå av den systematiska beskrivningen:

- **behandlingens art** (se avsnitt 3.1)
- **behandlingens omfattning** (se avsnitt 3.2)
- **behandlingens sammanhang** (se avsnitt 3.3)
- **behandlingens ändamål** (se avsnitt 3.4)
- **nödvändiga resurser** (se avsnitt 3.5)
- **funktionell beskrivning av behandlingen** (se avsnitt 3.6)
- **roller och ansvarsfördelning** (se avsnitt 3.7).

3.1 Behandlingens art

Allmän beskrivning och bakgrund

När personuppgiftsbehandlingen ska beskrivas är det lämpligt att börja med att definiera och avgränsa konsekvensbedömningens objekt, dvs. den aktuella produkten, tjänsten, programvaran eller processen. Det bildar en ram för den mer detaljerade beskrivningen av behandlingen som ska göras senare och tydliggör behandlingens kontext. Den inledande beskrivningen kan även innehålla en bakgrund till att behandlingen planeras (exempelvis att det har skett en verksamhetsförändring eller lagändring). Om det är ett komplext system som tas i bruk blir det ibland fråga om flera olika typer av behandlingar i samma system. Då är det ofta lämpligt att dela upp beskrivningen i flera delar.

Behovet av att genomföra en konsekvensbedömning identifieras ibland i samband med en behovsanalys, förstudie inför upphandling, processkartläggning, informationsklassning eller en riskanalys. Dokumentation från sådana arbeten är ofta användbar när behandlingen ska beskrivas. Det är dock viktigt att komma ihåg att beskrivningen ska möjliggöra för läsarna – dvs. de registrerade, organisationens ledning, dataskyddsombud, tillsynsmyndigheten och andra intressenter – att förstå behandlingsåtgärderna, vad de innebär och syftena med dem. Det är därför inte tillräckligt att enbart hänvisa till annan dokumentation för att uppfylla kravet på en systematisk beskrivning.

22 Kravet på systematisk beskrivning framgår av artikel 35.7 a i dataskyddsförordningen.

Kategorier av personuppgifter

Det är mycket viktigt att identifiera och beskriva de typer av personuppgifter som kommer att behandlas. Exempel på typer av personuppgifter kan vara uppgifter om

- ålder
- kön
- utbildning
- lön
- bildmaterial på människor
- ljudupptagning av röster.

Det är inte alltid självklart vad som är en personuppgift. Kom ihåg att tekniska data (exempelvis IP-adresser), spårningsdata (exempelvis kakor) eller registreringsnummer på bilar också kan vara personuppgifter.

Läs mer
IMY:s webbplats imy.se − Personuppgifter

Särskilda kategorier av personuppgifter (”känsliga personuppgifter”)

Det finns kategorier av personuppgifter som anses särskilt känsliga. Dit hör uppgifter som avslöjar ”ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, eller medlemskap i fackförening och uppgifter om hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter för att entydigt identifiera en person”.[23]

Utgångspunkten är att det är förbjudet att behandla sådana personuppgifter.[24] Det finns dock undantag. Om den planerade behandlingen omfattar känsliga personuppgifter måste det säkerställas att något av undantagen dataskyddsförordningen gäller för att behandlingen ska vara tillåten.[25] Ibland behövs det stöd i kompletterande nationell rätt, EU-rätt eller kollektivavtal för att behandling av sådana uppgifter ska vara tillåten. Konsekvensbedömningen bör i förekommande fall innehålla en beskrivning av det rättsliga stödet för att behandla särskilda kategorier av personuppgifter.

Läs mer
IMY:s webbplats imy.se − Känsliga personuppgifter

23 Artikel 9.1 i dataskyddsförordningen.
24 Artikel 9.1 i dataskyddsförordningen.
25 Undantagen framgår av artikel 9.2 i dataskyddsförordningen.

Personuppgifter som rör lagöverträdelser

Enligt dataskyddsförordningen får personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott endast behandlas under ”kontroll av en myndighet” eller om det finns lagstöd för behandlingen.[26] Om den personuppgifts-ansvarige inte är en myndighet och denna typ av uppgifter ingår i den planerade behandlingen bör den personuppgiftsansvarige noga säkerställa och ange lagstöd.

Läs mer

IMY:s webbplats imy.se − Personuppgifter om lagöverträdelser

Särskilt skyddsvärda personuppgifter

Vissa personuppgifter anses särskilt skyddsvärda trots att de inte tillhör någon av kategorierna ovan. Personuppgifter om barn och om personnummer är exempel på särskilt skyddsvärda personuppgifter. Det är därför viktigt att uppmärksamma om sådana uppgifter kommer att behandlas, och att i så fall uppskatta mängden sådana personuppgifter (exempelvis hur stor andel som rör barn).

26 Artikel 10 i dataskyddsförordningen.

Kategorier av registrerade

Av beskrivningen bör framgå vilka kategorier av registrerade som kommer att omfattas av behandlingen, exempelvis ”anställda” eller ”kunder”. Om de registrerade står i någon form av beroendeförhållande till den personuppgiftsansvarige (exempelvis anställda, patienter eller elever) bör detta anges. Det bör även framgå om någon eller några av kategorierna inkluderar barn eller andra särskilt sårbara grupper, exempelvis äldre eller personer med funktionsvariationer.

3.2 Behandlingens omfattning

Det är viktigt att göra en uppskattning av hur omfattande behandlingen väntas bli ifråga om antalet berörda individer och mängden personuppgifter. Även antalet olika kategorier av personuppgifter är relevant. Om det är svårt att bedöma detta (exempelvis för att det är osäkert hur stort intresset för produkten kommer att vara) bör den personuppgiftsansvarige ta höjd för olika scenarier i sin beskrivning. Behandlingens omfattning har generellt sett stor betydelse vid bedömningen och hanteringen av risker som senare ska genomföras. Även den geografiska omfattningen av behandlingen, dvs. i vilka länder uppgifterna kommer att behandlas och om det är fråga om länder utanför EU/EES, bör anges.

3.3 Behandlingens sammanhang

Att beskriva behandlingens sammanhang handlar om att redogöra för behandlingen utifrån ett större perspektiv med hänsyn till olika interna och externa faktorer.
Det kan exempelvis handla om

- tidigare erfarenheter av liknande behandlingar eller att detta saknas
- att verksamheten tidigare upplevt problem vid liknande behandlingar
- att behandlingen är innovativ på något sätt
- att behandlingen kan tänkas bli ifrågasatt eller upplevas som oförutsägbar
- den utsträckning i vilken enskilda kommer att ha kontroll över sina personuppgifter
- relevanta uppförandekoder eller andra certifieringssystem.

3.4 Behandlingens ändamål

Det är av central betydelse att behandling av personuppgifter har ett eller flera tydligt fastställda ändamål. Den personuppgiftsansvarige behöver ha helt klart för sig vad som ska uppnås med den planerade behandlingen och kunna specificera detta. Om det finns flera ändamål är det viktigt att göra åtskillnad mellan dessa. En detaljerad beskrivning i denna del är viktigt för att senare kunna bedöma om behandlingen uppfyller dataskyddsförordningens krav på nödvändighet och proportionalitet.

3.5 Nödvändiga resurser

Den personuppgiftsansvarige behöver identifiera vilka resurser som är nödvändiga för att utföra den planerade behandlingen. Det underlättar det framtida arbetet med att identifiera vilka potentiella risker som är kopplade till varje resurs. Det kan exempelvis handla om programvara, servrar, hårdvara, nätverk, molntjänster, m.m.

3.6 Funktionell beskrivning av behandlingen

I den funktionella beskrivningen ska den personuppgiftsansvarige beskriva hur behandlingen går till mer i detalj. I denna del kan ett flödesschema bidra till att förklara hur personuppgifterna ”rör sig”. Ett sådant schema är även användbart senare i konsekvensbedömningen när riskerna ska identifieras.

Av den funktionella beskrivningen bör det framgå hur personuppgifterna ska samlas in och varifrån de kommer (exempelvis om de kommer direkt från den registrerade via enkäter, webbformulär eller intervjuer, eller om de ska hämtas in utan den registrerades vetskap via offentliga uppgiftssamlingar eller databaser). Det bör framgå hur registreringen och informationsöverföringen av uppgifterna ska gå till (exempelvis om pappersenkäter ska skickas till en inläsningscentral eller om några uppgifter ska lämnas via telefon eller något digitalt verktyg). Det bör även tydliggöras vilka system som ska användas i de olika delarna av behandlingen, hur länge personuppgifterna ska lagras och rutinerna för radering eller anonymisering.

Det är viktigt att motivera lagringstiden och förklara vad som ligger till grund för den (exempelvis lagkrav eller speciella verksamhetskrav). Om det inte är möjligt att fastställa en uttrycklig sluttid för en behandling av personuppgifter (exempelvis två år från registreringen) bör behandlingstidens längd uttryckas på något annat sätt som kan följas upp av den personuppgiftsansvarige.

3.7 Roller och ansvarsfördelning

Personuppgiftsansvar

Ibland kan flera personuppgiftsansvariga vara inblandade i en och samma behandling. Det är då mycket viktigt att reda ut och tydliggöra ansvarsfördelningen innan behandlingen påbörjas. Specificera noga den eller de personuppgiftsansvariga, dvs. de aktörer som ensamt eller tillsammans bestämmer ändamålen och tillvägagångssätten för behandlingen av personuppgifterna.[27] Ange om behandlingen innebär ett gemensamt personuppgiftsansvar med en annan aktör eller om någon av aktörerna kommer att vara personuppgiftsbiträde. Ansvarsfördelningen bör finnas noggrant dokumenterad.

Mottagare inklusive personuppgiftsbiträden

Ofta finns det ett behov av att dela personuppgifterna med olika mottagare. Beskrivningen av behandlingen bör innehålla information om vilka som kommer att få del av personuppgifterna vid den planerade behandlingen (exempelvis IT-leverantörer eller andra bolag inom samma koncern).

Det bör framgå av konsekvensbedömningen om personuppgiftsbiträden kommer att vara involverade i behandlingen, och i så fall deras identitet (inklusive organisationsnummer och adress till verksamhetsstället), vilka tjänster som personuppgiftsbiträdet utför och landet där personuppgiftsbiträdet behandlar uppgifterna.

Läs mer

IMY:s webbplats imy.se – Personuppgiftsansvariga och personuppgiftsbiträden

27 Jfr artikel 4.7 i dataskyddsförordningen.

Steg 4.
Genomför en rättslig analys

Nästa steg är att bedöma om de rättsliga förutsättningarna för att genomföra behandlingen är uppfyllda. Det ger en god indikation på hur nödvändig och proportionerlig behandlingen är i förhållande till syftena med den. Om den planerade behandlingen inte är förenlig med gällande dataskyddslagstiftning (exempelvis för att den saknar rättslig grund) är den olaglig och får inte genomföras. En konsekvensbedömning kan inte ändra på det. Om behandlingen är olaglig saknas därmed skäl att gå vidare till nästa steg i konsekvensbedömningen.

4.1 Gällande regelverk

Börja med att sammanställa gällande regelverk. Utöver dataskyddsförordningen och dataskyddslagen[28] kan exempelvis marknadsföringslagar och myndighetsspecifik registerlagstiftning aktualiseras. Även antagna uppförandekoder, genomförda certifieringar och branschpraxis ska identifieras.

Läs mer

IMY:s webbplats imy.se − Så hänger lagarna ihop
IMY:s webbplats imy.se − Uppförandekoder enligt GDPR

4.2 Säkerställ att dataskyddsprinciperna följs och att det finns rättslig grund för behandlingen

Enligt dataskyddsförordningen gäller följande grundläggande principer vid behandling av personuppgifter:

- **laglighet, korrekthet och öppenhet** (artikel 5.1 a)
- **ändamålsbegränsning** (artikel 5.1 b)
- **uppgiftsminimering** (artikel 5.1 c)
- **riktighet** (artikel 5.1 d)
- **lagringsminimering** (artikel 5.1 e)
- **integritet och konfidentialitet** (artikel 5.1 f).

Konsekvensbedömningen ska innehålla en beskrivning av hur den planerade behandlingen lever upp till dessa principer. Att de grundläggande dataskyddsprinciperna följs är en central del i att säkerställa att behandlingen är nödvändig och proportionerlig.

28 Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Principen om laglighet, korrekthet och öppenhet

Laglighet

För att uppfylla principen om laglighet måste bestämmelserna i dataskyddsförordningen och annan kompletterande lagstiftning följas.

En grundförutsättning för att en behandling av personuppgifter ska vara laglig är att den har stöd i en rättslig grund.[29] Det finns sex rättsliga grunder:

- samtycke
- rättslig förpliktelse
- avtal
- skydd av grundläggande intresse
- myndighetsutövning och allmänt intresse
- intresseavvägning.

Den rättsliga grunden (eller grunderna) för den aktuella behandlingen ska finnas tydligt angiven i konsekvensbedömningen. Ibland kan en behandling stödjas på mer än en rättslig grund och det är i så fall viktigt att vara tydlig med vilken rättslig grund som används i det aktuella fallet. Det kan också vara så att olika delar av behandlingen ska stödjas på olika grunder, vilket också måste tydliggöras. Den rättsliga grundens giltighet och rimlighet ska motiveras. Om den rättsliga grunden är intresseavvägning[30] ska även en bedömning av intresseavvägningen dokumenteras.

29 Artikel 6.1 a–f i dataskyddsförordningen.
30 Artikel 6.1 f i dataskyddsförordningen.

Det krävs rättslig grund för att behandla personuppgifter

Samtycke (artikel 6.1 a)

Om samtycke övervägs som rättslig grund ska den personuppgiftsansvarige beakta villkoren för samtycke i artikel 7 i dataskyddsförordningen, vilket bl.a. innebär att:

- Den registrerades samtycke ska vara en frivillig, specifik, informerad och otvetydig viljeyttring i dataskyddsförordningens mening.
- Den personuppgiftsansvarige ska kunna visa att den registrerade har samtyckt till behandlingen av sina personuppgifter.
- Den registrerade har rätt att när som helst återkalla sitt samtycke, och att det ska vara lika lätt att återkalla som att ge sitt samtycke.
- Samtycket ska vara utformat enligt kraven i dataskyddsförordningen.

Avtal (artikel 6.1 b)

För att denna grund ska kunna användas krävs att den registrerade själv är eller ska bli part i avtalet.

Rättslig förpliktelse (artikel 6.1 c)

För att en rättslig förpliktelse ska kunna ge rättslig grund för behandling av personuppgifter måste den vara fastställd i enlighet med unionsrätten eller en medlemsstats nationella rätt. En rättslig förpliktelse enligt svensk rätt kan följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Det är viktigt att komma ihåg att även ändamålet med behandlingen måste framgå av den aktuella förpliktelsen.

Skydd av grundläggande intresse (artikel 6.1 d)

Denna rättsliga grund aktualiseras mycket sällan. Den är främst tillämplig när människors liv eller hälsa står på spel och aktualiseras ibland inom vården.

Myndighetsutövning och allmänt intresse (artikel 6.1 e)

Förutom myndigheter och andra offentliga organ som utför uppgifter av allmänt intresse i den mening som avses, kan privata aktörer som bedriver exempelvis vård- eller skolverksamhet omfattas. För att en uppgift av allmänt intresse ska ge rättslig grund för behandling av personuppgifter måste den vara fastställd i enlighet med unionsrätten eller en medlemsstats nationella rätt.

Intresseavvägning (artikel 6.1 f)

För att en intresseavvägning ska ge rättslig grund för personuppgiftsbehandling måste tre villkor vara uppfyllda. Den personuppgiftsansvarige måste kunna visa 1) att det finns ett berättigat intresse, 2) att den aktuella behandlingen av personuppgifter är nödvändig för att uppnå det intresset, och 3) att det berättigade intresset vid en avvägning väger tyngre än de registrerades intressen eller grundläggande rättigheter eller friheter.

Korrekthet

Att personuppgifter ska behandlas *korrekt* innebär på ett generellt plan att behandlingen ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade. Att behandlingen ska vara rättvis innebär att personuppgifter ska behandlas på ett sätt som den registrerade kan förvänta sig, och att den inte får vara diskriminerande. Personuppgiftsbehandlingen ska stå i rimlig proportion till nyttan den innebär. Den personuppgiftsansvarige behöver därför väga sina egna intressen mot de registrerades. Bedömningen påverkas också av vilken personuppgiftsbehandling som de registrerade rimligen kan förvänta sig. Personuppgiftsbehandlingen ska vara begriplig för de registrerade och inte ske på dolda eller manipulerande sätt.

Öppenhet

Kravet på *öppenhet* innebär att det ska vara klart och tydligt för de registrerade att och hur deras personuppgifter behandlas. De registrerade ska ha möjlighet att få veta varför deras personuppgifter behandlas, hur de samlas in och hur uppgifterna används. De registrerade ska också bli informerade om sina rättigheter (exempelvis hur de kan få felaktiga uppgifter rättade och hur de kan få personuppgifter raderade). Informationen om personuppgiftsbehandlingen ska vara lätt att hitta och den ska vara formulerad på ett sätt som är enkelt och begripligt för de registrerade. Det är särskilt viktigt att använda ett klart och tydligt språk när de registrerade är barn.

Exempel på frågor för att kontrollera att principen följs:

Laglighet

- Följer verksamheten bestämmelserna i gällande lagstiftning?
- Finns det en rättslig grund för behandlingen?
- Om den rättsliga grunden är intresseavvägning, har intresseavvägningen dokumenterats?
- Om den rättsliga grunden är samtycke, är samtycket frivilligt, specifikt, informerat och otvetydigt i dataskyddsförordningens mening?
- Om den rättsliga grunden är samtycke, kan samtycket återkallas?

Korrekthet

- Sker behandlingen på ett sätt som den registrerade rimligen kan förvänta sig?

Öppenhet

- På vilket sätt informeras de registrerade om behandlingen av personuppgifter?
- Är informationen lättillgänglig för de registrerade?
- Är informationen anpassad till målgruppen (t.ex. barn)?
- Finns det rutiner för att uppdatera informationen?

Läs mer

IMY:s webbplats imy.se − Rättslig grund för behandling av personuppgifter

Principen om ändamålsbegränsning

Principen om ändamålsbegränsning innebär att personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att de inte får behandlas på ett sätt som är oförenligt med dessa ändamål. Ändamålet ska definieras innan behandlingen påbörjas och ska vara noggrant specificerat. Ändamålet med behandlingen är avgörande för att bedöma vilka uppgifter som är nödvändiga att behandla, vilken rättslig grund som behandlingen kan stödjas på och för att uppfylla övriga grundläggande dataskyddsprinciper.

Den registrerade ska utifrån beskrivningen av ändamålet kunna förstå varför och hur personuppgifterna kommer att användas. Det är viktigt att vara medveten om att ändamålet inte kan ändras efter det att behandlingen väl har påbörjats och de registrerade har informerats om ändamålet med behandlingen. Personuppgifter som har samlats in för ett visst ändamål får inte senare behandlas för ett annat ändamål som är oförenligt med det ursprungliga. Det är viktigt att ha rutiner och andra åtgärder på plats för att säkerställa detta.

Exempel på frågor för att kontrollera att principen om ändamålsbegränsning följs:

- Har ändamålet/ändamålen dokumenterats och hur?
- Är ändamålet så konkret och specifikt beskrivet att det är enkelt att fastställa att behandlingen är förenlig med detta?
- Har behandling av uppgifterna för andra ändamål än de fastställda begränsats genom exempelvis avtalsklausuler, riktlinjer eller andra säkerhetsåtgärder?

Principen om uppgiftsminimering

Principen om uppgiftsminimering innebär att de personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen som de behandlas för. Beskriv hur (genom vilka åtgärder) det ska säkerställas att enbart personuppgifter som behövs för ändamålet kommer att behandlas. Det bör även framgå att den personuppgiftsansvarige har övervägt om det finns alternativa sätt att utföra behandlingen som är lika effektiva för att uppnå syftet, men som i mindre utsträckning gör intrång i enskildas grundläggande fri- och rättigheter (exempelvis genom att de medför en begränsad uppgiftsinsamling eller kräver mindre detaljerade uppgifter). Om ändamålet kan uppnås utan att vissa uppgifter behandlas, är behandlingen av just dessa personuppgifter inte nödvändig och ska inte utföras.

Exempel på frågor för att kontrollera att principen om uppgiftsminimering följs:

- Framgår det tydligt varför de personuppgifter som ska behandlas behövs för att uppfylla ändamålet med den aktuella behandlingen?
- Har ni kontrollerat att inga uppgifter samlas in enbart ”för att de kan vara bra att ha”?
- Fritextfält i formulär: Är det nödvändigt att använda sådana? Ges det tydliga instruktioner om vad som ska anges i fritextfälten (för att motverka insamling av onödiga uppgifter)? Framgår det tydligt vilka fält som är frivilliga respektive obligatoriska? Är de frivilliga fälten verkligen nödvändiga för att uppnå ändamålet med behandlingen?
- Kamerabevakning: Är det nödvändigt att samla in uppgifter från hela kamerans upptagningsområde eller bör vissa delar maskeras digitalt?

Principen om riktighet

Personuppgifter som behandlas ska vara riktiga och (om nödvändigt) uppdaterade. Om personuppgifterna inte stämmer ska uppgifterna rättas eller raderas. Det är därför viktigt att det finns rutiner för att upptäcka fel och för att korrigera och ta bort oriktiga personuppgifter när registrerade begär det.

Exempel på frågor för att kontrollera att principen om riktighet följs:

- Är uppgifterna statiska eller kräver de uppdateringar?
- Hur säkerställs att felaktiga uppgifter rättas?
- Hur ofta ska uppgifternas riktighet kontrolleras?
- Kan den registrerade själv påverka uppgifternas korrekthet och vid behov uppdatera dem?
- Hur säkerställs att uppgifter som har mottagits från en annan verksamhet är korrekta?
- Hur säkerställs att de insamlade uppgifterna gäller rätt person?

Principen om lagringsminimering

Principen om lagringsminimering innebär att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Den planerade lagringstiden bör därför motiveras utifrån vad som är nödvändigt för syftet med behandlingen. Eftersom det som är nödvändigt inte alltid är proportionerligt, behöver även proportionaliteten motiveras. Det är viktigt att det finns rutiner för gallring av personuppgifter.

Exempel på frågor för att kontrollera att principen om lagringsminimering följs:

- För vilka ändamål ska uppgifterna behandlas och hur länge ska de behandlas?
- Kommer uppgifterna att raderas när de inte längre behövs och hur ska det gå till i praktiken?
- Finns det lagkrav som bestämmer lagringstiden för de person-uppgifter som behandlas?
- Kommer det att vara möjligt att använda automatisk radering av uppgifter när lagringstiden har löpt ut, eller ska uppgifterna raderas manuellt?
- Om radering inte är lämpligt, kommer personuppgifterna att anonymiseras?

Principen om integritet och konfidentialitet

Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att trygga personuppgifternas integritet och konfidentialitet.

Integritet handlar om att uppgifterna förblir oförändrade när de behandlas, överförs och lagras. Personuppgifterna ska alltså skyddas mot att obehörigen gå förlorade, förstöras eller redigeras avsiktligt eller av misstag. Med konfidentialitet avses att personuppgifterna endast ska vara tillgängliga för dem som på grund av sina arbetsuppgifter har behov av och rätt att få tillgång till dem. Personuppgifterna ska skyddas så att de inte kan läsas eller på annat sätt behandlas av obehöriga.

Exempel på frågor för att kontrollera att principen följs:

Integritet

- Finns det riktlinjer eller rutiner för hur uppgifter får ändras och av vem?
- Görs säkerhetskopior och hur ser rutinerna för det ut?
- Sker loggning när uppgifterna ändras?

Konfidentialitet

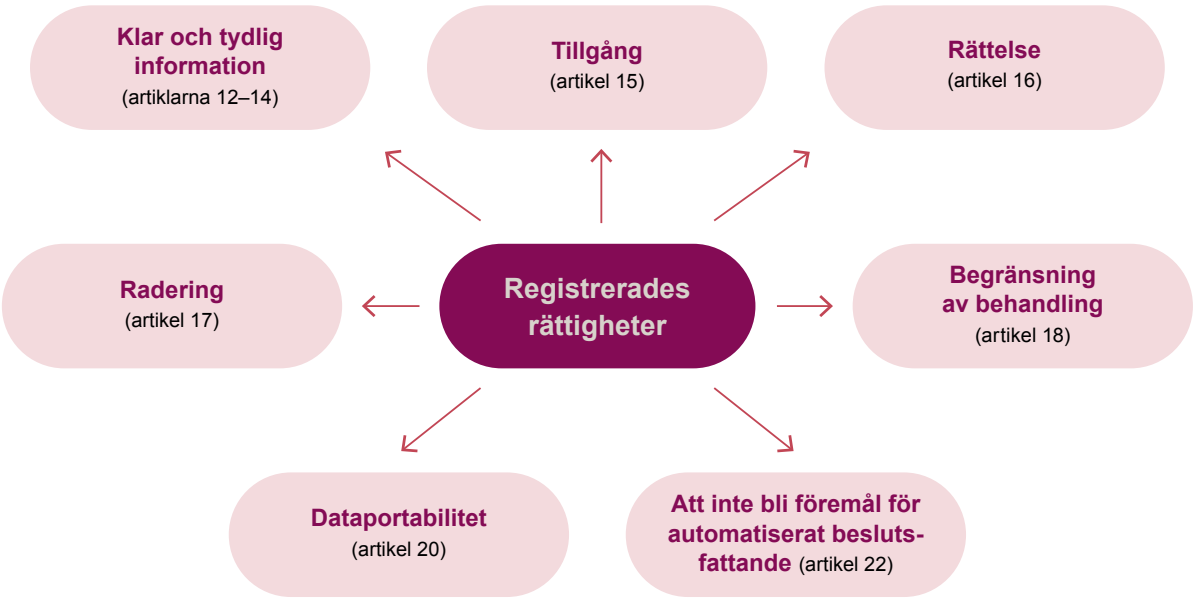
- Finns det rutiner och åtgärder för behörighetsstyrning?
- Finns det tillämpliga sekretessbestämmelser för uppgifterna?
- Har de personer som ska hantera uppgifterna en tillräckligt god kännedom om konfidentialitet och gällande sekretess?

Läs mer

IMY:s webbplats imy.se − Grundläggande principer enligt GDPR

4.3 Säkerställ att registrerades rättigheter kan tillgodoses

De registrerade har ett antal rättigheter som framgår av kapitel III i dataskyddsförordningen. Den personuppgiftsansvarige behöver säkerställa att dessa rättigheter kommer att kunna tillgodoses vid behandlingen. Den registrerade har (med vissa undantag) rätt till:



Exempel på frågor för att kontrollera att de registrerades rättigheter kan tillgodoses:

- Hur får de registrerade hjälp att utöva sina rättigheter enligt dataskyddförordningen?
- Finns det ett formulär eller någon annan kontaktkanal för registrerade som vill utöva sina rättigheter?
- Är informationen lätt att hitta för de registrerade?
- Finns det en process för att hantera de registrerades begäranden?
- Finns det en ansvarig person som säkerställer att de registrerades rättigheter kan tillgodoses?
- Får de registrerade tydlig och tillräcklig information om behandlingen av sina personuppgifter?
- Kan alla uppgifter som gäller de registrerade sammanställas?
- Kan en kopia av de registrerades uppgifter tas fram på ett enkelt sätt?
- Går det att lämna uppgifterna i elektronisk form om de registrerade begär det?
- Hur fungerar rutinen för att radera personuppgifter om registrerade återkallar sitt samtycke till behandlingen?
- Hur raderas uppgifterna i praktiken (manuell eller automatiserad radering)?
- Finns det hinder för raderingen (som lagstadgade lagringstider eller liknande)?
- Hur utövas rätten till dataportabilitet i praktiken? Är det tekniskt möjligt?
- Omfattar behandlingen av personuppgifter automatiserat beslutsfattande som i betydande grad påverkar den registrerade? Om ja, vad baseras detta på?

Läs mer

IMY:s webbplats imy.se – De registrerades rättigheter

4.4 Skyddsåtgärder för internationella överföringar

Personuppgifter får bara överföras till ett land utanför EU/EES, s.k. tredjeland, under vissa förutsättningar. För att en sådan tredjelandsöverföring ska vara tillåten krävs att den personuppgiftsansvarige säkerställer en tillräcklig nivå av skydd för fysiska personers fri- och rättigheter.[31] Exempel på säkerhetsåtgärder som kan göra tredjelandsöverföringen tillåten är bindande företagsbestämmelser, standardavtalsklausuler eller ett beslut från EU-kommissionen om adekvat skyddsnivå.

Om personuppgifter kommer att överföras till tredjeland ska den personuppgifts-ansvarige kunna visa att överföringen är laglig.

Läs mer

IMY:s webbplats imy.se − Överföring av personuppgifter till tredjeland

4.5 Gör en sammantagen bedömning

Innan ni påbörjar riskhanteringen bör en sammantagen bedömning av den rättsliga analysen göras. Dokumentera bedömningen av om behandlingen är nödvändig och proportionerlig i förhållande till syftena med den. Den sammantagna bedömningen i steg 4 bör leda till ett ställningstagande av om behandlingen, i den form som planeras, uppfyller de rättsliga förutsättningarna i dataskyddsförordningen och kompletterande lagstiftning. Om behandlingen inte uppfyller de rättsliga förutsättningarna ska behand-lingen inte genomföras på det sätt som planeras.

Observera att en samlad bedömning av behandlingens nödvändighet och proportionalitet i förhållande till syftena, även bör göras efter att riskhanteringen har genomförts och relevanta synpunkter har hämtats in (se steg 8). Detta för att säkerställa att nyttan med behandlingen står i rimlig proportion till de risker för enskildas fri- och rättigheter som har identifierats.

31 Bestämmelserna om överföring av personuppgifter till tredjeländer eller internationella organisationer framgår av Kapitel V i dataskyddsförordningen.

Steg 5.
Hantera risker: identifiera, analysera och åtgärda risker

Efter att den systematiska beskrivningen och den rättsliga analysen (inklusive bedömningen av behandlingens nödvändighet och proportionalitet) har genomförts, är det dags att genomföra riskhanteringen.

Riskhanteringen handlar om att:

1. **identifiera de risker för fysiska personers fri- och rättigheter som behandlingen innebär** (se avsnitt 5.1)
2. **analysera de identifierade riskerna utifrån hur sannolikt det är att de blir verklighet och hur allvarligt det i sådana fall vore om de inträffade**
   (se avsnitt 5.2)
3. **beskriva de riskreducerande åtgärderna**
   (se avsnitt 5.3)
4. **följa upp riskerna och göra ny riskbedömning**
   (se avsnitt 5.4).

Riskerna har ofta redan bedömts översiktligt när den personuppgiftsansvarige beslutade att genomföra en konsekvensbedömning. Denna inledande riskbedömning är ofta till nytta när riskerna ska bedömas inom ramen för själva konsekvensbedömningen. Bedömningen och hanteringen av riskerna kan genomföras vid en eller flera workshops där personer med olika kompetenser deltar. Om ett dataskyddsombud har utsetts bör detta rådfrågas i samband med riskbedömningen och vid bedömningen av riskreducerande åtgärder.

Mall till stöd i arbetet

Använd gärna Excelbilagan Riskhantering vid konsekvensbedömning för att underlätta utförandet av riskhanteringen och dokumentationen av identifierade risker, riskanalys och identifierade riskreducerande åtgärder.

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

Kom ihåg!

Det är skillnad mellan risk- och sårbarhetsanalyser i verksamhetens generella informationssäkerhetsarbete och den riskbedömning som ska göras inom ramen för en konsekvensbedömning avseende dataskydd. Den sistnämnda syftar till att skydda information vid behandling av personuppgifter och till att säkerställa att dataskyddsförordningen följs. Det är skyddet av enskildas fri- och rättigheter som är relevant. Informationssäkerhet handlar istället generellt sett om att skydda all typ av information som en organisation hanterar. Syftet kan exempelvis vara att upprätthålla samhällsviktiga funktioner eller verksamhetens egen förmåga att verka.

5.1 Identifiera riskerna

För att det ska vara möjligt att identifiera de risker som en viss personuppgifts-behandling kan innebära för enskilda personers fri- och rättigheter krävs att ni beaktar både interna och externa faktorer. En förutsättning för att kunna identifiera risker är att det är klarlagt vilka typer av personuppgifter som ska behandlas, för vilka ändamål och på vilket sätt.

Det är helt centralt att riskbedömningen görs utifrån enskildas perspektiv. Ibland antas felaktigt att det är risker för verksamheten som ska hanteras i detta steg. De risker som ska identifieras, bedömas och hanteras inom ramen för en konsekvensbedömning avseende dataskydd enligt artikel 35 i dataskyddsförordningen, är dock enbart sådana som avser enskilda personers fri- och rättigheter. I första hand deras 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).

Begreppet *risk* inom ramen för en konsekvensbedömning kan definieras som en brist, svaghet eller sårbarhet i samband med behandling av personuppgifter. Det kan också vara ett hot eller en händelse i anslutning till en behandling som kan ha en skadlig inverkan på efterlevnaden av dataskyddsprinciperna och få negativa konsekvenser på enskilda ifråga om deras fri- och rättigheter. Det är därmed fråga om hypotetiska scenarier med olika konsekvenser. Risker kan härröra från externa hot (exempelvis cyberattacker eller skadlig programvara) eller interna hot (exempelvis felaktig använd-ning av data eller bristande säkerhetsåtgärder i system). Risker kan uppstå både på grund av avsiktligt och oavsiktligt agerande.

Förutom risker för skador, kan personuppgiftsansvariga behöva ta hänsyn till risker för andra typer av negativa effekter för enskilda. Både för personer som berörs av behandlingen i fråga (exempelvis att de utsätts för diskriminering, identitetsstöld, ekonomisk förlust eller skadat anseende)[32] och för samhället i stort (exempelvis förlust av socialt förtroende).[33] I skäl 75 till dataskyddsförordningen ges fler exempel på vad som kan ses som risker för fysiska personers fri- och rättigheter.

Exempel på risker och vad de kan leda till

- **Risk:** För mycket information lagras via fritextfält.
  Kan leda till: Personuppgifter behandlas trots att det inte är nödvändigt.
- **Risk:** Uppgifter gallras eller avskiljs inte i tid.
  Kan leda till: Personuppgifter används för andra syften än de ursprungliga.
- **Risk:** Behörighetsstyrning tillämpas inte i praktiken.
  Kan leda till: Obehöriga får tillgång till personuppgifterna.
- **Risk:** Känsliga personuppgifter skyddas inte på tillräcklig säker-hetsnivå i produktions- respektive testmiljö.
  Kan leda till: Obehöriga får tillgång till personuppgifterna.

32 Skäl 75 till dataskyddsförordningen.
33 Jfr. Artikel 29-arbetsgruppens Yttrande om en riskbaserad metod inom den rättsliga ramen för uppgiftsskydd (WP 218), p. 11.

- **Risk:** Rutiner för loggning och logguppföljning följs inte.
  Kan leda till: Det går inte att utreda incidenter då obehöriga fått tillgång till personuppgifterna m.m.
- **Risk:** Uppgifterna överförs till tredjeland utan lagstöd.
  Kan leda till: Det saknas tillräcklig skyddsnivå för personuppgifterna.
- **Risk:** Det finns brister i ändamålsstyrning.
  Kan leda till: Personuppgifter används för andra ändamål än som avsetts ursprungligen.
- **Risk:** Det finns brister i rutiner för att kontrollera personuppgifters riktighet.
  Kan leda till: Personuppgifterna är inte korrekta.
- **Risk:** De registrerade får otillräcklig information om person-uppgiftsbehandlingen.
  Kan leda till: Enskilda kan inte ta tillvara sina rättigheter enligt dataskyddsförordningen.
- **Risk:** Det finns begränsade möjligheter att kontakta representanter för den personuppgiftsansvarige.
  Kan leda till: Enskilda kan inte ta tillvara sina rättigheter enligt dataskyddsförordningen.
- **Risk:** Det finns brister i rutiner för personuppgiftsbiträdeshantering eller otillräcklig kontroll av att dessa rutiner följs.
  Kan leda till: Personuppgifter lämnas ut till externa parter som inte kan garantera en tillräckligt säker hantering.

Fördjupad information

Bilagan Rättsligt tolkningsstöd: Avsnitt 4.1. Tolka artikel 35.1 i dataskyddsförordningen.

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

5.2 Analysera riskerna

Syftet med riskanalysen är att bedöma sannolikheten för att en oönskad händelse ska inträffa och händelsens allvarlighetsgrad, utifrån en objektiv bedömning av behandlingens art, omfattning, sammanhang och ändamål.[34] Att bedömningen ska vara objektiv innebär att risken för enskildas fri- och rättigheter inte kan tonas ned med hänvisning till sådant som att verksamheten exempelvis vill uppnå sina ekonomiska mål. Analysen av riskernas sannolikhet och allvarlighetsgrad ska göras för att den personuppgiftsansvarige sedan ska kunna avgöra vilken eller vilka åtgärder som är lämpliga för att reducera riskerna.

Bedöma riskernas sannolikhet

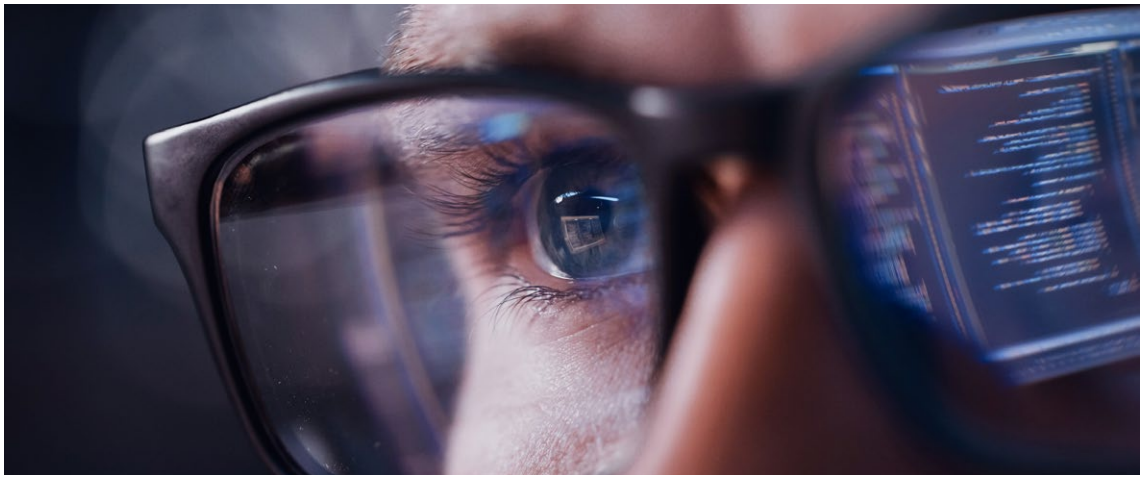
För att bedöma hur sannolikt det är att en identifierad risk blir verklighet bör bl.a. följande aspekter beaktas.

- ***Typen och omfattningen av personuppgifter***
  Vilka kategorier av personuppgifter som behandlas och mängden uppgifter kan påverka hur eftertraktade uppgifterna är och öka riskerna för antagonistiska hot.

- ***Erfarenhet och incidenthistorik***
  Genom att analysera brister och incidenter vid tidigare behandlingar kan den personuppgiftsansvarige identifiera mönster och trender som kan påverka sannolikheten för att en identifierad risk ska bli verklighet. Det är viktigt att ta hänsyn både till incidenter inom organisationen och den aktuella branschen.

- ***Effektivitet av säkerhetsåtgärder och kontroller***
  Genom att testa och utvärdera effektiviteten och robustheten hos olika säkerhetsåtgärder, och göra interna kontroller innan en personuppgiftsbehandling påbörjas, kan förmågan att förhindra och minimera risker bedömas. Det kan ske genom att utvärdera tekniska säkerhetslösningar och processer för hantering av personuppgifter samt utbildningar av personalen.

- ***Kontinuerlig översyn***
  Kontinuerlig översyn av behandlingen och säkerhetsåtgärderna kan minska sannolikheten för att riskerna inträffar. Revidering av sannolikheten bör ske i samband med nya eller förändrade omständigheter, som exempelvis byte av personuppgiftsbiträde, att en digital tjänst får nya tekniska funktioner eller att nya lagar träder i kraft.



34 Skäl 76 och 90 till dataskyddsförordningen.

Bedöm riskernas allvarlighetsgrad

För att bedöma hur allvarlig den oönskade händelsen kan bli om den inträffar bör bl.a. följande aspekter beaktas.

- ***Konsekvenser för enskildas fri- och rättigheter***
  En helt central faktor att beakta är på vilket sätt den oönskade händelsen skulle kunna skada enskildas privatliv eller påverka de registrerades möjligheter att utöva sina rättigheter enligt dataskyddsförordningen.

- ***Behandlingens art och typen av personuppgifter***
  Den aktuella riskens allvarlighetsgrad påverkas av vilken behandling som är aktuell och vilka personuppgifter som behandlas. Om en risk exempelvis involverar uppgifter om barn eller känsliga personuppgifter ökar allvarlighetsgraden.

- ***Riskens omfattning***
  Den personuppgiftsansvariges bedömning bör innefatta en analys av hur många personer som potentiellt skulle kunna påverkas om en identifierad risk faktiskt inträffar. Ju fler personer som kan tänkas drabbas, desto allvarligare är risken.

- ***Behandlingens sammanhang***
  Vid bedömningen bör den personuppgiftsansvarige även beakta om behandlingen kan upplevas som oförutsägbar. Även aspekter som den personuppgiftsansvariges relation till de enskilda personerna och i vilken utsträckning som enskilda har kontroll över sina personuppgifter bör beaktas.

Genomför riskvärdering

Nästa moment i riskhanteringen är *riskvärderingen*, då kombinationen av bedömd sannolikhet och allvarlighetsgrad ska värderas. Riskvärderingen kan göras på olika sätt, beroende på vilken typ av personuppgiftsbehandling det är fråga om.

Risk, sannolikhet och allvarlighetsgrad kan beskrivas i löpande text eller med hjälp av en s.k. riskmatris, där sannolikhet respektive allvarlighet uttrycks i en siffra mellan exempelvis 1–4 (från låg till hög sannolikhet eller allvar). En riskmatris *kan* vara ett bra verktyg för att visualisera och skapa en överblick över de identifierade riskerna och behovet av prioritering bland åtgärder inom ramen för en handlingsplan. Den personuppgiftsansvarige kan utifrån sin riskmatris och ett kombinerat siffervärde av sannolikhet och allvarlighet komma fram till en samlad värdering av risken.

I IMY:s föreslagna tillvägagångssätt och den mall för konsekvensbedömningar som IMY tagit fram används inte en riskmatris med kombinerat siffervärde. Istället kategoriseras sannolikhet och allvarlighetsgrad utifrån en fyrgradig skala varefter den samlade riskvärderingen beskrivs i löptext. Skälet är att det är svårt att omvandla bedömningar av sannolikhet för och allvarlighet av risker för enskildas fri- och rättigheter till ett kombinerat siffervärde, och att resonemangen bakom bedömningarna riskerar att gå förlorade.

5.3 Åtgärda riskerna

Efter att riskvärderingen har utförts återstår att identifiera lämpliga tekniska och organisatoriska säkerhetsåtgärder som kan reducera riskerna och säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna. Åtgärderna ska vara skräddarsydda för att hantera de specifika riskerna med den aktuella behandlingen, och stå i proportion till den specifika risken och de potentiella konsekvenserna för de enskildas fri- och rättigheter. Ni bör överväga vilka åtgärder som är mest effektiva och lämpliga för att hantera de identifierade riskerna.

Exempel på riskreducerande åtgärder för att hantera viss risk

Risken att fler personuppgifter samlas in än vad som är nödvändigt för ändamålen med behandlingen på grund av att fritextfält används för att samla in uppgifter.

- Ge information i anslutning till fritextfält om vilka uppgifter som är nödvändiga.
- Inför och genomför regelbundna kontroller, exempelvis stickprov av att de uppgifter som samlas in är nödvändiga.

Risken att system som automatiskt ska radera uppgifter utifrån de lagringsperioder som fastställts inte fungerar som det är tänkt, och att uppgifter därmed lagras under längre tid än vad som är nödvändigt.

- Genomför robusta tester av systemet.
- Inför och genomför regelbundna kontroller, exempelvis stickprov av resultatet av systemet.

Risken att rutiner för manuell radering av uppgifter utifrån de lagringsperioder som fastställts inte följs av personalen, och att uppgifter lagras under längre tid än vad som är nödvändigt.

- Genomför regelbundna utbildningsinsatser och andra aktiviteter för att påminna om vikten av att följa rutiner för manuell radering.
- Säkerställ att rutiner för manuell gallring är enkla att följa.
- Införliva hänvisningar till rutiner för manuell gallring i relevanta processer.
- Inför och genomför regelbundna kontroller, exempelvis stickprov av att personalen följer rutinerna. Om avvikelser upptäcks, utred orsakerna och vidta lämpliga åtgärder.

Dataskyddsförordningen innehåller inte något praktiskt tillvägagångssätt för riskhantering. Det finns därför möjlighet att integrera riskhanteringen som ska ske enligt dataskyddsförordningen med organisationens övriga riskhanteringsarbete och rutiner. Det är viktigt att den personuppgiftsansvarige fastställer vem som har ansvaret för att utföra riskreducerande arbetsuppgifter, både internt och i samarbete med andra parter. Detta för att löpande kunna utvärdera effektiviteten hos åtgärderna och för att kunna rapportera och korrigera eventuella identifierade brister eller hantera uppkomna incidenter. Att personuppgiftsansvariga måste kunna visa att dataskyddsförordningen följs[35] innebär att beslutsprocessen, genomförandet och förvaltningen av riskreducerande åtgärder ska dokumenteras på ett lämpligt sätt.

Att vidta rättsliga skyddsåtgärder för att friskriva organisationen från ansvar är inte en godtagbar hantering av de identifierade riskerna (att exempelvis ingå en försäkring som täcker de skador som kan uppstå för organisationen, eller ingå ett avtal som syftar till att överföra ansvaret till en tredje part, innebär inte att eventuella risker för enskildas rättigheter och friheter reduceras).

Beroende på hur åtgärderna utformas och implementeras kan de uppfylla krav i flera av artiklarna 5, 24, 25 och 32 i dataskyddsförordningen. Olika perspektiv kan resultera i olika bedömningar av vilken säkerhetsnivå som krävs för att säkerställa ett tillräckligt skydd, även om åtgärderna som vidtas för att reducera riskerna ofta är desamma. Exempelvis kan en brandvägg som filtrerar bort oönskad nättrafik skydda från hot mot både verksamhetens förmåga och enskildas fri- och rättigheter. Kryptering av information kan skydda såväl affärskritiska data som personuppgifter från obehörig åtkomst eller spridning.

35 Jfr artikel 5.2 i dataskyddsförordningen.

Exempel på riskreducerande åtgärder

Tekniska åtgärder

- funktioner för autentisering
- loggning
- teknisk åtkomstbegränsning och åtkomstkontroll
- kryptering av information
- användarvänliga och funktionella menyer, flöden och rapportfunktioner
- automatisk kontroll av uppgifter som kan uppmärksamma användaren vid felinmatning
- stöd för säkerhetskopiering och återställning
- begränsning av sökmöjligheter (t.ex. att det inte går att söka på känsliga personuppgifter)
- automatisk borttagning av personuppgifter som inte längre ska behandlas
- anonymisering av personuppgifter
- pseudonymisering av personuppgifter
- integritetsförbättrande teknologier (PET)
- teknik för att kunna upptäcka, hantera och rapportera incidenter

Organisatoriska åtgärder

- beslut om att inte samla in eller lagra viss typ av information
- skräddarsydda mallar för att garantera uppgiftsminimering
- rutiner för gallring och lagring
- rutiner för behörighetstilldelning
- tydligt definierad arbetsfördelning för enheter och anställda vid behandling av personuppgifter
- kontinuerlig information och utbildning till anställda om vilka beslut, rutiner, begränsningar m.m. som gäller vid personuppgiftsbehandling
- kvalifikationskrav för personal som är behörig att behandla person-uppgifter
- avtal med sekretessförbindelse för egen eller annans personal med tillgång till personuppgifterna (t.ex. IT-personal)
- kontroller för att säkerställa efterlevnad av rutiner och åtgärder
- uppdaterade personuppgiftsbiträdesavtal som tydligt reglerar tillgången till och behandlingen av personuppgifter hos person-uppgiftsbiträde
- information och utbildning till personal om hur de registrerade utövar sina rättigheter
- tydlig information till registrerade om personuppgiftsbehandlingen

Riskhantering inom olika branscher

Uppförandekoder och certifiering kan vara användbara för att få konkret vägledning i hur man identifierar risker och vidtar riskreducerande åtgärder. Dessa är skräddarsydda efter särdragen i en viss behandling och anpassade till tillämpningen av specifika bestämmelser för att skydda personuppgifter enligt dataskyddsförordningen.

I vissa fall kan unionslagstiftning eller nationell lagstiftning föreskriva särskilda skyddsåtgärder som ska vidtas av personuppgiftsansvariga när de utför vissa behandlingar för särskilda ändamål. Ett exempel på det från hälso- och sjukvårdens område är 4 kap. patientdatalagen (2008:355) och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

5.4 Följ upp och gör en ny riskbedömning

När de riskreducerande åtgärderna har identifierats ska riskbedömningen uppdateras. Sannolikhet och allvarlighetsgrad ska analyseras på nytt och en ny riskvärdering göras. Den nya riskvärderingen, som gjorts med beaktande av de riskreducerande åtgärderna, ska framgå av den dokumentation som upprättas i samband med riskhanteringen.

Om riskreducerande åtgärder inte är möjliga att genomföra, eller om åtgärderna inte kan sänka riskvärdet på ett tillräckligt sätt i förhållande till enskildas fri- och rättigheter, behöver den personuppgiftsansvarige genomföra ytterligare åtgärder. Om det inte är möjligt är alternativen att inte genomföra den planerade behandlingen eller att begära förhandssamråd med IMY.

Steg 6.
Begär förhandssamråd med IMY om risken förblir hög

Om riskerna förblir höga − trots att riskreducerande åtgärder har beaktats − har den personuppgiftsansvarige en skyldighet att begära förhandssamråd med IMY innan behandlingen påbörjas.[36] Detta gäller även om enbart en av de identifierade riskerna bedöms vara fortsatt hög.

Av artikel 36.3 i dataskyddsförordningen framgår vilket underlag den personuppgiftsansvarige ska lämna till tillsynsmyndigheten i samband med begäran om förhandssamråd. Vid en begäran om förhandssamråd ska konsekvensbedömningen ingå som en del av underlaget.[37] Om en konsekvensbedömning saknas eller bedöms vara bristfällig kan IMY komma att begära komplettering eller avvisa begäran om förhandssamråd.[38]

Läs mer

IMY:s webbplats imy.se − Förhandssamråd

36 Artikel 36 i dataskyddsförordningen.
37 Artikel 36.3 e i dataskyddsförordningen.
38 Jfr artikel 35.7 i dataskyddsförordningen som anger vad en konsekvensbedömning som minst ska innehålla.

Steg 7.
Hämta in synpunkter från berörda

7.1 Rekommendationer från dataskyddsombudet

Dataskyddsförordningen ställer krav på att dataskyddsombudet (om ett sådant har utsetts i organisationen) ska rådfrågas i arbetet med konsekvensbedömning.[39] Den personuppgiftsansvarige har ett visst utrymme att bestämma på vilket sätt och när dataskyddsombudet ska involveras. Dataskyddsombudet bör dock rådfrågas löpande, så tidigt som möjligt och i samband med viktiga beslut inom ramen för konsekvensbedömningen. Dataskyddsombudet bör framförallt rådfrågas inför beslutet att genomföra eller inte genomföra en konsekvensbedömning, och i samband med riskhanteringen. Dataskyddsombudet bör även ges möjlighet att utvärdera resultatet av konsekvensbedömningen.

Dataskyddsombudets rekommendationer och utlåtanden i olika skeden av konsekvensbedömningen bör i regel dokumenteras. Dataskyddsombudet bör även upprätta ett separat, skriftligt utlåtande av konsekvensbedömningen, där det bl.a. framgår hur dataskyddsombudet har involverats i genomförandet och vilken dokumentation som ligger till grund för utlåtandet. Om den personuppgiftsansvarige beslutar att inte följa en formell rekommendation från dataskyddsombudet bör den personuppgiftsansvarige även dokumentera en motivering för det.

Fördjupad information

Bilagan Rättsligt tolkningsstöd: Avsnitt 6. Dataskyddsombudets roll i konsekvensbedömningen

Allt material som hör till den praktiska guiden finns på imy.se/konsekvensbedomning

7.2 Synpunkter från de registrerade

När synpunkter behöver hämtas in

Av dataskyddsförordningen framgår att den personuppgiftsansvarige ska hämta in synpunkter från de registrerade ”när det är lämpligt”.[40] Det innebär att det inte är frivilligt att hämta in sådana synpunkter, utan när det är lämpligt, så ska det göras. Omständigheter som talar för att det är lämpligt är att den planerade behandlingen exempelvis påverkar ett stort antal registrerade, omfattar känsliga personuppgifter eller innebär automatiserat beslutsfattande.

Ett av syftena med att hämta in synpunkter från de registrerade är att få ett bra underlag för riskbedömningen och andra delar av konsekvensbedömningen. Synpunkterna bör därför hämtas in vid en tidpunkt som möjliggör för den personuppgiftsansvarige att beakta dem. De registrerade bör inte tillfrågas efter att riskbedömningen är färdigställd om den personuppgiftsansvarige inte kommer ha möjlighet att omvärdera riskerna utifrån de synpunkter som har kommit in. Ibland är det lämpligt att tillfråga de registrerade redan före eller i samband med riskbedömningen. Synpunkterna kan också bidra till att tydliggöra behandlingens lämplighet och proportionalitet för de registrerade och ge dem större insyn i hur verksamheten ska behandla deras personuppgifter.

39 T.ex. artikel 35.2 och artikel 38 i dataskyddsförordningen.
40 Artikel 35.9 i dataskyddsförordningen.

De synpunkter som hämtats in från de registrerade eller deras företrädare är inte bindande för den personuppgiftsansvarige. Oavsett vilka synpunkter de registrerade har på den avsedda behandlingen ska riskbedömningen genomföras i enlighet med kraven i dataskyddsförordningen. Den personuppgiftsansvarige kan därför inte dra slutsatsen att en planerad behandling är riskfri enbart med hänvisning till att de registrerade som tillfrågats inte har identifierat några risker med den planerade behandlingen.

Att de registrerade har lämnat sitt samtycke till en behandling innebär inte att deras synpunkter har hämtats in i aktuellt avseende.[41] En personuppgiftsansvarig kan därför inte låta bli att hämta in synpunkter enbart med hänvisning till att de registrerade har (eller kommer att ha) samtyckt till den avsedda behandlingen, om det i övrigt är lämpligt att hämta in sådana synpunkter.[42]

När synpunkter inte behöver hämtas in

Av dataskyddsförordningen framgår att den personuppgiftsansvarige inte behöver hämta in de registrerades synpunkter om det skulle påverka skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet. Exempel på godtagbara skäl till att inte hämta in de registrerades synpunkter är att det skulle äventyra företagets affärsplaner eller annan konfidentiell information om exempelvis immateriella rättigheter eller företagshemligheter. Andra godtagbara skäl kan vara att det är ogenomförbart eller att arbetsinsatsen är oproportionerlig i förhållande till de risker som behandlingen sannolikt innebär eller till de registrerades möjlighet att ge relevanta synpunkter på behandlingen.[43]

Vilka som ska tillfrågas

Vilka som ska tillfrågas beror på vilka grupper av personer som kommer att påverkas av riskerna med behandlingen. Den personuppgiftsansvarige bör särskilt hämta in synpunkter från registrerade som kan tänkas ha viktig information eller kan lämna synpunkter som är särskilt relevanta vid konsekvensbedömningen.

Av dataskyddsförordningen framgår att synpunkterna ska hämtas in från de *registrerade eller deras företrädare.*[44] Begreppet bör tolkas brett. Det kan handla om exempelvis

41 Jfr begreppet samtycke i artikel 6.1 a i dataskyddsförordningen med regeln om att hämta in synpunkter i artikel 35.9.
42 WP 248, s. 16 f.
43 Jfr WP 248, s. 16 f.
44 Artikel 35.9 i dataskyddsförordningen.

representanter för olika organisationer som försvarar de registrerades intressen, eller konsumenter rent generellt.[45] För behandlingar som omfattar elever på en skola kan det vara elevernas vårdnadshavare. För behandlingar som omfattar anställda kan skyddsombudet eller de arbetstagarorganisationer som finns representerade på arbetsplatsen tillfrågas. Företrädare kan även i vissa fall vara personal som arbetar nära de registrerade eller som av andra skäl har god insyn i deras intressen.

Om en föreslagen behandling endast medför risker för ett begränsat antal registrerade kan det vara tillräckligt att synpunkter hämtas in från representanter för just den berörda gruppen. För behandlingar som berör anställda kan det exempelvis vara lämpligt att tillfråga ett antal anställda eller deras fackliga ombud. Om den föreslagna behandlingen innebär risker för ett stort antal fysiska personer som ännu inte har identifierats (exempelvis alla invånare) kan det istället vara lämpligt att ta reda på hur potentiella registrerade generellt uppfattar en viss behandling.[46]

Hur de registrerades synpunkter bör hämtas in

På vilket sätt synpunkterna ska hämtas in beror bl.a. på vilka som ska tillfrågas, vilken typ av information som krävs för att de registrerade ska förstå innebörden av den planerade behandlingen och vad som är en proportionerlig arbetsinsats förhållande till riskerna med behandlingen. Insamlingen kan exempelvis ske i form av en enkät. Om en personuppgiftsansvarig redan har kontakter i form av exempelvis referensgrupper, användargrupper eller åsiktspaneler kan det vara lämpligt att använda dessa.

Frågorna bör vara tydligt avgränsade och formulerade på ett sätt som är lätt att förstå. För att undvika ”informationsutmattning” bör undersökningen utformas så kortfattat som möjligt.[47] De tillfrågade bör ges tillräckligt med tid att svara på frågorna. För att möjliggöra för de registrerade att faktiskt ta ställning till den avsedda behandlingen bör den personuppgiftsansvarige själv beskriva de riskfaktorer som verksamheten har identifierat.

Dokumentera synpunkterna

I regel räcker det att dokumentera de registrerades synpunkter genom att sammanställa resultatet av undersökningen. Om den personuppgiftsansvarige väljer att gå vidare med behandlingen trots att de registrerades synpunkter talar emot det bör en motivering för det dokumenteras. En personuppgiftsansvarig som beslutar att inte hämta in de registrerades synpunkter bör också dokumentera en motivering för det.[48]

7.3 Synpunkter från övriga intressenter

I vissa fall kan det finnas andra intressenter än de registrerade vars synpunkter bör hämtas in och dokumenteras i konsekvensbedömningen (exempelvis från informationssäkerhetsansvariga eller andra personer i organisationen med teknisk kompetens).

45 Jfr WP 248, s. 16 f.
46 Jfr WP 248, s. 16 f.
47 För vägledning kring öppenhet och information till de registrerade, se t.ex. Artikel 29-arbetsgruppens Riktlinjer om öppenhet enligt förordning (EU) 2016/679 (WP 260 rev. 01). EDPB har ställt sig bakom riktlinjerna, Endorsement 1/2018.
48 Jfr WP 248, s. 17.

Steg 8.
Gör en sammantagen bedömning

När ni kommer till det här steget har riskerna med den planerade personuppgifts-behandlingen hanterats och skyldigheten att begära förhandssamråd bedömts.

Det kan ha tillkommit information som är relevant och bör beaktas, och som medför att det är lämpligt att göra en sammantagen bedömning av om behandlingen kan genomföras. Den personuppgiftsansvarige ska i det här steget ta ställning till om de identifierade riskerna fortfarande kan anses vara hanterade i en utsträckning som är tillräcklig, och om den planerade behandlingen fortfarande kan anses nödvändig och proportionerlig i förhållande till ändamålet med den.

Steg 9.
Förankra bedömningen i organisationen

Behöriga personer i den personuppgiftsansvariga organisationens ledning ska få information om konsekvensbedömningen, de identifierade riskerna, riskvärderingen och de identifierade riskreducerande åtgärderna.

Varje organisation bör ha en fastställd process för hur förankringen ska gå till. Dataskyddsförordningen innehåller inga regler om hur konsekvensbedömningen rent konkret ska förankras inom den personuppgiftsansvariga organisationen. Förankringen kan exempelvis ske genom att ledningen får en sammanfattning med konsekvens-bedömningens slutresultat och nödvändiga motiveringar. Det bör tydliggöras vem eller vilken funktion i organisationen som ansvarar för att de riskreducerande åtgärderna genomförs. Även ansvaret för den eventuella kvarstående risken med behandlingen bör tydliggöras.

Steg 10.
Följ upp konsekvens-bedömningen kontinuerligt

En konsekvensbedömning är inte en engångshändelse utan en process. Det innebär att personuppgiftsansvariga vid behov behöver kontrollera om behandlingen genomförs i enlighet med konsekvensbedömningen och se över om risker förändras.[49]

Det är ofta lämpligt att bygga in översynen av konsekvensbedömningar i verksamhetens övriga processer och systematiska verksamhetsarbete, exempelvis i årshjul eller annan regelbunden översyn. Vilket tidsintervall som är lämpligt för att se över befintliga konsekvensbedömningar beror bl.a. på riskerna med behandlingen och den teknik som används. Den första uppföljningen bör alltid göras relativt nära inpå att behandlingen påbörjats; lämpligen efter ungefär ett år. Därefter bör konsekvensbedömningen som utgångspunkt ses över vartannat år. Översynen bör ske i tätare intervall om det är fråga om användning av ny teknik, omfattande behandling eller behandling som avser känsliga personuppgifter. För behandlingar som är väl beprövade eller väl inbyggda i verksamheten kan översynen dock ske mer sällan än vartannat år.

Kravet på regelbunden översyn gäller utöver den översyn som måste göras om riskbilden förändras. Om risken förändras måste den personuppgiftsansvarige bedöma om behandlingen fortfarande utförs i enlighet med den ursprungliga konsekvensbedömningen eller om denna behöver uppdateras. Riskbilden kan förändras på grund av faktorer som beror på den egna verksamheten (exempelvis organisatoriska förändringar), eller på grund av faktorer utanför den egna verksamheten (exempelvis ett förändrat rätts- eller omvärldsläge), eller en kombination av de båda.

Det är viktigt att den personuppgiftsansvarige säkerställer att eventuella förändringar av risker fångas upp inom organisationen, exempelvis med hjälp av rutiner och tydlig ansvarsfördelning.

Exempel på när risker kan förändras

- ny teknik börjar användas vid behandlingen (t.ex. en AI-modell)
- fler uppgifter än beräknat samlas in (t.ex. om ett system som tidigare bara har behandlat information om namn och adress föreslås behandla uppgifter av mer känslig karaktär)
- det sker viktiga förändringar på samhällsnivå (t.ex. så att vissa automatiska beslut får större praktisk påverkan på enskilda än tidigare, eller att nya kategorier av registrerade blir sårbara för diskriminering)
- den personuppgiftsansvarige upptäcker en säkerhetsbrist som visar att risken var högre än vad man tidigare hade trott (t.ex. genom en personuppgiftsincident).

49 Jfr artikel 35.11 i dataskyddsförordningen.

Källor

Vägledningen är, förutom dataskyddsförordningen, huvudsakligen baserad på

- Domar från EU-domstolen (framgår av fotnoter).
- IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen daterad den 16 januari 2019 med tillhörande beslut (dnr DI-2018-13200) (IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen).
- Riktlinjer från Europeiska dataskyddsstyrelsen (EDPB) och dess föregångare Artikel 29-arbetsgruppen:
  - *Statement on the role of a risk-based approach in data protection legal frameworks* (WP 218), adopted on 30 May 2014.
  - *Riktlinjer om dataskyddsombud* (WP 243 rev. 01), senast granskade och antagna den 5 april 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), antagna den 4 april 2017 och reviderade den 4 oktober 2017.
  - *Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679* (WP 251 rev 01), senast granskade och antagna den 6 februari 2018.
  - *Riktlinjer om öppenhet enligt förordning (EU) 2016/679* (WP 260 rev. 01), senast granskade och antagna den 11 april 2018.
  - *Riktlinjer 3/2019 för behandling av personuppgifter genom videoenheter,* version 2.0, antagna den 29 januari 2020.
  - *Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR,* version 2.1, antagna den 7 juli 2021.
- IMY:s tillsynsbeslut som rör artikel 35 i dataskyddsförordningen.
- Andra europeiska dataskyddsmyndigheters information på deras webbplatser om konsekvensbedömningar.
- Doktrin (framgår av fotnoter).

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