DATAOMBUDSMANNENS BYRÅ

Dataombudsmannens byrå

Anvisning om konsekvens-bedömning avseende data-skydd

Ändringshistorik

Tid	Ändring
12/2021	Anvisningen publicerades efter en kommentarsomgång.

Innehåll

Inledning

Vad är en konsekvensbedömning avseende dataskydd?

Syftet med en konsekvensbedömning avseende dataskydd är att identifiera och minimera risker förknippade med behandlingen av personuppgifter samt att ta fram material för att kunna bevisa efterlevnaden av dataskyddsregleringen. Konsekvensbedömningen kan användas som ett ständigt hjälpmedel för att tillgodose inbyggt dataskydd och dataskydd som standard samt för riskhantering när behandlingen av personuppgifter leder till en hög risk för den registrerade. Denna anvisning har tagits fram för att stödja utarbetandet av en konsekvensbedömning avseende dataskydd (nedan KBD) som avses i artikel 35 i den allmänna dataskyddsförordningen (nedan DSF) och i 20 § i dataskyddslagen avseende brottmål (nedan DSlB). Se även bilaga II gällande det sistnämnda.

Enligt artikel 35 i DSF ska en konsekvensbedömning göras när man planerar en behandling av personuppgifter som sannolikt leder till en hög risk för den registrerades rättigheter och friheter. Se på dataombudsmannens byrås webbplats när en konsekvensbedömning ska göras[1].

Det finns inga närmare bestämmelser i DSF om hur en konsekvensbedömning ska göras. I artikel 35 i DSF anges minimiinnehållet i KBD som preciseras ytterligare i anvisningen om konsekvensbedömning[2].

Alla organisationer ska säkerställa att regleringen om behandling av personuppgifter följs i deras verksamhet, oavsett om behandlingen leder till en hög risk eller inte. Här skiljer sig KBD från säkerställande av lagenlighet. Den förutsätter att risker och skyddsåtgärder som hör samman med dem identifieras, specificeras och beskrivs noggrannare på förhand.

Kärnfrågor i konsekvensbedömningen avseende dataskydd

Varför och hur avser vi behandla personuppgifter?

Vilka personuppgifter har vi för avsikt att behandla?

Hur påverkar den behandling av personuppgifter som vi planerat de registrerade, när behandlingen går enligt plan?

Vad kan gå fel i den planerade behandlingen av personuppgifter?

Hur sannolikt kommer något att gå fel?

Hur kan vi minska denna sannolikhet?

KBD ska uppdateras när verksamhetsmiljön, lagstiftningen och riskerna förändras, till exempel när vissa funktioner som påverkar behandlingen av personuppgifter eller som anknyter till behandlingen tas i bruk. Det rekommenderas också att bedöma behovet av att uppdatera konsekvensbedömningen regelbundet, till exempel med två års mellanrum.

Kraven på konsekvensbedömning tillämpas också på behandlingsåtgärder som påbörjats före 25.5.2018 och som fortfarande pågår. Den personuppgiftsansvarige ska alltså göra en konsekvensbedömning av pågående behandling då en sådan plikt skulle förekomma också i övrigt enligt dataskyddslagstiftningen. Konsekvensbedömningen kan gälla en enskild behandlingsåtgärd eller en serie liknande åtgärder.

[1] https://tietosuoja.fi/sv/konsekvensbedomning
[2] Anvisning av Arbetsgruppen för skydd av personuppgifter (WP 29) WP 248 rev.01, bilaga II.

Varför görs en konsekvensbedömning avseende dataskydd?

Att göra upp en konsekvensbedömning avseende dataskydd kan ha flera fördelar för en organisation. Med hjälp av konsekvensbedömningen är det möjligt att upptäcka hot relaterade till behandlingen av personuppgifter och identifiera vilka åtgärder som behöver vidtas för att undvika hoten innan betydande ekonomiska satsningar görs. Att ändra den planerade behandlingen i planeringsfasen kostar i allmänhet en bråkdel jämfört med kostnaderna orsakas senare. Om dataskyddskonsekvenserna inte är acceptabla, är det till och med möjligt att man måste stryka planen.

En konsekvensbedömning avseende dataskydd kan också medföra fördelar när det gäller anseende. Den personuppgiftsansvarige kan samråda med de registrerade om deras åsikter om den planerade behandlingen innan behandlingen börjas, eller så kan konsekvensbedömningen avseende dataskydd läggas fram för de registrerade för att öka transparensen och förbättra användarupplevelsen. Om ett hot som är förknippat med behandlingen realiseras, kan dokumentationen gällande konsekvensbedömningen avseende dataskydd hjälpa till att påvisa att den personuppgiftsansvarige på behörigt sätt försökte förhindra händelsen. På detta sätt kan risken för skadeansvar, negativ publicitet och förlorat anseende minimeras.

Att låta bli att göra en konsekvensbedömning avseende dataskydd i en situation där den bör göras kan leda till administrativa påföljder, inklusive påföljdsavgift eller förbud mot behandling. Därför uppmanas personuppgiftsansvariga att dokumentera varför man i vissa situationer beslutat att låta bli att göra en KBD. Detta är särskilt viktigt i situationer inom den s.k. gråzonen. Genom att göra en konsekvensbedömning i sådana situationer kan personuppgiftsansvariga kommunicera till sina intressentgrupper att de förhåller sig allvarliga till dataskyddsrelaterade frågor.

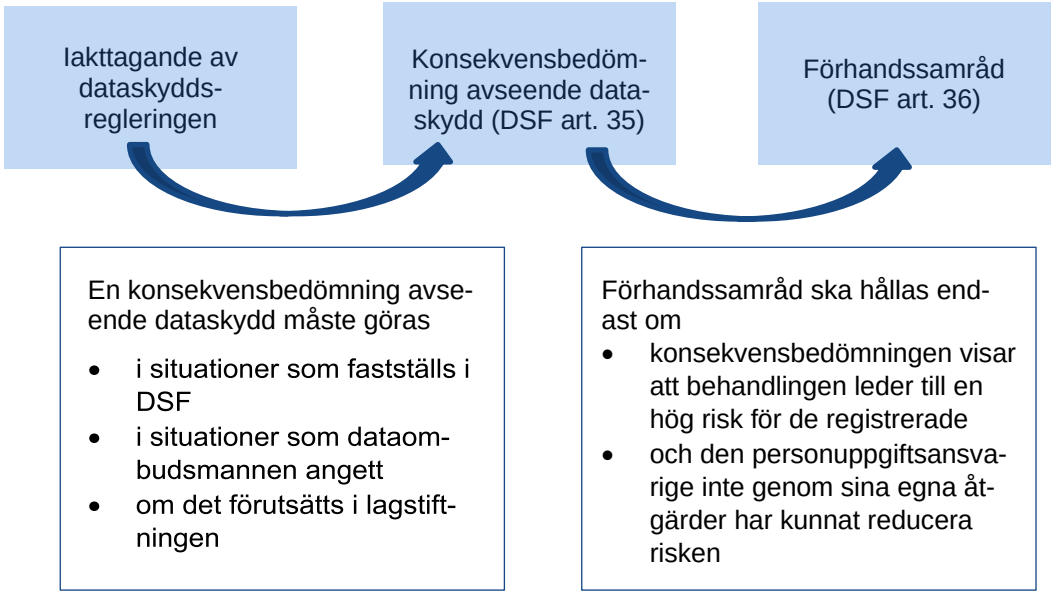


Bild 1. Konsekvensbedömningens placering i helheten för skyldigheter som gäller behandling av personuppgifter. När behandlingen är förknippad med en hög risk för den registrerade, ska man utöver att iaktta dataskyddsregleringen också göra en konsekvensbedömning avseende dataskydd. Det är alltså inte nödvändigt att göra en konsekvensbedömning i alla situationer. Om den kvarstående risken efter de att korrigerande åtgärder som bestäms i konsekvensbedömningen genomförts fortfarande är hög, ska förhandssamråd med dataombudsmannen begäras.

Hur görs en konsekvensbedömning avseende dataskydd?

Den personuppgiftsansvarige ansvarar för att göra KBD. Den personuppgiftsansvarige ska specificera konsekvensbedömningens objekt. Dessutom rekommenderas det att specificera personerna som deltar i uppgörandet (som den personuppgiftsansvariges representanter, personuppgiftsbiträdets representanter, dataskyddsombudet, it-sakkunniga, informationssäkerhetssakkunniga, personer förtrogna med den praktiska behandlingen och eventuella utomstående sakkunniga). Den personuppgiftsansvarige ska också bestämma processen för att godkänna identifierade risker, eventuella åtgärdsförslag för att reducera dessa samt eventuell kvarstående risk.

Personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige att göra KBD och ge den personuppgiftsansvarige de uppgifter som behövs för att göra konsekvensbedömningen.

Den personuppgiftsansvarige ska vid uppgörandet av konsekvensbedömningen be om råd av dataskyddsombudet, om ett sådant utsetts.

Det rekommenderas att samråda med personerna som är föremål för behandlingen eller deras representanter om de planerade behandlingsåtgärderna. Vid samrådet ska intressen som hänför sig till kommersiella eller allmänna intressen eller behandlingens säkerhet beaktas. Genom att samråda med de registrerade eller deras representanter är det möjligt att få mer information om huruvida den planerade behandlingen av personuppgifter är godtagbar och om eventuella missförstånd.

En enskild konsekvensbedömning avseende dataskydd kan användas för att bedöma andra behandlingsåtgärder av liknande art, omfattning, sammanhang, ändamål och risker. En konsekvensbedömning behöver alltså inte göras om sådana planerade behandlingsåtgärder vars konsekvenser redan har bedömts. Detta kan vara fallet till exempel när liknande teknik har använts för att insamla uppgifter av samma typ för samma ändamål.[3]

Ta hänsyn till följande när du förbereder en konsekvensbedömning:

1) Definiera konsekvensbedömningens objekt. Är det fråga om en produkt/ett program/en process? En IT-baserad produkt eller en IT-baserad tjänst?
2) Definiera roller och ansvar. Identifiera vilka som deltar i behandlingen och deras roller och ansvar: personuppgiftsansvarig(a) och personuppgiftsbiträde(n) samt mottagare av personuppgifter
3) Ta reda på regleringen rörande skydd av personuppgifter som tillämpas på konsekvensbedömningens objekt (vid sidan av EU:s allmänna dataskyddsförordning bl.a. branschspecifik reglering).
4) Välj deltagarna och definiera deras roller (juridisk och teknisk kompetens, personer som känner till behandling av personuppgifter i praktiken, dataskyddsombud). Fundera ut det bästa sättet för att göra bedömningen (t.ex. workshop-arbete, syner) och se till att bedömningen har tillräckliga resurser. Personuppgiftsbiträdet (t.ex. systemleverantören) bör hjälpa den personuppgiftsansvarige att göra en konsekvensbedömning avseende dataskydd. Det rekommenderas också att ge de personer som är föremål för behandlingen av personuppgifter eller deras representanter tillfälle att bli hörda.

[3] WP 248 rev.01, s. 8.

5) Konsultera det eventuella dataskyddsombudet när du gör en konsekvensbedömning avseende dataskydd. Ansvaret för att göra konsekvensbedömningen (inkl. valda skyddsåtgärder) samt ansvaret för att börja ett eventuellt samrådsförfarande ligger dock hos den personuppgiftsansvarige.

6) Kartlägg och utnyttja redan befintligt material om dataskydd/informationssäkerhet (t.ex. personuppgiftsinventeringar, dataflödesscheman, register över behandlingar enligt artikel 30 osv.)

   Se till att det finns en process för att godkänna konsekvensbedömningen avseende dataskydd och att eventuella nödvändiga åtgärder som framkommer i och med konsekvensbedömningen schemaläggs och delegeras till vissa personer. Försäkra dig också om att utförandet av åtgärderna följs upp konkret och att konsekvensbedömningen uppdateras vid behov, åtminstone om riskerna förknippade med behandlingen av personuppgifter förändras.

Anvisningens struktur

I denna anvisning är KBD indelad i fyra steg. Först beskrivs konsekvensbedömningens objekt (kapitel 1). Därefter bedöms det om den planerade behandlingen av personuppgifter stämmer överens med regleringen avseende behandling av personuppgifter (kapitel 2). I samband med detta granskas behovet av och proportionaliteten hos behandlingen av personuppgifter och hur dataskyddsprinciperna följs och dataskyddsrättigheterna tillgodoses. Dessutom säkerställs iakttagande av övrig lagstiftning som gäller den planerade behandlingen av personuppgifter.

Därefter bedöms de risker som orsakas den registrerade av behandlingen av personuppgifter. Detta görs genom att identifiera hoten, hur allvarliga de är samt hur sannolikt det är att de realiseras (kapitel 3).

Avslutningsvis beskrivs vilka åtgärder som förutsätts för att slutföra KBD (kapitel 4).

På de sista sidorna i anvisningen definieras de viktigaste begreppen och förkortningarna som används i anvisningen.

Dataombudsmannens byrå har som en bilaga till anvisningen tagit fram ett registreringsverktyg i Excel, som kan användas för att göra en konsekvensbedömning (bilaga I). Verktyget är enkelt, grundläggande och frivilligt att använda. Organisationerna uppmuntras att ändra verktyget så att det bättre motsvarar deras behov.

Denna anvisning kan i tillämpliga delar också användas för att göra en i 20 § i dataskyddslagen avseende brottmål avsedd konsekvensbedömning. Mer information om detta finns i bilaga II.

1 Beskrivning av behandlingen av personuppgifter (uppfatta kontexten)

I det första steget av konsekvensbedömningen specificeras och avgränsas bedömningsobjektet. Samtidigt skapas en översikt av behandlingen av personuppgifter. Utgångspunkten kan vara en plan eller beskrivning av vad som eftersträvas med behandlingen av personuppgifter, då genomförandet av behandlingen och detaljerna i skyddsåtgärderna kompletteras när konsekvensbedömningen framskrider. I detta fall kan man bli tvungen att upprepa stegen i konsekvensbedömningen så att en tillräckligt detaljerad nivå nås. Av beskrivningen bör behandlingens art, omfattning, sammanhang och ändamål framgå.

Ett flödesschema hjälper till att uppfatta hur uppgifterna rör sig. Det rekommenderas att bifoga ett eventuellt schema till konsekvensbedömningen avseende dataskydd. Schemat kan också utnyttjas senare i avsnittet som gäller identifiering av hot (se kapitel 3.2).

När du gör upp en beskrivning av behandlingen av personuppgifter, ska du definiera följande saker:

- **Syftet med och målet för behandlingen av personuppgifter**: I vilket sammanhang behandlas personuppgifterna? Vilka av de registrerades rättigheter och friheter gäller behandlingen? Vad vill man åstadkomma med behandlingen och varför behövs personuppgifterna för att uppnå dessa ändamål?
- **Personer vars uppgifter behandlingen gäller (de registrerade)**: Vilka personers uppgifter behandlas? Vilken är den personuppgiftsansvariges relation/samband med de registrerade? Behandlas uppgifter om personer som är i en svagare ställning än den personuppgiftsansvarige (t.ex. seniorer, barn, anställda, patienter)? Kan uppgifter om minderåriga bli föremål för behandlingen? Observera olika grupper av registrerade (t.ex. anställda och kunder). Hur många registrerade finns det? Vilket geografiskt område omfattar behandlingen i sin helhet?
- **Roller och ansvar**: Specificera den personuppgiftsansvarige/de personuppgiftsansvariga, dvs. de aktörer som har befogenheter och ansvar att bestämma om ändamålen och metoderna för behandlingen av personuppgifter. Diskutera om gemensamt personuppgiftsansvariga kommer på fråga (se artikel 26). Specificera också personuppgiftsbiträdet/personuppgiftbiträdena för behandlingen.
- **Personuppgifter**: Vilka personuppgifter behandlas? Behandlas särskilda kategorier av personuppgifter, uppgifter om brottmålsdomar och förseelser eller personbeteckningar? Observera även tekniska data som räknas som personuppgifter (bedöm t.ex. loggdata, nätidentifierare).
- **Mängden personuppgifter som behandlas**: Hur stora mängder personuppgifter behandlas? Observera olika kategorier av personuppgifter.
- **Geografisk omfattning för de uppgifter som behandlas**: I vilka länder behandlas uppgifterna? Behandlas uppgifterna i andra EU- eller EES-länder? Behandlas uppgifter utanför dessa länder?
- **Personuppgifternas livscykel**: Varifrån insamlas eller inhämtas uppgifterna (uppgiftskällor)? Hur länge förvaras uppgifterna (lagringstider för personuppgifter och grunderna för hur de bestäms)? Till vem lämnas uppgifter ut (mottagare av uppgifter)?
- **Tekniskt utförande**: Vilka informationstekniska resurser och funktioner förutsätter den planerade behandlingen? Har alternativa utföranden bedömts ur ett dataskydds- och informationssäkerhetsperspektiv? Observera även gränssnitt, servrar, maskinsalar, användargrupper samt användarbehörigheter m.m. när det gäller livscykeln.

2 Bedömning av efterlevnad av dataskyddsregleringen

Innan de risker som förknippas med behandlingen av personuppgifter bedöms gäller det att säkerställa att lagstiftningen om behandling av personuppgifter iakttas. I detta skede beskrivs på vilket sätt de krav som hänför sig till DSF samt annan lagstiftning som tillämpas på behandlingen av personuppgifter uppfylls. Märk väl att denna anvisning inte omfattar förpliktelser som ställs i branschspecifik reglering.

En bedömning av efterlevnad av dataskyddsprinciper och den registrerades rättigheter enligt detta avsnitt bör göras alltid när personuppgifter behandlas, oavsett om behandlingen också omfattar en skyldighet att göra en konsekvensbedömning.

2.1 Iakttagande av dataskyddsprinciper

2.1.1 Allmän bedömning om att den planerade behandlingen är nödvändig och proportionell

Konsekvensbedömningen avseende dataskydd ska innehålla en bedömning av att den planerade behandlingen av personuppgifter är nödvändig och proportionell för att nå de lagliga ändamålen med behandlingen, m.a.o. att behandlingen effektivt svarar mot detta behov och minst kränker den registrerades integritet och skyddet av personuppgifter. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel.

Bedöm om hur nödvändig och proportionell den planerade behandlingen är. Diskutera åtminstone följande frågor:

- Varför är behandlingsåtgärderna ett effektivt medel för din organisation till exempel för att utföra en uppgift som anvisats den, uppfylla ett avtal eller utföra en tjänst som den tillhandahåller?
- Finns det andra medel som kränker skyddet av personuppgifter i mindre utsträckning för att uppnå samma mål?
- Varför kan omfattningen på eller medlen för behandlingen anses vara proportionella för att utföra den aktuella uppgiften/uppnå syftet? Jämför fördelarna med behandlingen med de potentiella risker som den medför för de registrerade. Det är möjligt att riskerna som förknippas med en behandling av personuppgifter som i princip verkar nödvändig är så höga att behandlingen inte kan anses vara proportionell.

När konsekvensbedömningen uppdateras är det bra att kontrollera om man med den genomförda behandlingen av personuppgifter har nått målen som ställts upp för behandlingen så att behandlingsåtgärderna fortfarande kan anses vara nödvändiga och korrekta.

Om den planerade behandlingen inte är nödvändig och korrekt, kan behandlingen inte utföras som sådan. I detta fall behöver inte heller konsekvensbedömningen fortsättas, om planen inte ändras.

2.1.2 Efterlevnad av dataskyddsprinciper

För att kunna bedöma efterlevnaden av dataskyddsprinciper på ett heltäckande sätt, gäller det att ta reda vilken dataskyddslagstiftning som tillämpas på behandlingen som konsekvensbedömningen avseende dataskydd gäller. Branschspecifik lagstiftning ska beaktas genomgripande. Dataskyddsprinciperna kan ha beaktats redan vid beredning av lagstiftningen om behandling av personuppgifter. Till exempel kan grunderna för behandlingen, personuppgifterna som behandlas samt uppgifternas ändamål och utlämning av uppgifter föreskrivas i lag.

Tillämplig reglering: Fastställ vilken reglering som lämpar sig för konsekvensbedömningens objekt: DSF, dataskyddslagen och eventuell annan lagstiftning om behandling av personuppgifter. Beakta också eventuella uppförandekoder enligt artikel 40 i DSF och certifieringar enligt artikel 42, om sådana blir tillämpliga i fallet.

Dataskyddsprinciperna[4] framgår av artikel 5 i dataskyddsförordningen. Det finns sex principer och enligt dessa ska personuppgifter:

- behandlas på ett **lagligt, korrekt och öppet sätt** i förhållande till den registrerade[5]
- samlas in och behandlas **för särskilda, uttryckligt angivna och berättigade ändamål**[6]
- samlas in endast **i den mängd som behövs** med tanke på ändamålet med behandlingen[7]
- uppdateras alltid när det är nödvändigt: felaktiga personuppgifter ska **raderas eller rättas utan dröjsmål**[8]
- **förvaras** i en form som möjliggör identifiering av den registrerade **endast så länge som är nödvändigt** för de ändamål för vilka personuppgifterna behandlas[9]
- Behandlas **konfidentiellt** och **säkert**[10]

2.1.3 Laglighet (grund för behandling) och korrekthet

För att personuppgifter ska kunna behandlas ska det finnas en laglig grund för behandlingen. Bestämmelser om grunderna för behandling finns i artikel 6 i DSF och i 4 § i dataskyddslagen som kompletterar den, samt i fråga om uppgifter som hör till särskilda kategorier av personuppgifter i artikel 9 i DSF och 6 § i dataskyddslagen. Dessutom föreskrivs om behandling av uppgifter som gäller brottmålsdomar och överträdelser i artikel 10 i DSF, och om behandlingen av personbeteckning i 29 § i dataskyddslagen. På motsvarande sätt ska behandlingen i en konsekvensbedömning som görs på basis av dataskyddsbestämmelserna för brottmål grunda sig på DSIB och/eller en mer detaljerad speciallag som gäller myndigheter (t.ex. lag om behandling av personuppgifter i polisens verksamhet 616/2019).

Mer information om grunderna för behandling[11]

[4] tietosuoja.fi/sv/dataskyddsprinciper
[5] tietosuoja.fi/sv/lagenlighet-korrekthet-och-transparens
[6] tietosuoja.fi/sv/bundenhet-till-anvandningsandamalet
[7] tietosuoja.fi/sv/uppgiftsminimering
[8] tietosuoja.fi/sv/uppgifternas-korrekthet
[9] tietosuoja.fi/sv/lagringsminimering
[10] tietosuoja.fi/sv/konfidentialitet-och-sakerhet
[11] tietosuoja.fi/sv/nar-far-personuppgifter-behandlas

Om det i den branschspecifika lagstiftningen föreskrivs om behandling av personuppgifter, ska denna reglering följas.

Om parterna i behandlingen har identifierats som gemensamt personuppgiftsansvariga, ska det säkerställas att ansvarsfördelningen mellan dem har fastställts och att de centrala delarna av arrangemanget finns tillgängliga för den registrerade i enlighet med artikel 26 i DSF.

När du bedömer om det finns en grund för behandling samt om behandlingen är laglig och korrekt kan du använda dig av följande exempelfrågor:

- Vilken är grunden eller grunderna för behandling av personuppgifter?
- Om det är frågan om berättigat intresse, har eventuella prövnings- och dokumentationsskyldigheter som anknyter till grunden för behandling beaktats (t.ex. balanstest för berättigat intresse)?
- Om behandlingen grundar sig på samtycke, är samtycket en frivillig, specifik, informerad och otvetydig viljeyttring?
- Har det gjorts lika lätt att återkalla samtycket som att ge det?
- Om det är frågan om särskilda kategorier av personuppgifter (artikel 9), vilken är den tillämpliga undantagsgrunden för att behandla dem? (artikel 9.2, 6 § i dataskyddslagen)
- Om uppgifter som gäller fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, uppfylls förutsättningarna för att behandla dem (artikel 10, 7 § i dataskyddslagen)?
- Om personbeteckningar behandlas, uppfylls förutsättningarna för att behandla dem (29 § i dataskyddslagen)?
- Tillämpas sådan speciallagstiftning där det föreskrivs om behandling av personuppgifter på verksamheten? Om ja, hur säkerställs efterlevnaden av denna lagstiftning?
- På vilket sätt svarar behandlingen mot de registrerades motiverade förväntningar?

2.1.2 Öppenhet (information till de registrerade)

Den personuppgiftsansvarige ska berätta för de registrerade om behandlingen av personuppgifter tydligt och begripligt. Det finns vissa undantag från denna allmänna information (se artikel 13.4 i DSF och 33 § i dataskyddslagen).

Den närmare kraven på information beror delvis på om uppgifterna insamlas hos personen själv eller någon annanstans. De närmare informationskraven är:

- informatiosinnehåll[12]
- krav på presentationssätt[13]
- krav på distribution och sändningssätt[14]
- krav gällande tidpunkt[15]

[12] https://tietosuoja.fi/documents/6927448/8214536/Informointivelvoitteen+edellytt%C3%A4m%C3%A4t+tiedot/419957bd-fd5a-4090-9c64-cf4769b10570/Informointivelvoitteen+edellytt%C3%A4m%C3%A4t+tiedot.pdf (på finska)
[13] https://tietosuoja.fi/sv/beratta-om-behandlingen-for-den-registrerade
[14] https://tietosuoja.fi/sv/ratten-att-fa-information-om-behandlingen-av-personuppgifter
[15] https://tietosuoja.fi/sv/ratten-att-fa-information-om-behandlingen-av-personuppgifter

När du bedömer hur dessa krav uppfylls kan du använda dig av följande exempelfrågor:

- Hur och i vilket sammanhang informeras om behandlingen av personuppgifter? I vilket skede av kundresan berättar ni om behandlingen?
- Får den registrerade omfattande information om behandlingen för att kunna försäkra sig om ett effektivt skydd av sina personuppgifter?
- Var finns uppgifterna? Finns de lättillgängliga för den registrerade?
- Är den information som tillhandahållits begriplig ur målpublikens perspektiv (t.ex. barn)?
- Framförs informationen på ett begripligt sätt? Har olika lager eller något annat sätt för att underlätta läsbarheten utnyttjats i det sätt som uppgifterna presenteras på?
- Hur ser man till att informationen är uppdaterad?
- Om de registrerade inte informeras eller om informationen skjuts upp, hur motiveras detta?

2.1.3 Ändamålsbegränsning

Specificering av ändamål på förhand

Ändamålet eller ändamålen med behandlingen av personuppgifter ska planeras och definieras tydligt innan behandlingen påbörjas. Personuppgifter får samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål. Detta kräver att ändamålet specificeras och motiveras. Personuppgifter som samlats in ett särskilt ändamål får inte behandlas för ändamål som är oförenligt med det ursprungliga ändamålet.

Ändamålet påverkar de övriga principerna som gäller de uppgifter som behandlas. Dessa principer är till exempel uppgiftsminimering, begränsning av lagringstid, korrekthet samt förenlighet vid ytterligare behandling. Därför ska ändamålen med behandlingen av personuppgifter specificeras på förhand. Ändamålen ska vara specifika, uttryckliga och berättigade.

Den personuppgiftsansvarige beskriver målen med behandlingen med tanke på sin egen verksamhet. En mycket allmän beskrivning av ändamålet är inte tillräcklig, utan ändamålet med behandlingen ska definieras tillräckligt exakt för att kravet på specificering och uttrycklighet ska uppfyllas. Den registrerade ska utifrån definitionen kunna skapa sig en tillräckligt exakt uppfattning om vad personuppgifterna avses användas för.

Förenlighet vid ytterligare behandling

Ändamålet binder ytterligare behandling så att den bör vara förenlig med den ursprungliga behandlingen. Bestämmelser om bedömning av huruvida den ytterligare behandlingen är förenlig finns i artikel 6.4 i DSF. Behandlingen av personuppgifter för arkiveringsändamål som gäller statistikföring, vetenskaplig forskning och allmänt intresse är förenlig om adekvata skyddsåtgärder följs. Dessutom kan den registrerades samtycke eller speciallagstiftning berättiga behandling för något annat ändamål.

Mer information om ändamålsbegränsning på dataombudsmannens byrås webbplats[16].

När du bedömer hur denna princip följs kan du använda dig av följande exempelfrågor:

[16] https://tietosuoja.fi/sv/bundenhet-till-anvandningsandamalet

- Vilka är ändamålen med behandlingen av personuppgifter? Beskriv målen för den planerade behandlingen med tanke på den personuppgiftsansvariges verksamhet.
- Vad eftersträvar man med behandlingen?
- Är ändamålen berättigade och tydligt specificerade?
- Hur har ändamålen dokumenterats?
- Hur försäkrar man sig om att behandlingen förblir förenlig med ändamålet eller ändamålen?
- Har behandlingen av uppgifterna för andra ändamål begränsats med tekniska och/eller organisatoriska metoder (t.ex. sekretess, decentralisering, anvisningar, avtalsförpliktelser)? Beskriv hur.
- På vilka grunder kan ytterligare behandling anses vara förenlig med det ursprungliga ändamålet?
- Är syftet med behandlingen för den registrerade tillräckligt förutsägbar med tanke på den registrerades berättigade förväntningar samt informationen som ges om behandlingen?

2.1.4 Uppgiftsminimering och lagringsminimering

Med uppgiftsminimering avses minimering av de uppgifter om den registrerade som samlas in och behandlas[17]. Personuppgifter får behandlas enbart då det är nödvändigt med tanke på behandlingens ändamål. För att bedöma vilka uppgifter som anses vara korrekta och relevanta ska man tydligt identifiera orsaken till att de aktuella personuppgifterna behövs. Om ändamålet, till exempel utförandet av en tjänst, kan uppnås så att vissa uppgifter inte behandlas, är behandlingen av personuppgifter inte nödvändig till dessa delar och personuppgifter ska i detta fall inte behandlas. Personuppgifter får inte samlas in eller behandlas i större utsträckning än vad som behövs med tanke på ändamålet. Det ska också motiveras varför de uppgifter som samlas in och behandlas är nödvändiga.

Mer information om uppgiftsminimering[18].

När du bedömer hur dessa krav uppfylls kan du använda dig av följande exempelfrågor:

Minimeringskrav i behandlingen av personuppgifter:

- För vika syften insamlas uppgifterna?
- Kan syftet med behandlingen uppnås utan dessa uppgifter?
- Beskriver den insamlade uppgiften den egenskap som är avsedd att bedömas?
- Hur har man sett till att uppgifter inte samlas in ”för säkerhets skull”?
- Har det motiverats varför de uppgifter som samlas in och behandlas är nödvändiga?
- Är det möjligt att använda pseudonymisering? Om ja, lagras de tilläggsuppgifter som möjliggör förening separat?

Minimeringskravet i planeringen av informationssystem:

- Används fritextfält i formulär? Är det nödvändigt att använda dem? Har det getts instruktioner om ifyllande av fritextfält så att inga onödiga uppgifter ifylls?
- Har frivilliga och obligatoriska uppgiftsfält markerats tillräckligt väl? Är de frivilliga uppgiftsfälten nödvändiga för att nå ändamålet med behandlingen?
- Hur har det säkerställts att behandlingen av personuppgifter inte ger upphov till/lämnar onödiga kopior?

[17] Artikel 5:1(c) i EU:s allmänna dataskyddsförordning. Mer information: Guidelines 4/2019 on article 25 Data Protection by Design and by Default, s. 19-20.
[18] https://tietosuoja.fi/sv/uppgiftsminimering

- Hur har det säkerställts att systemet inte samlar in onödiga uppgifter? Uppstår det tillfälliga filer – om ja, har åtkomsten till dem begränsats och ser man till att de raderas?
- Hur har det säkerställts att åtkomst- och användarbehörigheterna till personuppgifterna kan begränsas?
- Hur hanteras användarbehörigheter när personerna byts?
- Har åtkomst- och användarbehörigheterna till personuppgifter minimerats?

Personuppgifter får lagras endast så länge som de behövs för ändamålet med personuppgifterna. Lagringsminimering hänger samman med principen om uppgiftsminimering: behandlingen av personuppgifter bör minimeras också tidsmässigt. I DSF definieras inga exakta lagringstider för personuppgifter. Även annan tillämplig lagstiftning kan påverka lagringstiden för personuppgifter. Olika tider för väckande av talan kan följa av lagstiftningen. Dessa tider ska beaktas när lagringstiderna fastställs. Det är också möjligt att det i lagstiftningen ställs minimi- eller maximilagringstider för vissa uppgifter samt ett krav på att uppgifterna ska raderas inom en viss tid.

Den personuppgiftsansvarig ska bedöma personuppgifternas nödvändighet i förhållande till det ifrågavarande ändamålet. Om det inte är möjligt att fastställa en exakt sluttid, bör behandlingens längd uttryckas på något annat sätt som kan följas upp senare. Det finns skäl att dokumentera personuppgifternas lagringstider för att kunna påvisa att principen om lagringsminimering iakttas.

När personuppgifterna inte längre behövs, ska de raders eller permanent omvandlas till en sådan form att en enskild person inte längre kan identifieras i dem.

Läs mer om lagringsminimering[19] och förstöring av material[20].

När du bedömer hur dessa krav uppfylls kan du använda dig av följande exempelfrågor:

- För vilka syften behandlas uppgifterna och hur länge behöver de behandlas för dessa syften?
- Har uppgifternas lagringstider begränsats till ett minimum?
- Granskas nödvändigheten regelbundet och raderas eventuella uppgifter som inte behövs?
- Tillämpas sådan lagstiftning som kräver eller styr till att lagra uppgifterna under en viss tid på de uppgifter som behandlas?
- Från och med vilken tidpunkt börjar uppgifternas lagringstid och när slutar den?
- Omfattas olika uppgifter eller kategorier av uppgifter av olika lagringstider?
- Kan olika delars lagringsperioder skiljas från varandra?
- Hur raderas uppgifterna?
- Hur genomförs raderingen av personuppgifter i praktiken: vem raderar dem, hur och när?
- Är det möjligt att börja använda automatisk förstöring av uppgifter när lagringstiden går ut, eller raderas uppgifterna manuellt?
- Hur raderas uppgifterna i fråga om säkerhetskopior och loggdata?
- Hur följs det upp att lagringstiderna och raderingsprocesserna följs?
- Kan personuppgifterna anonymiseras (ens i slutet av behandlingen)?
- Om personuppgifterna anonymiseras i stället för att raderas, hur säkerställs det att anonymiseringen görs på det sätt som DSF förutsätter?
- Hur ser man till att personerna inte kan identifieras på nytt i uppgifterna?

[19] https://tietosuoja.fi/sv/lagringsminimering
[20] https://tietosuoja.fi/sv/bortskaffning-anonymisering-eller-arkivering-av-material-vid-avslutning-av-studien

2.1.5 Uppgifternas korrekthet

Personuppgifterna som behandlas ska vara korrekta med tanke på ändamålet. Uppgifterna ska uppdateras vid behov. Inexakta och felaktiga personuppgifter ska rättas eller raderas utan dröjsmål.

Läs mer om korrekta uppgifter[21].

När du bedömer hur kraven som gäller korrekta uppgifter uppfylls kan du använda dig av följande exempelfrågor:

- Är uppgifterna statiska till sin art eller kräver de uppdateringar?
- Hur säkerställs det att de personuppgifter som behandlas är korrekta, uppdaterade och riktiga?
- Hur säkerställs det att inexakta och felaktiga uppgifter raderas eller rättas utan dröjsmål?
- Hur uppdateras uppgifterna? Hur övervakas det att uppgifterna är uppdaterade?
- Hur ofta bedömer man uppgifternas riktighet? Till exempel regelbundet, vid behov osv.
- Hur kan den registrerade påverka uppgifternas korrekthet och vid behov uppdatera uppgifterna?
- Hur säkerställs det att uppgifter som mottagits från en tredje part är korrekta?
- Hur säkerställs det att de insamlade uppgifterna gäller rätt person?

2.1.6 Säkerhet i samband med behandling av personuppgifter (konfidentialitet, integritet och tillgänglighet)

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

Med konfidentialitet avses att personuppgifterna endast ska vara tillgängliga för sådana personer som på grund av sina arbetsuppgifter har behov av och rätt till att få tillgång till uppgifterna. Personuppgifterna ska skyddas så att de inte kan läsas eller i övrigt behandlas obehörigt. Kränkningar av personuppgifternas konfidentialitet kan orsaka olika olägenheter och skador för individen, som psykiskt lidande, om uppgifter om hälsotillstånd blir tillgängliga för utomstående, eller ekonomisk skada, om de läckta personuppgifterna används obehörigt för att begå identitetsstöld. För att undvika detta ska behandlingen av personuppgifter planera så att uppgifterna är skyddade mot obehörig åtkomst och användning under såväl behandling som överföring och förvaring av uppgifterna.

Integritet betyder att uppgifterna förblir oförändrade när de behandlas, överförs och lagras. Personuppgifterna ska alltså skyddas mot att de obehörigen går förlorade, förstörs eller redigeras avsiktligt eller av misstag. Brister i personuppgifternas integritet kan påverka personer, om beslut som rör dem fattas utifrån uppgifter som är felaktiga eller som ändrats obehörigt. Till denna del sammanlänkas personuppgifternas integritet med principen om korrekthet (se kapitel 2.1.5).

Även om uppgifternas tillgänglighet inte separat omnämns i samband med dataskyddsprinciperna, har också detta beaktats i olika sammanhang i DSF. Den personuppgiftsansvarige ska försäkra sig om att personuppgifterna finns tillgängliga när de behövs. Personuppgifterna ska alltså skyddas mot att något av misstag eller avsiktligt, tillfälligt eller permanent hindrar användningen av personuppgifter för det planerade ändamålet. Sådana situationer kan även påverka de berörda personerna så att till exempel en tjänst eller tillhörande fri- eller rättighet inte kan utövas (t.ex. en

[21] https://tietosuoja.fi/sv/uppgifternas-korrekthet

löneutbetalning lyckas inte eller ersättningar enligt arbetsavtal för arbetsprestationer kan inte betalas, eller kontogireringar lyckas inte och det tillhörande utbytet fungerar inte).

Dataskyddsförordningen innehåller inga exakta definitioner av vilka tekniska och organisatoriska åtgärder de personuppgiftsansvariga och personuppgiftsbiträdena vid var tid ska genomföra. Åtgärderna kan förstås att på ett heltäckande sätt omfatta alla sätt och metoder vilka den personuppgiftsansvarige kan vidta i samband med behandlingen. Med lämplighet avses att dessa metoder är fungerande och tillräckligt effektiva. Tekniska eller organisatoriska åtgärder omfattar olika åtgärder på ett heltäckande sätt, från användning av tekniska lösningar till utbildning av anställda.

För att undvika obehöriga förändringar ska informationssystemet planeras så att endast behöriga användare kan ändra uppgifterna och att även sådana ändringar loggas för eventuell senare utredning. Loggdata är ett sätt att genomföra passerkontroll och bidra till att iaktta och ingripa i eventuella avvikelser. Tillgängligheten och integriteten kan stödjas till exempel genom att sörja för lämplig säkerhetskopiering.

Det förutsätts att de personuppgiftsansvariga följer den tekniska utvecklingen samt uppdaterar de tekniska och organisatoriska skyddsåtgärderna efter behov för att garantera att de är effektiva.

Mer information om att beakta dataskyddsprinciperna med hjälp av olika tekniska och organisatoriska åtgärder finns i anvisning 04/2019 om inbyggt dataskydd och dataskydd som standard[22].

När du bedömer hur dessa principer följs kan du använda dig av följande exempelfrågor:

- Vilka åtgärder som främjar personuppgifternas **konfidentialitet** används redan inom organisationen och i vilken utsträckning kan man stödja sig på dem i den behandling som bedöms?
- Vilka åtgärder som främjar personuppgifternas **integritet** används redan inom organisationen och i vilken utsträckning kan man stödja sig på dem i den behandling som bedöms?
- Vilka åtgärder som främjar personuppgifternas **tillgänglighet** används redan inom organisationen och i vilken utsträckning kan man stödja sig på dem i den behandling som bedöms?
- Har organisationen tillvägagångssätt för att regelbundet identifiera och analysera säkerhetshot mot personuppgifter och behandlings- och överföringssystem som gäller dem?
- Har organisationen förmåga att observera eventuella personuppgiftincidenter som gäller personuppgifternas säkerhet?
- Finns det en process och tillvägagångssätt för att reagera på personuppgiftsincidenter (inkl. rapporteringskanal för incidenter och riskbedömning gällande anmälningsskyldighet till dataskyddsmyndigheten/den registrerade)?
- Hur säkerställs det att åtgärder som tryggar personuppgifternas konfidentialitet, integritet och tillgänglighet är lämplig och tillräcklig även i framtiden?

2.2 Personuppgiftsbiträden

Ett personuppgiftsbiträde agerar i enlighet med den personuppgiftsansvariges anvisningar för den personuppgiftsansvarige eller för dennes räkning.

[22] edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

Den personuppgiftsansvarige bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige får använda endast sådana personuppgiftsbiträden som vidtar tillräckliga tekniska och organisatoriska säkerhetsåtgärder så att behandlingen uppfyller kraven i DSF.

Observera att personuppgiftsbiträde inte avser anställda hos en personuppgiftsansvarig som behandlar personuppgifter i sitt arbete. Du hittar mer information om den personuppgiftsansvariges och personuppgiftsbiträdets rolldefinition och skyldigheter i Europeiska dataskyddsstyrelsens anvisningar[23].

I dataskyddsförordningen föreskrivs direkta förpliktelser för personuppgiftsbiträden. Personuppgiftsbiträdet bör bistå den personuppgiftsansvarige med och ge den personuppgiftsansvarige råd i vissa skyldigheter som definieras i dataskyddsförordningen. Dessa skyldigheter är bland annat konsekvensbedömningar avseende dataskydd, anmälningar om personuppgiftsincidenter och deltagande i revisioner.

Personuppgiftsbiträdet ska dessutom genomföra tillräckliga skyddsåtgärder och lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna. Den personuppgiftsansvarige är skyldig att visa att dataskyddsprinciperna fullgörs effektivt också till de delar som ett personuppgiftsbiträde behandlar personuppgifter för den personuppgiftsansvariges räkning.

Läs mer om personuppgiftsbiträdens skyldigheter[24].

När du bedömer hur kraven som gäller användning av personuppgiftsbiträden uppfylls kan du använda dig av följande exempelfrågor:

- Deltar personuppgiftsbiträden i behandlingen? Identifiera personuppgiftsbiträdena.
- Uppfyller de anlitade personuppgiftsbiträdena de kriterier som ställs på dem (DSF artikel 28.1)? Hur säkerställs detta?
- Ar ett avtal som uppfyller kraven i artikel 28 i dataskyddsförordningen gjorts upp om behandlingen av personuppgifter?
- Har personuppgiftsbiträdena getts övriga nödvändiga, dokumenterade anvisningar? Vad har parterna kommit överens om i fråga om leveranssättet och ändringar i anvisningarna?

2.3 Överföring av personuppgifter utanför EES-området

Med stöd av DSF får personuppgifter överföras utanför Europeiska ekonomiska samarbetsområdet (EES) eller till internationella organisationer endast med de förutsättningar som definieras i kapitel V i DSF. Syftet med bestämmelserna i kapitel V är att säkerställa att nivån på dataskyddet i huvudsak är likadant som inom EES-området, när personuppgifter överförs till tredjeländer eller internationella organisationer.

Observera också i fråga om personuppgiftsbiträden (t.ex. molntjänstleverantörer) var personuppgifterna är belägna fysiskt. Till exempel anses åtkomsten till personuppgifter för ett

[23] edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
[24] https://tietosuoja.fi/sv/personuppgiftsbitraden

personuppgiftsbiträde som fungerar som tjänsteleverantör via fjärråtkomst utanför EES vara en överföring av personuppgifter utanför EES-området.

Om kommissionen har fattat ett beslut om adekvat skyddsnivå gällande det aktuella landet eller internationella organisationen[25], kan du överföra personuppgifter på samma förutsättningar som inom EES-området och ingen separat grund för överföring behövs. Observera dock att kommissionens beslut kan vara begränsat till ett visst område i eller en eller flera sektorer i tredjelandet (t.ex. beslutet som gäller Kanada omfattar endast kommersiella organisationer). Dessutom kan utvecklingen som sker i tredjeländer och internationella organisationer medföra förändringar i besluten. Om personuppgifter överförs till tredjeländer eller internationella organisationer och kommissionen inte har fattat ett beslut om adekvat skyddsnivå avseende det aktuella landet eller internationella organisationen, ska du försäkra dig om en lämplig grund för överföring i kapitel V i dataskyddsförordningen (t.ex. standardiserade dataskyddsbestämmelser som kommissionen antagit).

Mer information om olika grunder för överföring[26] samt om undantag som föreskrivs i artikel 49 i DSF och som endast är tillämpliga i separat specificerade särskilda situationer[27].

När internationella överföringar av personuppgifter och den överföringsgrund/de överföringsgrunder som används för dem har identifierats, ska personuppgiftsansvariga och personuppgiftsbiträden som överför uppgifterna från fall till fall kontrollera om de personuppgifter som överförs garanteras en sådan nivå på skyddet av personuppgifter som i huvudsak motsvarar nivån inom EES-området i tredjelandets lagstiftning och/eller tillvägagångssätt. Vid bedömningen ska överföringens omständigheter, det aktuella tredjelandets lagstiftning och den grund för överföring som används beaktas från fall till fall. Bedömningen ska dokumenteras omsorgsfullt på grund av ansvarsskyldigheten. Om skyddsåtgärderna som ingår i den grund för överförings om använts inte är tillräckliga, kan de i vissa fall kompletteras med tekniska, organisatoriska eller avtalsbaserade skyddsåtgärder. Om den grund för överföring som använts inte räcker till för att i huvudsak garantera samma nivå på dataskyddet och kompletterande skyddsåtgärder inte heller finns för att garantera en adekvat nivå på dataskyddet, ska överföringen inte genomföras.

Mer information om skyddsåtgärder som kompletterar grunderna för överföring och tillhörande bedömning[28].

Överföringar av personuppgifter till tredjeländer eller internationella organisationer kan ske också när behöriga myndigheter, till exempel Försvarsmakten, polisen, domstolar, Tullen, Gränsbevakningsväsendet och Brottspåföljdsmyndigheten utför uppgifter enligt 1 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (dataskyddslagen avseende brottmål, 1054/2018). På dessa överföringar tillämpas bestämmelserna i 7 kap. i dataskyddslagen avseende brottmål, vilka skiljer sig från artiklarna gällande överföring av personuppgifter i dataskyddsförordningen.

---

[25] Listning https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions.
[26] https://tietosuoja.fi/sv/overforing-av-personuppgifter-till-lander-utanfor-ees
[27] https://tietosuoja.fi/sv/undantag-i-sarskilda-situationer
[28] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, se också https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

När du bedömer lagligheten i överföringen av personuppgifter till tredjeländer kan du använda dig av följande exempelfrågor:

- Överförs personuppgifter utanför EU/EES eller till en internationell organisation? Om ja, till vilka länder och/eller vilken organisation?
- Har kommissionen fattat ett beslut om adekvat skyddsnivå (art. 45) avseende det aktuella landet eller internationella organisationen?
- Om inte, vilka skyddsåtgärder används vid överföring av personuppgifter utanför EES (art. 46)?
- Är den använda överföringsmekanismen tillräcklig för att garantera i huvudsak samma nivå på dataskyddet som inom EES utifrån en fallspecifik bedömning som du gjort? Om inte, vilka kompletterande skyddsåtgärder har införts och varför?

2.4. Se till att den registrerades rättigheter tillgodoses

Den personuppgiftsansvarige ska göra det lättare för den registrerade att utöva sina dataskyddsrättigheter samt vid behov tillgodose dataskyddsrättigheterna i enlighet med den registrerades begäran.

Med dataskyddsrättigheter avses den registrerades rättigheter i enlighet med kapitel III i den allmänna dataskyddsförordningen. Den registrerade har rätt till att

- få information om behandlingen av sina personuppgifter (se avsnitt 2.1.2)[29]
- få tillgång till uppgifterna[30]
- rätta uppgifter[31]
- radera uppgifter och bli glömd[32]
- begränsa behandlingen av uppgifterna[33]
- överföra uppgifterna från ett system till ett annat[34]
- invända mot behandlingen av uppgifterna[35]
- inte bli föremål för automatiserat beslutsfattande[36].

Vilka rättigheter den registrerade vid var tid kan utöva är beroende av vilken grund de ifrågavarande personuppgifterna behandlas. På dataombudsmannens byrås webbplats finns en tabell över på vilket sätt grunden för behandling påverkar de tillgängliga rättigheterna[37].

Fastställ i enlighet med grunden för behandling vilka dataskyddsrättigheter som hör samma med den aktuella behandlingen. Beskriv på vilket sätt rättigheterna beaktas vid behandlingen av personuppgifter samt hur begäranden som gäller rättigheterna behandlas och genomförs.

[29] https://tietosuoja.fi/sv/ratten-att-fa-information-om-behandlingen-av-personuppgifter
[30] https://tietosuoja.fi/sv/ratten-till-tillgang-till-uppgifter
[31] https://tietosuoja.fi/sv/ratten-att-ratta-uppgifter
[32] https://tietosuoja.fi/sv/ratten-att-radera-uppgifter
[33] https://tietosuoja.fi/sv/ratten-att-begransa-behandlingen-av-uppgifter
[34] https://tietosuoja.fi/sv/ratten-att-flytta-uppgifterna-mellan-system
[35] https://tietosuoja.fi/sv/ratten-att-gora-invandning-mot-behandlingen-av-uppgifter
[36] https://tietosuoja.fi/sv/ratten-att-inte-bli-foremal-for-automatiskt-beslutsfattande
[37] https://tietosuoja.fi/sv/vilka-rattigheter-har-den-registrerade-i-olika-situationer

2.4.1 Tillgodoseende av den registrerades rättigheter (DSF art. 12)

I artikel 12 i DSF fastställs på vilket sätt begäranden som gäller dataskyddsrättigheter ska behandlas. Den personuppgiftsansvarige ska säkerställa att dessa krav på behandling av begäranden uppfylls.

Läs mer om att tillgodose rättigheter[38].

När du bedömer hur kraven på detta uppfylls kan du använda dig av följande exempelfrågor:

- Finns det en process för att identifiera och behandla de registrerades begäranden?
- Hur säkerställs det att de tidsfrister som ställts för att besvara begäran i DSF följs?
- Har personalen utbildats i att identifiera begäranden från registrerade?
- Finns det en ansvarig person för att tillgodose den registrerades rättigheter?
- Hur säkerställs det att begäranden behandlas i rätt tid?
- Hur hjälper man de registrerade med att utöva sina dataskyddsrättigheter?
- Om den registrerade ombeds precisera sin begäran, hur säkerställs det att det inte gör det svårare att tillgodose hans eller hennes rättigheter?
- Hur försäkrar man sig om den registrerades identitet? Finns det förfaranden för oklara situationer? Hur säkerställs det att uppgifter inte lämnas till fel person?
- På vilka språk tillhandahålls tjänsten? Tillgodoses den registrerades rättigheter på dessa språk?
- Finns det ett formulär eller någon annan kontaktkanal för de registrerade att utöva sina rättigheter? Kan de registrerade hitta den lätt?
- Hur ser man till att anvisningar som gäller utövande av de registrerades rättigheter finns lättillgängliga för de registrerade?
- Hur sköts dokumenteringen av besvarande av de registrerades begäranden?
- I vilken form lämnas uppgifterna? Till exempel ljudband, video, skriftligt dokument osv.
- Hur har man försäkrat sig om att uppgifterna lämnas till den registrerade på ett informationssäkert sätt?

2.4.2 Rätt till tillgång (DSF artikel 15)

Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och en kopia av de uppgifter som behandlas. Dessutom ska den registrerade ges information om behandlingen av personuppgifterna. På detta sätt har den registrerade möjlighet att bedöma och säkerställa att behandlingen är laglig.

Läs mer om rätt till tillgång[39].

När du bedömer hur krav som gäller denna rätt uppfylls kan du använda dig av följande exempelfrågor:

- Är det möjligt att erbjuda den registrerade tillgång till sina egna uppgifter via en e-tjänst?
- Har det identifierats några grunder för begränsning som härrör från dataskyddsförordningen eller dataskyddslagen och som påverkar vilka uppgifter som ges till den registrerade?

[38] https://tietosuoja.fi/sv/den-registrerades-rattigheter
[39] https://tietosuoja.fi/sv/ratten-till-tillgang-till-uppgifter

- Kan alla uppgifter som gäller den registrerade sammanställas från olika källor inom tidsfristerna enligt artikel 12 i DSF?
- Kan en kopia av den registrerades uppgifter tas fram enkelt?
- Om den registrerade begär uppgifterna elektroniskt, finns det en möjlighet att lämna dem i elektronisk form?

2.4.3 Rätt till rättelse (DSF art. 16) samt anmälningsskyldighet (DSF art. 19)

Den registrerade har rätt att bli bedömd utifrån riktiga och korrekta uppgifter. Om uppgifterna är felaktiga eller bristfälliga ska de rättas.

Den personuppgiftsansvarige ska om möjligt underrätta varje mottagare till vilken personuppgifterna har lämnats ut om rättelser av personuppgifter. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Läs mer om rätten till rättelse[40].

När du bedömer hur krav som gäller denna rätt uppfylls kan du använda dig av följande exempelfrågor:

- Kan den registrerade erbjudas möjlighet att rätta uppgifter som gäller honom eller henne själv via en e-tjänst?
- Finns det ett tillvägagångssätt för att tillgodose olika rättelsebegäranden?
- Om enighet inte kan nås om rättelsens innehåll, är det möjligt att lägga till den registrerades synpunkter i samband med de uppgifter som påstås vara felaktiga?
- Kan mottagarna av uppgifterna utredas?

2.4.4 Rätt till radering (DSF art. 17) samt anmälningsskyldighet (TSA art. 19)

Den registrerade har i vissa situationer rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade.

Den personuppgiftsansvarige ska om möjligt underrätta varje mottagare till vilken personuppgifterna har lämnats ut om radering av personuppgifter. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Om den personuppgiftsansvarige har offentliggjort personuppgifterna och är skyldig att radera personuppgifterna, ska den personuppgiftsansvarige vidta rimliga åtgärder för att underrätta personuppgiftsansvariga som behandlar personuppgifterna om att den registrerade har begärt att de ska radera eventuella länkar till, eller kopior eller reproduktioner av personuppgifterna.

Läs mer om rätten till radering[41].

När du bedömer hur krav som gäller denna rätt uppfylls kan du använda dig av följande exempelfrågor:

[40] https://tietosuoja.fi/sv/ratten-att-ratta-uppgifter
[41] https://tietosuoja.fi/sv/ratten-att-radera-uppgifter

- Kan den registrerade erbjudas möjlighet att radera uppgifter om sig själv via en e-tjänst?
- Hur görs bedömningen om huruvida rätten till radering är tillämplig från fall till fall?
- Hur fungerar raderingsprocessen om den registrerade har återkallat sitt samtycke till behandling av uppgifter?
- Hur har det beaktats i raderingsprocessen om den registrerade gjort invändningar mot behandlingen av sina uppgifter för direktmarknadsföringsändamål?
- Hur genomförs raderingen av uppgifterna i praktiken (manuell/automatiserad radering, säkerhetskopior osv.)?
- Inom vilken tid raderas uppgifterna konkret (ångerfrister, profilåterställningar osv.)?
- Finns det hinder för raderingen? (lagstadgade lagringstider osv.)

2.4.5 Rätt till begränsning av behandling (DSF art. 18) samt anmälningsskyldighet (DSF art. 19)

Den registrerade kan i vissa situationer be den personuppgiftsansvarige att tillfälligt begränsa behandlingen av sina personuppgifter. I detta fall får personuppgifter som omfattas av begränsningen, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

Den personuppgiftsansvarige ska om möjligt underrätta varje mottagare till vilken personuppgifterna har lämnats ut om begränsning av behandling av personuppgifter. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Läs mer om rätten till begränsning av behandling[42].

När du bedömer hur krav som gäller denna rätt uppfylls kan du använda dig av följande exempelfrågor:

- Hur görs bedömningen om huruvida rätten till begränsning av behandling är tillämplig från fall till fall?
- Hur informeras den registrerade om att en genomförd begränsning lyfts?
- Hur genomförs begränsningen i praktiken i fråga om respektive informationssystem eller behandlingsfunktion?
- Har det identifierats några grunder för att vägra tillgodose begränsningsrätten?

2.4.6 Rätt till dataportabilitet (DSF art. 20)

Den registrerade har rätt att i vissa situationer få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig.

[42] https://tietosuoja.fi/sv/ratten-att-begransa-behandlingen-av-uppgifter

Läs mer om rätten till dataportabilitet[43].

När du bedömer hur krav som gäller denna rätt uppfylls kan du använda dig av följande exempelfrågor:

- Tillämpas rätten till dataportabilitet på den behandling som bedöms och vilka uppgifter gäller den?
- Hur utövas rätten till dataportabilitet i praktiken? Är det tekniskt möjligt?
- Kan man vid behov ta emot uppgifter som den registrerade överfört med stöd av rätten till dataportabilitet?

2.4.7 Rätt att göra invändningar (DSF art. 21)

Den registrerade har i vissa situationer rätt att invända mot behandlingen av sina personuppgifter, dvs. be att de inte behandlas alls.

Läs mer om rätten att göra invändningar[44].

När du bedömer hur krav som gäller denna rätt uppfylls kan du använda dig av följande exempelfrågor:

- Tillämpas rätten att göra invändningar på den behandling som bedöms? Vilka uppgifter gäller rätten att göra invändningar?
- Har frågor som gäller rätten att göra invändningar behandlats vid en eventuell analys av berättigat intresse?
- Hur utövas rätten att göra invändningar i praktiken?

2.4.8 Automatiserat beslutsfattande (inbegripet profilering) (DSF art. 22)

Den registrerade har i regel rätt att inte bli föremål för sådana beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Det finns dock undantag till denna huvudregel.

Läs mer om profilering och automatiserat beslutsfattande[45].

När du bedömer hur krav som gäller denna rätt uppfylls kan du använda dig av följande exempelfrågor:

- Omfattar behandlingen av personuppgifter automatiserat beslutsfattande som har rättsliga följder för den registrerade eller på liknande sätt i betydande grad påverkar den registrerade? Om ja, vad baseras detta på?
- Används uppgifter som hör till särskilda kategorier av personuppgifter? På vilken grund är detta möjligt?

[43] https://tietosuoja.fi/sv/ratten-att-flytta-uppgifterna-mellan-system
[44] https://tietosuoja.fi/sv/ratten-att-gora-invandning-mot-behandlingen-av-uppgifter
[45] https://tietosuoja.fi/sv/ratten-att-inte-bli-foremal-for-automatiskt-beslutsfattande

- Om grunden är a) att detta är nödvändigt för ingående eller fullgörande av ett avtal eller b) den registrerades uttryckliga samtycke, är skyddsåtgärderna tillräckliga?
- Vilka skyddsåtgärder används?
- Hur har dataskyddsprinciperna beaktats? Särskilt ändamålsbegränsning, minimering, korrekthet.
- Hur kan den registrerade kräva att en människa deltar i beslutsfattandet?
- Hur har man sett till att dataskyddsrättigheterna tillgodoses? Hur utövas rätten till rättelse och radering i både uppgifter som utgör grunden för beslutsfattande//profilering och skapade profiler?
- När och hur ges information om den registrerades rättigheter? I vilket skede av kundresan ges informationen?
- Hur har man skött om den skärpta informationsskyldigheten?
- Hur säkerställs den registrerades möjlighet att få tillgång till relevanta uppgifter om algoritmen? Vilka uppgifter lämnas till den registrerade?
- Hur informeras den registrerade om de uppgiftstyper eller uppgifter som använts vid skapandet av profilen/beslutsfattandet?
- Hur beskrivs de segment som den registrerade placerats i för honom eller henne?

3 Riskbedömning

När det har beskrivits på vilket sätt man försäkrat sig om att behandlingen av personuppgifter är laglig, ska de risker som förknippas med behandlingen av personuppgifter bedömas.

Riskbedömningen omfattar en identifiering av hot och konsekvenserna av att hoten realiseras samt en bedömning av konsekvensernas allvar och hotets sannolikhet.

3.1 Bedöm riskerna ur den registrerades perspektiv

Den personuppgiftsansvarige ska bedöma de risker som förknippas med behandlingen av personuppgifter ur den registrerades perspektiv. I detta fall bedömer den personuppgiftsansvarige vilka av den registrerades fri- och rättigheter ett hot som realiseras i behandlingen av personuppgifter kan äventyra och på vilket sätt samt vilka konsekvenser detta kan orsaka den registrerade.

Riskbedömning är en fortlöpande verksamhet: åtgärdernas tillräcklighet i förhållande till den risk som förknippas med behandlingen ska bedömas ständigt och uppdateras vid behov. Den personuppgiftsansvarige är också skyldig att påvisa att ett riskbaserat tillvägagångssätt har följts.

Risk

I denna anvisning avses med ”risk” ett scenario som beskriver en händelse och dess konsekvenser för den registrerade samt en bedömning av hur allvarliga och sannolika konsekvenserna är. Med en konsekvensbedömning enligt den allmänna dataskyddsförordningen strävar man efter att identifiera och hantera dessa risker.

Bild 2. En risk består av fyra faktorer: ett hot, konsekvenserna av hotet för den registrerade, konsekvensernas allvarlighet för den registrerade samt hotets sannolikhet.

Hot

Med hot avses en brist, svaghet eller sårbarhet i behandlingen av personuppgifter eller en händelse i anknytning till behandlingen som har en skadlig inverkan på dataskyddsprinciperna eller dataskyddsrättigheterna, och som kan ha negativa konsekvenser för den registrerades övriga rättigheter och friheter.

Vid riskbedömningen identifieras hoten och bedöms konsekvenserna för den registrerades rättigheter och friheter.

Vid identifiering av hot ska både interna och externa källor beaktas. Hoten kan uppstå av såväl uppsåtlig som oaktsam verksamhet.

Exempel på hot:

- utlämnande av uppgifter till fel person
- cyberattack som leder till driftsavbrott i informationssystemet
- dataintrång
- eldsvåda i maskinsal
- den registrerades begäran dirigeras till fel ställe

Konsekvenser

Hänvisningen till rättigheter och friheter i artikel 35 i DSF gäller i första hand rätten till dataskydd och rätten till integritet, men omfattar även andra grundläggande fri- och rättigheter, som uttrycksfrihet, tankefrihet, rörelsefrihet, förbud mot diskriminering, rätten till frihet eller religions- och samvetsfrihet. Konsekvenserna av hotet kan vara fysiska, materiella eller immateriella.

Relevanta konsekvenser med tanke på konsekvensbedömningen avseende dataskydd är sådana som föranleds av ett hot som realiserats i samband med behandlingen av personuppgifter. Dessa konsekvenser beaktas i stor omfattning. Konsekvenserna som gäller övriga fri- och rättigheter faller utanför konsekvensbedömningen när de är en följd av att sådana hot som inte förknippas med behandlingen av personuppgifter realiseras.

Målet med den allmänna dataskyddsförordningen är att skydda personers grundläggande fri- och rättigheter, särskilt deras rätt till personuppgiftsskydd. Till exempel berör konsekvenserna av förlorad konfidentialitet för personuppgifterna skyddet av personuppgifter och dataskyddsrättigheterna. Dessutom kan konsekvenserna beröra personens andra grundläggande fri- och rättigheter, som informerad självbestämmanderätt, likabehandling eller rörelsefrihet. Vilka andra fri- och rättigheter som behandlingen av personuppgifter kan äventyra beror på behandlingens art.

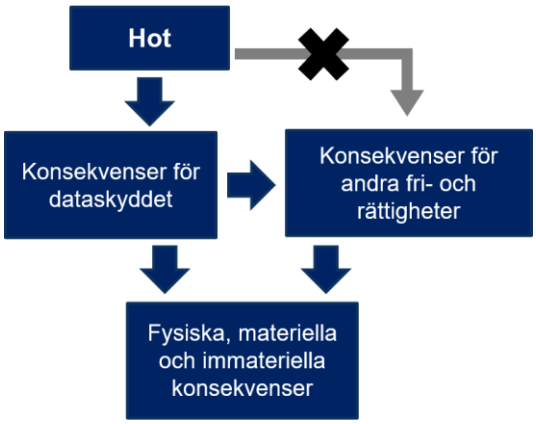


Bild 3. Konsekvenser som bedöms i KBD. Konsekvenserna för den registrerade kan indelas i fysiska, materiella och immateriella. De konsekvenser som bedöms i KBD berör primärt individens dataskydd. I KBD bedöms inte konsekvenser som berör endast andra fri- och rättigheter utan en koppling till behandlingen av personuppgifter. Konsekvenser för integritetsskyddet och behandlingen av personuppgifter kan dock återspeglas, och gör det också ofta, på personens övriga fri- och rättigheter. Sådana konsekvenser bedöms i KBD.

Allvar och sannolikhet

När de hot som föranleds av behandlingen av personuppgifter och deras konsekvenser för den registrerades fri- och rättigheter har identifierats, ska det bedömas hur allvarliga konsekvenserna är

samt hur sannolikt det är att hoten realiseras. Utifrån denna övergripande bedömning väljs de mest ändamålsenliga skyddsåtgärderna, med vilka man försöker sänka risknivån till en acceptabel nivå. Det är ofta omöjligt att helt eliminera riskerna.

3.2. Identifiera hoten

Bedömningen av risker relaterade till behandlingen av personuppgifter startas genom att kartlägga hoten som riktas mot behandlingen av personuppgifter. Därefter bedöms de eventuella konsekvenserna av att hoten realiseras, hur allvarliga de är samt hur sannolikt det är att hotet realiseras.

3.2.1 Tabell över hot

Som ett verktyg för att identifiera hoten kan man använda den tabell över hot som beskrivs i Excel-verktyget. I tabellen anges olika eventuella skeden i livscykeln för behandlingen av personuppgifter samt de dataskyddsprinciper som presenteras i början av anvisningen. När det gäller Säkerhet i samband med behandlingen-principen (DSF art. 5.1.f) behandlas konfidentialiteten, integriteten och tillgängligheten i behandlingen separat. Målet med tabellen är att främja en systematisk identifiering av hot och hjälpa att identifiera konkreta hot förknippade med den behandling som bedöms.

Tabellen fylls i på ett så konkret plan som möjligt. I varje punkt är det inte nödvändigtvis möjligt att identifiera ett hot. Å andra sidan kan det finnas flera hot i enskilda punkter. Vissa hot kan gälla flera dataskyddsprinciper eller behandlingsskeden. I detta fall är det viktigt att säkerställa att hotet antecknas i minst en punkt i tabellen.

Målet med exemplen på följande sida är att visa med vilken noggrannhet det är ändamålsenligt att identifiera och beskriva hoten.

Exempel 1
Identifiering av olika hot i ett s.k. visselblåsarsystem.

När hoten bedöms ur de registrerades perspektiv ska man i bedömningen specificera vilka personer eller personroller de uppgifter som ska behandlas i ett sådant syfte gäller. Med hjälp av identifiering av roller kan man specificera personens fri- och rättigheter i den aktuella behandlingen. Typiska roller är anmälare och den som anmälan gäller, om anmälan specificerar personen. Anmälarna uppmuntras att göra anmälningar och ett sätt för detta är ett löfte om att anmälningarna behandlas anonymt. I detta fall förknippas hotet som riktas mot anmälaren med att anonymiteten bryts och konsekvenser som detta medför för fri- och rättigheter (uttrycksfrihet) samt individuella materiella, fysiska och mentala konsekvenser.

Den andra personrollen är den som anmälan gäller, och till denna del kan som hot identifieras den diffusa och oidentifierade uppgiftskälla som anonymiteten orsakar (korrekthet). När uppgifter samlas in hos någon annan än personen själv, kan hotet riktas mot principen om öppenhet och den registrerades rättigheter. För det tredje kan uppgifter som gäller misstanke om missbruk hamna hos utomstående och till slut är det frågan om lagringstiden för sådana anmälningar och skyddet under lagringstiden och tillförlitlig förstöring. De övriga rättigheterna för den som anmälan gäller kan anses gälla oskuldspresumtion och omständigheter förknippade med en rättvis rättegång, som rätten att ta del av bevisningen och att bli hörd.

Exempel 2
En ifylld hottabell som beskriver hot som identifierats i en konsekvensbedömning av ett hypotetiskt informationssystem. Det rör sig om ett hypotetiskt informationssystem som används i ett stort hypotetiskt

företag, där man behandlar stora mängder uppgifter som hör till särskilda kategorier av personuppgifter samt utnyttjar ny teknik.

	Laglighet och korrekthet	Öppenhet	Ändamålsbegränsning	Uppgiftsminimering och lagringsminimering	Korrekthet	Integritet	Konfidentialitet	Tillgänglighet
Insamling		Man glömmer att datera information som ges till den registrerade, och de registrerade är inte medvetna om att uppgifter som gäller dem också fås från källa X.						
Registrering							Lösenorden registreras okrypterade i systemet.	
Sammanföring					En anställd samlar in personuppgifter om den registrerade också från en källa, vars riktighet man inte kan försäkra sig om.			
Användning och bearbetning			Den anställda använder personuppgifterna för ett annat ändamål än vad som ursprungligen avsågs.			På grund av en misslyckad uppdatering av användarbehörigheter kan vem som helst inom organisationen obehörigen redigera personuppgifterna.		
Utlämning och tillgängliggörande							Personuppgifter sparas av misstag på plats X, där de också finns tillgängliga för organisation B.	
Överföring till tredjeländer och övriga överföringssituationer	Personuppgifter sparas i strid med anvisningarna i en molntjänst utanför EES, vilket innebär överföring av uppgifter till ett tredjeland utan skyddsmetoder enligt den allmänna dataskyddsförordningen							

Lagring	En anställd raderar personuppgifter i enlighet med en fastslagen raderingsplan.				På grund av en driftstörning i systemet kan de registrerade inte själva uppdatera sina personuppgifter.			Man glömmer bort att säkerhetskopiera personuppgifterna.
Förstöring				Den anställda raderar personuppgifter som inte skulle få raderas.				

3.2.2 Andra verktyg och perspektiv på identifiering av hot

Nedan ges exempel på verktyg för effektiv identifiering av hot. Listan är inte uttömmande eller tvingande. Verktygen väljs efter den vid var tid aktuella behandlingens art och kontext.

Organisationens sakkunskap

När förutom sakkunniga inom dataskydd även sakkunniga inom informationssäkerhet, riskhantering och den praktiska verksamheten deltar i att göra konsekvensbedömningen, kan eventuella hot identifieras på ett heltäckande sätt ur olika perspektiv.

Befintliga visualiseringar

Till exempel är dataflödes- eller arbetsförloppsscheman eller andra motsvarande visuella beskrivningar till nytta när det gäller att identifiera möjliga hot. Genom att utnyttja en beskrivning av alla skeden i behandlingen av personuppgifter, redskap, dataflöden osv. kan man konkret iaktta de punkter som är exponerade för hot.

Identifiering av orsaker och källor till hot

Att skapa en uppfattning om orsakerna till olika hot hjälper att identifiera hoten. Med orsaker till hot avses aktörer eller praxis, vars åtgärder eller funktioner kan leda till att hotet realiseras.

Orsaker till hot kan finnas både inom organisationen och utanför den. Hoten kan bero på människors verksamhet eller icke-mänskliga orsaker.

När det är frågan om automatiserad behandling, kan det anses att även datamedier, enheter och program kan orsaka hot (t.ex. datorhaveri som sådant) Även kunder som deltar i behandlingen av uppgifter om dem själva samt deras terminaler och program som de använder kan orsaka hot. Traditionella orsaker till hot är obehöriga eller utomstående aktörer, som hackare.

Orsak till hot	Exempel
Interna	Anställda, IT-chefer, praktikanter, chefer som den personuppgiftsansvariges representanter
Externa	Mottagare av personuppgifter, behöriga tredje parter, tjänsteleverantörer, hackare, besökare, tidigare anställda, konkurrenter, kunder, underhållspersonal, kriminella, brottsligor, terroristorganisationer

Icke-mänskliga	Skadlig kod från en okänd källa (virus, skadliga program osv.), vatten (rörsystem osv.), lättantändliga, frätande eller explosiva material, naturkatastrofer, epidemier, djur

Tabell 1. De vanligaste orsakerna till hot[46]

Redskap som används för behandling av personuppgifter

För att identifiera hot rekommenderas det att kartlägga även hot som förknippas med de redskap som används för att behandla personuppgifter.

Särskilt när det gäller s.k. informationssäkerhetsrisker som riktas till exempel mot enheter, överföringskanaler och programvara som används för behandlingen är det nyttigt att gå igenom hoten mot konfidentialitet, integritet och tillgänglighet i den bifogade tabellen över hot ur perspektivet för enheter, dataöverföring och program (s.k. *supporting assets*) som är inkopplade till de planerade behandlingarna. Här kan man ta hjälp av till exempel ett dataflödesschema.

Resurser	Exempel
System	Utrustning och elektroniska datamedier (datorer, hårddiskar, USB-station); programvara (operativsystem, databaser, kommunikation, applikationer); datakommunikationsförbindelser (kablar, WiFI, fiberoptik)
Organisationer	Människor, dokument (utskrifter, kopior, handskrivna), dokumentöverföringskanaler (bl.a. e-post)

Tabell 2. Exempel på redskap som används för behandling av personuppgifter[47]

Personuppgifternas livscykel

Ett sätt att identifiera hot är att närma sig behandlingsfunktionerna i kronologisk ordning efter personuppgifternas livscykel. Då kan man identifiera de eventuella hot som kan realiseras vid behandlingen av personuppgifter i respektive skede av livscykeln. Hottabellverktyget som behandlades i avsnitt 3.2.1. visar ett tillvägagångssätt som baserar sig på personuppgifternas livscykel för identifiering av hot.

3.3. Bedöm hur allvarliga konsekvenserna är ur den registrerades perspektiv

När hoten mot de registrerade har identifierats, gäller det att bedöma hur allvarliga konsekvenserna av dessa hot är. Vid bedömningen ska man utöver de hot som direkt medför konsekvenser för den registrerades dataskydd även beakta konsekvenserna för de registrerades övriga grundläggande fri- och rättigheter. Beroende på fallet kan fri- och rättigheterna förenade med behandlingen av personuppgifter vara t.ex. hemfrid, skydd av konfidentiella meddelanden, rörelsefrihet, uttrycksfrihet och likabehandling. Vid bedömningen av allvarligheten ska de vanligaste fysiska, materiella och immateriella skadorna beaktas.

[46] CNIL: Privacy Impact Assessment (PIA) Knowledge Bases (February 2018 edition), https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf, s.3
[47] CNIL: Privacy Impact Assessment (PIA) Knowledge Bases (February 2018 edition), https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf, s. 2

Exempel på konsekvenser för övriga fri- och rättigheter:

- den registrerade har inte tillgång till sin nätbank på grund av ett förlängt underhållsstopp och kan inte göra betalningar i tid.
- att patientjournaler hamnar ut på det öppna nätet medför psykiskt lidande och möjliggör att uppgifterna missbrukas
- patientjournalernas tillgänglighet är förhindrad, vilket leder till att hälsa eller liv äventyras
- den registrerade har inte tillgång till uppgifter om samtalsupptagningar, och kan därför inte utreda sina avtalsrättsliga ansvar
- förlusten av konfidentialiteten för uppgifter som omfattas av spärrmarkering medför ett hot för personens säkerhet
- spridning av användarnamn och lösenord leder till att skyddet av konfidentiella meddelanden förloras och/eller obehörig användning av identiteten

Vid bedömningen av allvarligheten ska man också beakta personuppgifternas art, till exempel om uppgifterna är känsliga, sekretessbelagda eller om det rör sig om uppgifter som hör till särskilda kategorier av personuppgifter enligt artikel 9 i DSF eller uppgifter som rör fällande domar i brottmål samt överträdelser enligt artikel 10. Dessutom kan allvarligheten ökas om personerna som är föremål för behandlingen är särskilt sårbara, till exempel vid behandling av uppgifter om minderåriga eller personer som i övrigt är sårbara. Eftersom personuppgifter och olika personidentifierare (personbeteckning, kreditkortsuppgifter, användarnamn/lösenord) kan användas som redskap för olika brott vid t.ex. dataintrång, identitetsstölder och relaterade brott, ska man också fästa vikt vid hur lätt det är att missbruka uppgifterna.

Vid bedömningen av allvarligheten i de konsekvenser som orsakas de registrerade kan följande fyrastegstabell användas som hjälp[48]:

	Allmän beskrivning av konsekvenser	Exempel på individuella konsekvenser
1. Låg allvarlighet	Inga konsekvenser orsakas de registrerade eller de kan stöta på några problem som de lätt klarar sig igenom	Fysiska konsekvenser: • Tillfällig huvudvärk Materiella konsekvenser: • Tidsspillan för utredande av saken • Mottagning av skräppost • Återanvändning av uppgift som publicerats på en webbplats för riktad marknadsföring[49] Psykiska konsekvenser: • Känsla av kränkning av integritet utan riktig eller objektiv olägenhet

[48] CNIL: Privacy Impact Assessment (PIA) Knowledge Bases (February 2018 edition), https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf, s.4-5
[49] Se också: EDPB Guidelines 8/2020 on the targeting of social media users.

		• Rädsla för förlorad kontroll över uppgifterna
2. Måttlig allvarlighet	De registrerade kan stöta på betydande konsekvenser som de klarar sig igenom trots vissa svårigheter.	Fysiska konsekvenser: • Mindre fysiska besvär • Att bli utan vård för ett lindrigt besvär som därför blir allvarligare Materiella konsekvenser: • Oväntade eller extra avgifter, som felaktigt förelagda böter eller rättegångskostnader • Förhindrad tillgång till administrativa eller kommersiella tjänster • Kostnadsökning (t.ex. höjda försäkringspremier) • Förlust av bekvämligheter (t.ex. förlust av fritid, inköp eller semester, spärrning av användarnamn) Psykiska konsekvenser: • Mindre, men objektiva psykologiska men (ärekränkning, anseendeskador) • Relationsproblem med personliga eller yrkesbekanta (t.ex. försämrat anseende, förlust av erkänsla) • Hotelser i sociala nätverkstjänster • Känsla av kränkt integritet utan oåterkallelig skada
3. Betydande allvarlighet	De registrerade kan stöta på betydande problem som de borde klara sig igenom, även om detta sker via verkliga och betydande svårigheter.	Fysiska konsekvenser: • allvarligt fysiskt men som medför långvarig olägenhet (t.ex. försämrad hälsa på grund av avsaknad av vård) • kränkning av den fysiska integriteten Materiella konsekvenser: • Ekonomiska förluster som inte ersätts när uppgifterna har använts obehörigt • Icke-tillfälliga ekonomiska konsekvenser (tvingad låntagning), • Förbud mot att få bankkonto • Förlust av unik möjlighet till studie- eller praktikplats eller anställning • Förlust av bostad eller arbetsplats • Sitta fast utomlands Psykiska konsekvenser: • Allvarligt psykologiskt men (t.ex. depression eller fobiutveckling)

		• Känsla av kränkning av grundläggande fri- och rättigheter eller integritet på ett oåterkalleligt sätt • Nätmobbning och trakasserier • Bli offer för utpressning
4. Kritisk allvarlighet	De registrerade kan stöta på betydande eller till och med bestående konsekvenser som de inte nödvändigtvis klarar sig igenom.	Fysiska konsekvenser: • Långvarigt eller bestående fysiskt besvär • Död (t.ex. mord, självmord eller olycka med dödlig utgång) • Bestående men på grund av kränkning av den fysiska integriteten Materiella konsekvenser: • Avsevärd skuldsättning • Arbetsoförmåga • Förlust av bevismaterial i rättegång • Förhindrad tillgång till vital infrastruktur (vatten, el) Psykiska konsekvenser: • Långvarigt eller bestående psykologiskt men • Brutna familjeband • Straffrättsligt straff • Ändrad administrativ ställning eller förlust av rättslig autonomi (t.ex. intressebevakning)

3.4 Bedöm hur sannolikt det är att hoten realiseras

Efter att möjliga hot identifierats ska man bedöma hur sannolikt det är att de identifierade hoten realiseras.

Sannolikheten kan bedömas genom att identifiera eventuella svagheter eller sårbarheter som påverkar dataskyddet samt orsakerna till hoten och deras förmåga och villighet att utnyttja befintliga svagheter eller sårbarheter.

I praktiken startar man ofta inte från noll i bedömningen av sannolikheten, utan organisationen använder redan olika tekniska och organisatoriska skyddsåtgärder som minskar sannolikheten för hotet och som dataskyddsförordningen kräver. I detta fall bedöms hotets sannolikhet med hänsyn till de tillgängliga skyddsåtgärderna. Du kan beakta de faktorer som du identifierat i samband med bedömningen av hur principen för säkra uppgifter iakttas (avsnitt 3.1.6 Säkerhet i samband med behandling av personuppgifter).

Som bakgrund till bedömningen kan den historiska förekomsten av motsvarande hot användas, till exempel om det finns statistik över hur vanligt förekommande hotet är.

Exempel 3
Utomstående (orsak till hot) kan obehörigen få uppgifter genom att begära dem (hotfull händelse), och inga kontrollmetoder för att förhindra en sådan utlämning används. I detta fall är det sannolikt att orsaken till hotet förmår realisera hotet.

Vid bedömningen av hur sannolikt hotet är kan följande skala användas:

Osannolikt	Det verkar mycket osannolikt att det identifierade hotet skulle realiseras i den aktuella situationen (t.ex. stöld av pappersdokument från ett låst rum som är skyddat med passerkontroll eller åtkomst till en databas via det öppna nätet är möjligt, men kräver stark autentisering).
Möjligt	Det verkar osannolikt att det identifierade hotet skulle realiseras (t.ex. stöld av pappersdokument från ett låst rum eller åtkomst till en databas via det öppna nätet är möjligt, men lösenordet är svagt).
Sannolikt	Det verkar sannolikt att det identifierade hotet kommer att realiseras (t.ex. stöld av pappersdokument från ett kontor dit man inte kommer in utan att anmäla sig i receptionen eller databasen är helt öppen i det öppna nätet, men databasen kan inte hittas med sökmotorer).
Nästan säkert	Det verkar mycket sannolikt att det identifierade hotet kommer att realiseras (t.ex. stöld av pappersdokument från en offentlig entréhall eller databasen är helt öppen i det öppna nätet och hittas med sökmotorer.)

3.5 Definiera och genomför ytterligare skyddsåtgärder för att sänka hotens sannolikhet och konsekvensernas allvarlighet till en acceptabel nivå

När de skyddsåtgärder som genomförs i behandlingen av personuppgifter har planerats preliminärt, ska deras lämplighet och proportionalitet bedömas i förhållande till de identifierade hoten.

I fråga om skyddsåtgärdernas tillämplighet är det väsentligt att bedöma hur skyddsåtgärderna påverkar hoten. Minskar åtgärden hotets sannolikhet eller allvarlighet? Påverkar den båda? Till exempel påverkar inte en kryptering av uppgifter i ett datamedium inte i sig sannolikheten för att datamediet skulle försvinna, men den påverkar sannolikheten för att en eventuell utomstående innehavare av datamediet förmår utnyttja uppgifterna eller orsaka olägenhet eller skada med hjälp av dem.

Vid bedömningen av lämplighet och proportionalitet ska förutom behandlingens art, omfattning, sammanhang och ändamål även den senaste utvecklingen och genomförandekostnaderna beaktas.

Det förutsätts att de personuppgiftsansvariga följer den tekniska utvecklingen samt uppdaterar de tekniska och organisatoriska skyddsåtgärderna efter behov för att garantera att de är effektiva. När det gäller genomförandekostnader krävs inte en orimligt stor ekonomisk satsning på skyddsåtgärder av den personuppgiftsansvarige i förhållande till den risk som förknippas med behandlingen i situationer där förmånligare och effektiva skyddsåtgärder står till buds. Å andra sidan, även om hotets sannolikhet inte har bedömts att vara hög, men dess konsekvens för den registrerades fri- och rättigheter är allvarlig, kan det vara lämpligt och proportionellt att börja använda skyddsåtgärder som inte vore motiverade enbart utifrån en ekonomisk bedömning. En risk som felaktigt bedömts i underkant är inte en grund för att försumma skyddsåtgärderna.

Hotbedömning är en fortlöpande verksamhet, vilket innebär att skyddsåtgärdernas lämplighet och proportionalitet i förhållande till riskerna som förknippas med behandlingen ska bedömas ständigt och uppdateras vid behov.

Om man i bedömningen av skyddsåtgärdernas lämplighet och proportionalitet kommer fram till att hotets sannolikhet eller allvarlighet inte kan accepteras, ska nödvändiga ytterligare åtgärder genomföras för att reducera denna kvarstående risk till en acceptabel nivå. Skyddsåtgärderna kan vara förberedande inför hot, förebyggande, begränsande, iakttagande eller korrigerande med avseende på realiserade hot eller orsaker som lett till dem.

När ytterligare skyddsåtgärder väljs ska det beaktas att de krav som uttryckligen ställs i DSF utgör minimistandarden som ska iakttas i alla fall. Således kan den ytterligare åtgärden inte vara en åtgärd som den allmänna dataskyddsförordningen kräver att ska genomföras i vilket fall som helst. Till exempel ska man i behandlingsprocessen för iakttagande av kravet på uppgiftsminimering (DSF art. 5.1.c samt avsnitt 3.1.4) säkerställa att inga onödiga kopior på personuppgifterna inte uppstår vid behandlingen. De valda åtgärderna ska dessutom stämma överens med författningarna (t.ex. föreskrivna lagringstider).

Exempel 4

I tabellen nedan anges vissa av de hot som illustreras ovan i exempel 1, ytterligare skyddsåtgärder som riktas mot dem samt konsekvenser av dessa åtgärder.

	Åtgärd	Konsekvens
Laglighet och korrekthet	Automatisera radering av personuppgifter.	Det är mer osannolikt att raderingen av uppgifterna glöms bort och att uppgifterna lagras för länge utan grund.
Öppenhet och den registrerades rättigheter	Uppdateringen av information som ges till den registrerade görs till en regelbundet återkommande uppgift. Definiera ansvariga personer för uppdatering av informationen.	Det är mer osannolikt att informationen som den registrerade får är föråldrad eller bristfällig.
Ändamålsbegränsning	Anordna personalutbildning som behandlar tillåtna ändamål för personuppgifter.	Det är mer osannolikt att personuppgifter behandlas i strid med ändamålet.

Uppgiftsminimering och lagringsminimering	Pseudonymisera de uppgifter som behandlas.	Till exempel vid ett eventuellt datainträng blir konsekvenserna inte lika allvarliga.
Korrekthet	Ordna möjlighet för de registrerade att själva uppdatera sina uppgifter eller uppdatera uppgifterna automatiskt från en tillförlitlig källa.	Det är mer osannolikt att personuppgifterna som behandlas är felaktiga eller föråldrade.
Integritet, konfidentialitet och tillgänglighet	Ta fram anvisningar för personalen om besvarande av utlämnings- och informationsbegäranden gällande personuppgifter.	Det är mer osannolikt att personuppgifter lämnas ut obehörigen av misstag utanför organisationen.
	Lägg till en egenskap som förhindrar användare att radera vissa uppgifter i systemet.	Det är mer osannolikt att nödvändiga personuppgifter raderas av misstag eller avsiktligt.
	Automatisera säkerhetskopiering.	Det är mer osannolikt att säkerhetskopieringen glöms bort och att personuppgifterna går slutgiltigt förlorade.

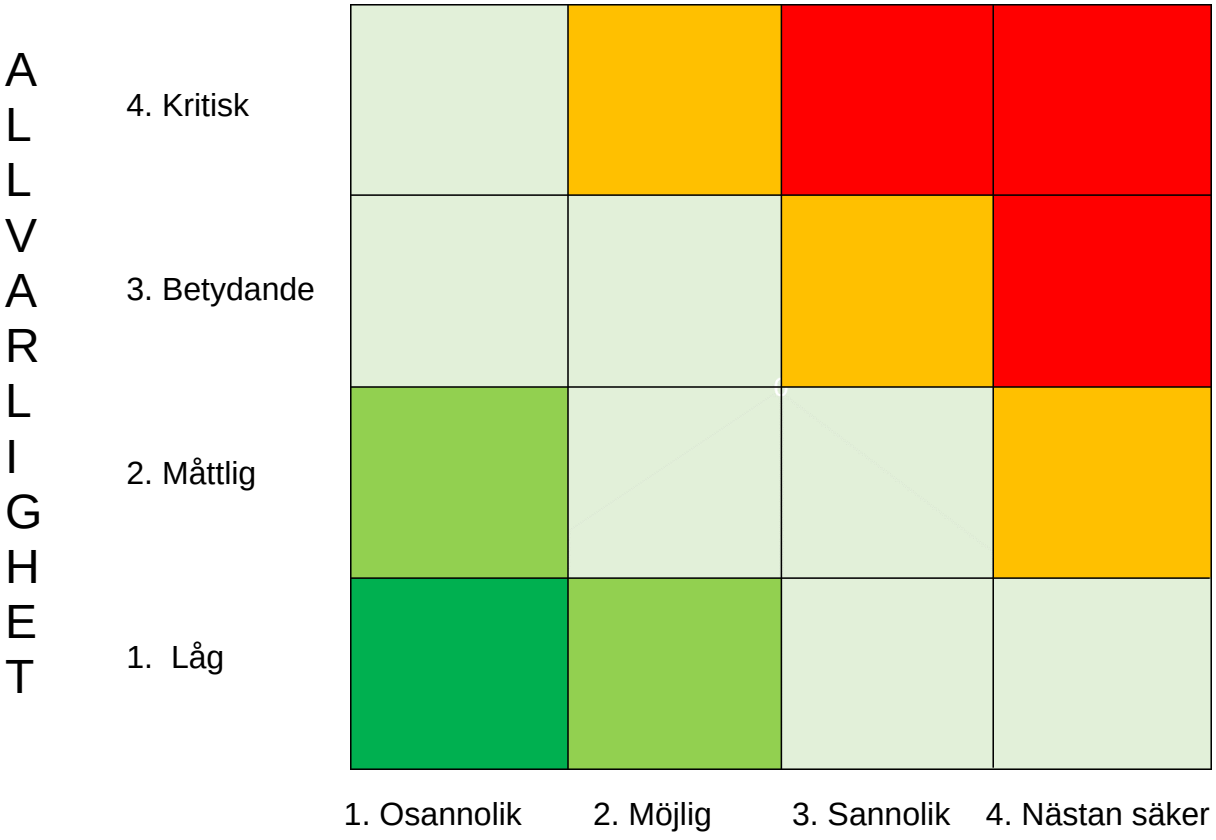
3.6 Gör upp en sammanfattning bedömningen av hotens sannolikhet och konsekvensernas allvarlighet

Placera varje hot efter den allvarlighet och sannolikhet som bestämts för den enligt tabellen på nästa sida.

Tabellen som uppstår innehåller varje identifierat hot efter hur allvarliga dess konsekvenser är och hur sannolikt det är. Tabellen visar nivån för varje identifierad risk.

När risken är placerad på nivån som anges med röd färg, är risknivån mycket hög. När risken anges med orange färg, är den hög. Risknivån minskar stegvis, och i den mörkgröna punkten är risknivån låg.

När risken ligger på en nivå som anges med röd eller orange färg, finns det skäl att inleda förhandssamråd.


ALLVARLIGHET
4. Kritisk
3. Betydande
2. Måttlig
1. Låg
1. Osannolik
2. Möjlig
3. Sannolik
4. Nästan säker
SANNOLIKHET

4 Godkännande av konsekvensbedömning avseende dataskydd och möjliga korrigerande åtgärder

När de steg som beskrivs ovan har utförts, godkänner den personuppgiftsansvarige konsekvensbedömningen avseende dataskydd, riskerna och risknivåerna som identifierats i den, samt de valda korrigerande åtgärderna. Varje organisation bör fastställa en process för godkännandet. För ledningen kan man till exempel göra upp en sammanfattning, där konsekvensbedömningens slutresultat samt behövliga motiveringar framgår.

Det rekommenderas att offentliggöra konsekvensbedömningen avseende dataskydd, men det är inte obligatoriskt. Alternativt kan konsekvensbedömningen offentliggöras delvis, så att till exempel affärshemligheter eller omständigheter som äventyrar dataskyddet för behandlingen röjs.

Åtminstone följande omständigheter ska dokumenteras innan konsekvensbedömningen godkänns:
- Vilka ytterligare skyddsåtgärder kommer att införas? Vilken är tidsplanen? Vem genomför dem?
- Har riskerna kunnat elimineras helt eller reduceras till en godtagbar nivå? Eller accepteras riskerna sådana som de är?
- Slutlig kvarstående risk efter ytterligare skyddsåtgärder
- Finns det anledning att begära förhandssamråd med dataskyddsmyndigheten?

Förhandssamråd

Det är inte alltid möjligt att helt eliminera alla risker. Vissa risker kan anses vara acceptabla med hänsyn till de tillgängliga skyddsåtgärderna och fördelarna som behandlingen medför. Om risken förblir hög trots att de ytterligare åtgärderna utförts, ska man begära förhandssamråd med dataskyddsmyndigheten innan behandlingen påbörjas. Den personuppgiftsansvarige har ansvaret för att inleda förhandssamrådsförfarandet.

Förhandssamråd ska begäras till exempel om de registrerade kan drabbas av betydande eller till och med oåterkalleliga konsekvenser som de inte kan övervinna (t.ex. obehörig åtkomst till uppgifter som innebär risk för de registrerades liv, en uppsägning, en finansiell risk), och/eller när det förefaller uppenbart att risken kommer att inträffa (t.ex. genom att inte kunna minska antalet personer som har tillgång till uppgifterna på grund av delning, användning eller distributionsmetoder, eller om en välkänd sårbarhet inte kan avhjälpas).

Dataombudsmannen ger med anledning av begäran om förhandssamråd vid behov skriftliga anvisningar till den personuppgiftsansvarige eller personuppgiftsbiträdet om de åtgärder som sak vidtas för att reducera risken. Dataombudsmannens skriftliga anvisningar begränsas efter konsekvensbedömningens objekt samt de höga kvarstående risker som identifierats i den. Vid behov kan dataombudsmannen i samband med samrådet också utöva de befogenheter som getts den i dataskyddsförordningen, som varning. Den personuppgiftsansvarige och personuppgiftsbiträdet bör utföra de ytterligare åtgärderna enligt anvisningen för att reducera riskerna innan behandlingen av personuppgifter inleds.

Läs mer om förhandssamråd[50].

[50] https://tietosuoja.fi/sv/forhandssamrad

Övriga anvisningar om konsekvensbedömning avseende data-skydd och källmaterial:

- Anvisning av Arbetsgruppen för skydd av personuppgifter (WP 29) 4.10.2017 wp 248 rev.01
- EDPB guidelines 4/2019 (v.2.0) on Data Protection by Design and by Default
- EDPS Accountability on the ground Part II: Data Protection Impact Assessment & Prior Consultation (v.1.3 July 2019)
- CNIL Privacy Impact Assessment (PIA) 2.2018
    - Methodology, Template and Knowledge bases
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems (v.2, 13.9.2018)
- SFS-ISO/IEC 29134:2018 Ohjeita tietosuojavaikutusten arviointiin

Begrepp

Anonymisering
Anonymisering innebär behandling av personuppgifter så att en person inte längre kan identifieras i dem. Identifieringen måste förhindras oåterkalleligt och så att den personuppgiftsansvarige eller någon annan utomstående aktör inte med de uppgifter som innehas kan omvandla uppgifterna så att de åter är identifierbara. Anonymiserade uppgifter anses inte längre vara personuppgifter. På dessa tillämpas inte dataskyddsbestämmelserna.

Ansvarsskyldighet
Ansvarsskyldighet innebär att den personuppgiftsansvarige och personuppgiftsbiträdet i praktiken ska kunna visa att dataskyddsförordningen efterlevs. Ansvarsskyldigheten kan fullgöras till exempel genom att dokumentera.

Behandling av personuppgifter
Med behandling avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Dataskyddsdirektivet och dataskyddslagen avseende brottmål (DSIB)
Bestämmelser om behandlingen av personuppgifter i brottmål finns i dataskyddslagen avseende brottmål, som trädde i kraft 1.1.2019. Lagen tillämpas när polisen, åklagarna domstolarna, Brottspåföljdsmyndigheten, Tullen, gränsbevakningsmyndigheterna och andra behöriga myndigheter behandlar personuppgifter i brottmål.

Dataskyddsdirektivet har genomförts genom dataskyddslagen avseende brottmål. Syftet med EU-direktivet är att modernisera bestämmelserna, att underlätta det fria flödet av uppgifter mellan polismyndigheter och straffrättsliga myndigheter i EU-länderna och att säkerställa skyddet för personuppgifter när brottmål handläggs.

Dataskyddslagen
En nationell allmän lag som preciserar EU:s allmänna dataskyddsförordning och som trädde i kraft 1.1.2019.

Dataskyddsombud
Dataskyddsombudet är en intern sakkunnig inom organisationen, som följer behandlingen av personuppgifter och hjälper till att följa dataskyddsbestämmelserna. När de förutsättningar som ställs i dataskyddsförordningen uppfylls är det obligatoriskt för organisationen att utse ett dataskyddsombud.

Europeiska dataskyddsstyrelsen (EDPB)
Europeiska dataskyddsstyrelsen är ett oberoende EU-organ som bidrar till en enhetlig tillämpning av dataskyddsregler i hela Europeiska unionen och främjar samarbete mellan EU:s dataskyddsmyndigheter. Europeiska dataskyddsstyrelsen består av företrädare för nationella dataskyddsmyndigheter (inkl. dataombudsmannens byrå) och Europeiska datatillsynsmannen (EDPS).

EU:s allmänna dataskyddsförordning (DSF, GDPR)
En förordning som reglerar behandlingen av personuppgifter, som började tillämpas i alla EU-länder 25.5.2018.

Förhandssamråd
Med förhandssamråd avses en situation där den personuppgiftsansvarige innan behandlingen av personuppgifter inleds ska samråda med dataskyddsmyndigheten. Förhandssamråd ska hållas när konsekvensbedömningen visar att behandlingen skulle leda till en hög risk för de registrerade och om den personuppgiftsansvarige inte genom sina egna åtgärder har kunnat minska risken.

Gemensamt personuppgiftsansvariga
Om minst två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen är de gemensamt personuppgiftsansvariga.

Inbyggt dataskydd och dataskydd som standard
Med inbyggt dataskydd avses att dataskyddsprinciperna byggs in i verktyg, produkter, applikationer eller tjänster som erbjuds personuppgiftsansvariga. Med dataskydd som standard avses att verktyg, produkter, applikationer eller tjänster som standard garanterar att behandlingen begränsas till bara sådana personuppgifter som är nödvändiga med tanke på ändamålet med behandlingen.

Informationssäkerhet
Informationssäkerhet är ett sätt för att genomföra dataskyddet. Dess syfte är att skydda data och informationssystem. Informationssäkerhet avser bland annat organisatoriska och tekniska åtgärder för att säkerställa informationens konfidentialitet och integritet, systemens tillgänglighet samt tillgodoseende av den registrerades rättigheter.

Konsekvensbedömning avseende dataskydd (KBD)
Syftet med en konsekvensbedömning avseende dataskydd är att identifiera och minimera risker förknippade med behandlingen av personuppgifter samt att ta fram material för att kunna bevisa efterlevnaden av dataskyddsregleringen.

Kvarstående risk
Den risk som återstår efter att skyddsåtgärderna genomförts och som man inte kan eller vill eliminera. Den slutliga bedömningen om risken efter att skyddsåtgärder tagits i bruk.

Mottagare
Med mottagare avses i dataskyddsförordningen alla de aktörer (fysiska eller juridiska personer, myndigheter, ämbetsverk eller andra organ) till vilka personuppgifter överförs eller lämnas ut.

(Person)register
Med register avses en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.
Observera att dataskyddsförordningen till skillnad från den tidigare personuppgiftslagen tillämpas på automatiserad behandling av personuppgifter, oavsett om uppgifterna bildar ett register.
Huruvida ett register eller en del av ett register bildas är väsentligt endast när det är frågan om manuell behandling.

Personuppgift
Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person. Personuppgifter kan finnas lagrade i till exempel elektroniska filer, databaser, på papper, i ett kartotek, i mappar eller som ljud- eller bildupptagningar.
Som identifierbar ses en fysisk person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsansvarig
Med personuppgiftsansvarig avses en person, ett företag, en myndighet eller ett samfund som fastställer syftet och metoderna för behandling av personuppgifter.

Personuppgiftsbiträde
Personuppgiftsbiträde kallas en aktör som är utomstående i förhållande till den personuppgiftsansvarige och som behandlar personuppgifter för den personuppgiftsansvariges räkning och enligt den personuppgiftsansvariges anvisningar.

Personuppgiftsincident
Med en personuppgiftsincident avses en händelse som leder till att personuppgifter förstörs, försvinner, ändras, olovligen överlåts eller hamnar i händerna på en aktör som saknar rätt att behandla dem.

Profilering
Profilering avser automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person. Med profilering avses särskilt analys eller förutseende av aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar.

Pseudonymisering
Pseudonymisering avser behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik person utan kompletterande uppgifter. Sådana kompletterande uppgifter ska förvaras omsorgsfullt och separat från personuppgifterna. Pseudonymiserade uppgifter är fortfarande personuppgifter, och dataskyddsbestämmelserna ska tillämpas på behandlingen av dem.

Register över behandling
Register över behandling är en skriftlig beskrivning av den behandling av personuppgifter som en organisation utfört. Registret är ett internt dokument inom organisationen. Det fungerar som ett hjälpmedel för att skapa en uppfattning om behandlingen av personuppgifter, och dess syfte är att för sin del påvisa att personuppgifterna behandlas i enlighet med dataskyddslagstiftningen.

Registrerad
Registrerad är den person som personuppgiften gäller (se även **Personuppgift**).

Risk
Med risk avses ett scenario som beskriver en händelse och dess påföljder för den registrerade samt en bedömning om påföljdernas allvar och händelsens sannolikhet.

Riskhantering
En samordnad verksamhet för att styra och övervaka organisationen i fråga om risker.

Samtycke
Samtycke är en möjlig rättslig grund för behandling av personuppgifter. Samtycke ger den registrerade möjlighet att övervaka behandlingen av sina personuppgifter och påverka behandlingen av personuppgifter genom att återkalla samtycket. Bestämmelser om förutsättningarna för samtycke finns i artikel 7 i dataskyddsförordningen.

Särskilda kategorier av personuppgifter
Behandlingen av personuppgifter som hör till så kallade särskilda kategorier av personuppgifter är i princip förbjuden. Sådana uppgifter avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter om hälsa, uppgifter om sexualliv eller

sexuell läggning eller genetiska uppgifter och biometriska uppgifter för att identifiera en fysisk person.

Tredjeland
Ett land utanför Europeiska ekonomiska samarbetsområdet (EES). Till EES-området hör förutom EU-länderna även Island, Liechtenstein och Norge.

WP29
WP 29-arbetsgruppen, efter artikel 29 i dataskyddsdirektivet, var en oberoende EU-arbetsgrupp som behandlade frågor gällande skyddet för individer i behandling av personuppgifter fram tills att den allmänna dataskyddsförordningen började tillämpas. (se. Europeiska dataskyddsstyrelsen (EDPB))

Bilagor

BILAGA I Excel-verktyg
BILAGA II Konsekvensbedömning avseende dataskydd enligt dataskyddslagen avseende brottmål