**Konsekvens-bedömning avseende dataskydd (DPIA)**

[*Namn på projekt/it-system/behandling/etc.*]



**Versionshistorik mall**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Ansvarig | Ändringar |
| 1.0 | 2021-03-16 | Regional dataskyddsfunktion,  Region Skånes dataskyddsombud | Dokument upprättat. Innehåll utformat utifrån Integritetsskyddsmyndigheten, ICO, CNIL och EDPB:s riktlinjer för konsekvensbedömning avseende dataskydd. |
|  | | | |

**Versionshistorik konsekvensbedömning**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Datum | Ansvarig | Deltagare | Ändringar |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  | | | | |

**Innehållsförteckning**

[1 Övergripande information](#_Toc66779501)

[2 Krav på att en konsekvensbedömning ska genomföras](#_Toc66779502)

[3 Systematisk beskrivning av personuppgiftsbehandlingen](#_Toc66779503)

[4 Uppfyllnad av grundläggande dataskyddsprinciper](#_Toc66779504)

[5 Åtgärder som stärker den registrerades rättigheter](#_Toc66779505)

[6 Risker och mitigerande åtgärder](#_Toc66779506)

[7 Rådfrågan och granskning](#_Toc66779507)

# Övergripande information

## Personuppgiftsansvarig(a) för personuppgiftsbehandlingen

|  |
| --- |
| Region Skåne, organisationsnummer 232100–0255 |

## Kontaktuppgifter till dataskyddsombud

|  |
| --- |
| Dataskyddsombudet, Region Skåne, 291 89 Kristianstad  Telefon: 044-309 30 00  E-post: region@skane.se |

## Ansvarig(a) för konsekvensbedömningen

### Genomförande

**Namn och e-post till den/de som ansvarar för konsekvensbedömningens genomförande och kan fungera som kontaktperson i ärendet om någon del behöver förtydligas eller följas upp.**

|  |
| --- |
|  |

### Förvaltning

**Namn och e-post till den/de som ansvarar för att förvalta konsekvensbedömningen, vilket innebär att se till att den är aktuell och att åtgärderna är fortsatt effektiva om behandlingen, omständigheter eller risker ändras.**

|  |
| --- |
|  |

## Projektinformation

**Om personuppgiftsbehandlingen planeras inom ett projekt, ange projektnamn och eventuellt projekt-ID.**

|  |
| --- |
|  |

## Systeminformation

**Om personuppgiftsbehandlingen sker eller kommer att ske inom ett it-system, ange systemnamn och system-ID.**

|  |
| --- |
|  |

## Kortfattad beskrivning av personuppgiftsbehandlingen

**Beskriv kortfattat projektet, it-systemet, den nya funktionen i it-systemet etc. som behandlingen omfattar. Denna information kan exempelvis finnas i en projektplan. Beskriv även avgränsningen för denna konsekvensbedömning.**

|  |
| --- |
|  |

## Personuppgiftsbehandlingens effektmål

**Beskriv vilka förväntade effekter personuppgiftsbehandlingen kommer att få för den registrerade.**

*Dessa frågor besvarar vad Region Skåne vill uppnå med personuppgifts-behandlingen och vilka positiva effekter den kommer att få.*

*i*

**Beskriv vilka förväntade effekter behandlingen kommer att få både för Region Skåne och i ett bredare perspektiv, exempelvis för sjukvården i ett nationellt eller globalt perspektiv.**

|  |
| --- |
|  |

## Extern konsekvensbedömning

Om konsekvensbedömningen ska genomföras inom ramen för ett större projekt eller ett program ska Region Skånes dataskyddsombud rådfrågas avseende genomförande, resurssättning och behov av externa resurser.

|  |  |
| --- | --- |
|  |  |
| Dataskyddsombudet har rådfrågats |  |
| Frågan är ej tillämplig för denna konsekvensbedömning |  |
|  |  |

# Krav på att en konsekvensbedömning ska genomföras

## Om personuppgiftsbehandlingen sannolikt innebär en hög risk[[1]](#footnote-2)

*Genom att svara på frågorna i avsnitt 2.1.1. och 2.1.2 kan man avgöra om behandlingen sannolikt innebär en hög risk för den registrerades rättigheter och friheter och därför kräver en konsekvensbedömning. Vid bedömningen om behandlingen sannolikt innebär en hög risk är det lämpligt att ta hjälp av en dataskyddssamordnare. Kontaktuppgifter finns på Region Skånes intranät.*

*i*

### Kriterier för hög risk (art. 35.3 DSF)[[2]](#footnote-3)

*Om en eller fler av frågorna i detta avsnitt besvaras med ”ja” krävs en konsekvensbedömning.*

*i*

|  |  |  |
| --- | --- | --- |
| Kriterium | Ja | Nej |
| Systematisk och omfattande profilering som har rättsliga följder för individer eller på liknande sätt i betydande grad påverkar individer |  |  |
| Behandling i stor omfattning av känsliga personuppgifter |  |  |
| Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser |  |  |
| Systematisk övervakning av en allmän plats i stor omfattning |  |  |
|  | | |

### Kontrollfrågor för hög risk[[3]](#footnote-4)

*Om två eller fler av frågorna i detta avsnitt besvaras med ”ja” krävs en konsekvensbedömning.*

*i*

|  |  |  |
| --- | --- | --- |
| Kriterium | Ja | Nej |
| Kommer personer att analyseras, utvärderas, profileras eller poängsättas på något sätt? |  |  |
| Kommer det fattas automatiserade beslut med rättsliga eller liknande betydande följder för den registrerade? |  |  |
| Kommer personer att övervakas på ett systematiskt sätt? |  |  |
| Omfattar personuppgiftsbehandlingen känsliga personuppgifter eller personuppgifter av mycket personlig karaktär? |  |  |
| Kommer personuppgifter att behandlas i stor omfattning? |  |  |
| Kommer olika register att samköras? |  |  |
| Rör personuppgifterna sårbara personer, till exempel barn, anställda, asylsökande, äldre och patienter? |  |  |
| Kommer teknik användas på ett nytt och innovativt sätt eller kommer nya organisatoriska lösningar användas? |  |  |
| Är det risk för att personuppgiftsbehandlingen i sig hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal? |  |  |
|  | | |

### Övriga faktorer som leder till hög risk

**Beskriv övriga faktorer som leder till att personuppgiftsbehandlingen kan innebära en hög risk.**

*Att behandlingen innebär en hög risk för den registrerade kan även framgå av en riskanalys, exempelvis genom att man identifierar tidigare oidentifierade person-uppgiftsbehandlingar såsom tredjelandsöverföringar.*

*i*

|  |
| --- |
|  |

### Undantag från att genomföra en konsekvensbedömning (art. 35.3 DSF)

*En konsekvensbedömning behöver inte genomföras om något av följande kriterier uppfylls. Om ”ja” väljs för något av kriterierna ska detta motiveras och en data-skyddssamordnare ska skriva ett utlåtande i avsnitt 7.2.*

*i*

|  |  |  |  |
| --- | --- | --- | --- |
| Kriterium | Ja | Nej | Motivering |
| Behandlingen leder sannolikt *inte* till höga risker |  |  |  |
| Behandlingens art, omfattning, sammanhang och ändamål är mycket lika en behandling för vilken en konsekvensbedömning redan har genomförts inom Region Skåne |  |  |  |
| Konsekvensbedömning är redan genomförd som en del av upprättandet av en lag som reglerar behandlingen |  |  |  |
|  | | | |

# Systematisk beskrivning av personuppgiftsbehandlingen

Detta avsnitt ska ge en tydlig överblick över de aktuella personuppgiftsbehandlingarna (art. 35.7 a DSF).

## Beskrivning av behandlingar

*I tabellen nedan ska det inventeras vilka personuppgiftsbehandlingar som är aktuella, vad de innehåller och hur de utförs. Om konsekvens-bedömningen omfattar mer än en personuppgiftsbehandling med mer än ett ändamål, beskriv dessa behandlingar och deras olika ändamål. Ett it-system kan innehålla flera behandlingar med olika ändamål som ”loggning för uppföljning av att interna regler följs” och ”drift och support i enlighet med huvudavtalet”. Kursiv text i tabellen är exempel och inte en uttömmande lista över behandlingar.*

*i*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Personuppgifts-behandling | Ändamål | Personuppgifter | Person-uppgifts-biträde | Kategorier av registrerade | Insamling | Externa mottagare | Lagring/  lagringstid | Radering/  arkivering |
| [*Loggning av information i vårdsystem, görs kontinuerligt*] | [*För uppföljning av verksamheten*] | [*Namn, RSID, personnummer* *i form av metadata*] | [*Tieto. PUB-avtal inklusive instruktioner tecknat.*] | [*Anställda, patienter, barn, asylsökande*] | [*Direkt från de registrerade:* *användning av tjänsten loggas automatiskt*] | [*Tjänste-leverantören och dess underbiträden, Lunds universitet*] | [*Vissa loggar lagras i Region Skåne it-infrastruktur i Sverige. Andra loggar lagras i Microsofts egen infrastruktur på servrar på Irland. Loggarna lagras i fem år.*] | [*Administratörer har möjlighet att radera personuppgifter. Gallring av loggar sker i enlighet med Region Skånes styrande dokument för gallring.*] |
| [*Lagring av filer innehållandes personuppgifter som laddas upp i tjänsten, görs kontinuerligt*] | [*För att administrera anställdas anställning*] |  |  |  |  |  |  |  |
| [*Underbiträdens åtkomst* *till personuppgifter i klartext för att kunna genomföra support, görs på regelbunden basis*] | [*Drift och support i enlighet med huvudavtalet*] |  |  |  |  |  |  |  |
| [*Automatiserat beslutsfattande, görs dagligen*] |  |  |  |  |  |  |  |  |
| [*Forskningsdata skickas till internationell forskningsnod för bearbetning av personuppgifter, görs en gång*] |  |  |  |  |  |  |  |  |
|  | | | | | | | | |

## Översiktlig beskrivning av personuppgiftsflödet

**Bifoga en schematisk bild över hur personuppgifterna flödar som inkluderar externa mottagare för uppgifterna. Om uppgifter överförs till andra länder ska detta framgå av bilden.**

|  |
| --- |
|  |

## Ny, innovativ eller kontroversiell personuppgiftsbehandling

*Exempel på nya eller kontroversiella behandlingar är innovativ användning eller tillämpning av tekniska eller organisatoriska lösningar som innefattar person-uppgiftsbehandling såsom användning av artificiell intelligens (AI) i hälso- och sjukvården, ansiktsigenkänning och ”internet of things”, det vill säga apparater, maskiner, mätutrustning och fordon som har inbyggd teknik och internet-uppkoppling, men typiskt sett inte ses som datorer.*

*Om det inte finns känd problematik med liknande behandlingar inom Region Skåne så kan exempelvis Integritetsskyddsmyndigheten ha tagit upp kända risker och utmaningar för liknande behandlingar i publikationer eller tillsynsbeslut.*

*i*

**Finns det känd problematik med liknande personuppgiftsbehandlingar? Kan personuppgiftsbehandlingen anses vara ny, innovativ eller kontroversiell på något sätt?**

|  |
| --- |
|  |

## Behandlingens omfattning

I detta avsnitt beskrivs behandlingens omfattning genom att specificera vilka typer av personuppgifter som behandlas, hur många registrerade som påverkas av personuppgiftsbehandlingen, hur många personuppgifter som behandlas samt vilken geografisk räckvidd personuppgiftsbehandlingen har*.*

### Känsliga personuppgifter

**Utgå från svaren i avsnitt 3.1 och sammanfatta vilka känsliga personuppgifter (art. 9 DSF) eller andra integritetskänsliga eller särskilt skyddsvärda personuppgifter (art. 10 och 87 DSF) som behandlas.[[4]](#footnote-5)**

|  |
| --- |
|  |

### Mängd registrerade

**Uppskatta hur många registrerade som kommer att påverkas av personuppgiftsbehandlingen.**

|  |
| --- |
|  |

### Mängd personuppgifter

*För att räkna ut mängd personuppgifter kan man överslagsräkna genom att ta mängden registrerade som uppskattas bli påverkade av behandlingen gånger hur många olika typer av personuppgifter som behandlas.*

*i*

**Ange hur många personuppgifter som uppskattningsvis kommer att behandlas.**

|  |
| --- |
|  |

### Behandlingens geografiska räckvidd

*Med geografisk räckvidd avses om de registrerade vars personuppgifter behandlas exempelvis bara finns i en avgränsad del av Skåne, hela Skåne, andra delar av Sverige eller i andra länder.*

*i*

**Beskriv personuppgiftbehandlingens geografiska räckvidd.**

|  |
| --- |
|  |

### Nödvändiga informationstillgångar

**Specificera de informationstillgångar som är nödvändiga för att personuppgiftsbehandlingen ska gå att genomföra**.

*Exempel på informationstillgångar är maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper. Om en informations-klassificering har genomförts kan nödvändiga informationstillgångar ha dokumenterats i samband med denna.*

*i*

|  |
| --- |
|  |

## Uppförandekoder

*Olika branscher kommer att kunna ta fram särskilda uppförandekoder för personuppgiftsbehandling. Ännu finns dock inga sådana uppförandekoder.*

*i*

**Ange om behandlingen är ansluten till en av Integritetsskyddsmyndighetens godkända uppförandekoder som reglerar personuppgiftsbehandlingen.**

|  |
| --- |
|  |

## Den registrerades kontroll över sina personuppgifter

**Beskriv hur mycket och på vilket sätt den registrerade kommer ha kontroll över sina personuppgifter.**

*Med kontroll avses om den registrerade själv kan påverka hur och om personuppgifterna behandlas. Exempelvis har den registrerade kontroll om hen själv kan återkalla ett samtycke genom digitala funktioner som finns tillgängliga för den registrerade, eller om hen själv kan ladda ner alla sina personuppgifter från den personuppgiftsansvarige i ett strukturerat, elektroniskt format.*

*i*

|  |
| --- |
|  |

# Uppfyllnad av grundläggande dataskyddsprinciper

I detta avsnitt dokumenteras hur de grundläggande dataskyddsprinciperna (art. 5 DSF) uppfylls.

## Laglighet

*Region Skåne utför i sin roll som myndighet uppgifter av allmänt intresse och det är därför primärt denna rättsliga grund samt att fullgöra en rättslig förpliktelse som regionen baserar sin behandling av personuppgifter på.*

*Om uppgift av allmänt intresse är valt, hänvisa till vilket lagrum som avses, exempelvis kommunallag (2017:725) eller hälso- och sjukvårdslag (2017:30). Om rättslig förpliktelse är valt, ange vilken lag som avses, exempelvis patientdatalag (2008:355). Om samtycke är valt, motivera på vilket sätt samtycket uppfyller kraven i DSF (exempelvis genom att bifoga en kopia av samtyckesblanketten). För avtal, hänvisa till avtal med namn och diarienummer.*

*En verksamhetsrepresentant bör alltid delta i laglighetsbedömningen. Vid osäkerhet om vilken rättslig grund som är tillämplig för de aktuella behandlingarna, kontakta en dataskyddssamordnare eller en regionjurist.*

*i*

**Ange vilken rättslig grund som behandlingen stödjer sig på (art. 6 DSF).[[5]](#footnote-6) Förekommer flera behandlingar med olika rättsliga grunder behöver det framgå tydligt vilken rättslig grund som gäller för respektive personuppgiftsbehandling.**

**Om känsliga personuppgifter (art. 9 DSF) behandlas, ange vilket undantag som möjliggör behandlingen (art. 9.2 DSF).**

|  |  |  |  |
| --- | --- | --- | --- |
| Personuppgifts-behandling | Rättslig grund | Motivering | Undantag som möjliggör behandling av känsliga personuppgifter |
|  | Klicka här: Välj en rättslig grund från rullgardinslistan |  | Klicka här: Välj undantag från rullgardinslistan |
|  | Klicka här: Välj en rättslig grund från rullgardinslistan |  | Klicka här: Välj undantag från rullgardinslistan |
|  | Klicka här: Välj en rättslig grund från rullgardinslistan |  | Klicka här: Välj undantag från rullgardinslistan |
|  | | | |

## Ändamål

### Andra lämpliga sätt att uppnå ändamålet

*Med annat lämpligt sätt avses om det finns andra, mindre riskfyllda sätt att uppnå ändamålet med personuppgiftsbehandlingen. Det kan till exempel finnas andra tekniska lösningar, möjlighet att använda andra, färre eller mindre känsliga uppgifter, anonyma och aggregerade data och så vidare.*

*Denna fråga besvaras lämpligen av projektledaren med stöd av beställaren av tjänsten och en verksamhetsrepresentant.*

*i*

**Ange om det finns något annat lämpligt sätt än den planerade personuppgifts-behandlingen för att uppnå samma ändamål.**

|  |
| --- |
| [*Man hade kunnat använda AI som beslutsstöd med krav på granskning och signering av ansvarig i stället för automatiserat beslutsfattande.*]  [*Drift och support av den föreslagna lösningen hade kunnat tillhandahållas inom EU/EES i stället för i Indien.*] |

### Nödvändighet

**Om behandlingen bygger på en annan rättslig grund än samtycke, beskriv varför den planerade behandlingen är nödvändig för att uppnå ändamålet samt varför man valt detta sätt att uppnå ändamålet snarare än något av de andra lämpliga sätten som beskrivits i 4.2.1.**

**Om den planerade behandlingen bygger på den rättsliga grunden samtycke, beskriv varför den planerade personuppgiftsbehandlingen har valts samt varför man valt detta sätt att uppnå ändamålet snarare än något av de andra lämpliga sätten som beskrivits i 4.2.1.**

|  |
| --- |
|  |

### Ändamålsglidning

**Beskriv hur ändamålsglidning motverkas.**

*Ändamålsglidning är att uppgifterna behandlas för ett specifikt ändamål men att man sedan börjar behandla dem för ett annat, otillåtet ändamål. Exempelvis att ett system upphandlas för att behandla personuppgifter för ett visst syfte, men att personuppgifterna utan analys och bedömning börjar användas för andra ändamål eftersom det är tekniskt möjligt i systemet.*

*i*

|  |
| --- |
| [*Genom beslutade organisatoriska åtgärder för vilka ändamål personuppgifterna får behandlas för*.]  [*Genom instruktioner för hur personuppgifterna får användas.*]  [*Genom tekniska begränsningar av hur personuppgifterna kan användas i it-systemet.*] |

## Uppgiftsminimering

**Redogör för både tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna är adekvata, relevanta och inte för omfattande i förhållande till det specificerade ändamålet.**

*Endast personuppgifter som är nödvändiga för ändamålet får behandlas. Ett exempel på uppgiftsminimering är att inte ”för säkerhets skull” även samla in personnummer när endast namn och födelsedatum behövs för att uppnå ändamålet.*

*i*

|  |
| --- |
| [*Tagit bort fritextfält från formuläret.*]  [*Inkluderat principen om uppgiftsminimering i utbildning för personal som ska inhämta personuppgifter.*] |

## Lagringsminimering

*Personuppgifter får inte sparas längre än vad som behövs för att uppnå ändamålen med behandlingen. När ändamålen som angetts i avsnitt 3.1 har uppnåtts ska gallring eller avidentifiering alltid övervägas om personuppgifterna inte ska arkiveras eller behövs för forskning eller statistik.*

*Se till att all lagring av personuppgifter, inklusive mellanlagring eller tillfällig lagring, tas höjd för när denna fråga besvaras.*

*Eftersom leverantörer ofta har standardinställningar för hur länge information sparas behöver Region Skåne i egenskap av personuppgiftsansvarig göra ett aktivt val och informera leverantörer om vilka lagringstider som är aktuella.*

*En arkivansvarig eller enheten för informationsstyrning kan vara behjälplig vid utredning av lämpliga lagringstider.*

*i*

**Ange hur det tekniskt och organisatoriskt säkerställs att personuppgifter endast lagras så länge de behövs.[[6]](#footnote-7)**

|  |
| --- |
|  |

# Åtgärder som stärker den registrerades rättigheter

I detta avsnitt ska effektiva åtgärder som vidtagits för att stärka den registrerades rättigheter dokumenteras (art. 12–23 och art. 34 DSF). Åtgärderna kan vara organisatoriska, som framtagande av en rutin för handläggning och att utse ansvariga, och tekniska, t. ex. att alla personuppgifter i ett system går att utsöka. För att åtgärderna ska kunna anses vara effektiva ska de utgå från behandlingen och dess ändamål (art. 35.7 b DSF).

## Information till den registrerade (art. 12, 13 och 14 DSF)

**Beskriv hur information om personuppgiftsbehandlingen utformats och kommer att lämnas till den registrerade.**

*Informationen till den registrerade ska uppfylla de krav som ställs i dataskydds-förordningen. Mer information och vägledning om hur informationskravet kan uppfyllas finns på Region Skånes intranät på sidan ”Informera om personuppgiftsbehandling” samt i anvisningen med samma namn.*

*i*

|  |
| --- |
|  |

## Rätt till tillgång (registerutdrag) (art. 15 DSF)

**Beskriv hur den registrerades rätt till tillgång (registerutdrag) säkerställs.**

*Det behöver både finnas teknisk möjlighet att tillgodose rätten till tillgång och en rutin för hur en begäran ska handläggas.*

*i*

|  |
| --- |
| [*Alla personuppgifter som tillhör nu levande personer går att utsöka.*]  [*Det är säkerställt att Journal- och arkivservice inkluderar systemet när de begär registerutdrag från verksamheten.*]  [*Det finns teknisk möjlighet att exportera personuppgifterna som tillhör den registrerade.*]  [*Det finns rutiner för hur export av personuppgifter ska ske samt tilldelat ansvar för hur dessa rutiner ska utföras.*] |

## Rätt till dataportabilitet (art. 20 DSF)

*Rätten till dataportabilitet är endast aktuell för personuppgifter som har lämnats av den registrerade själv och som behandlas med stöd av samtycke eller för att uppfylla ett avtal med den registrerade.*

*i*

**Om applicerbart, ange hur den registrerades rätt till dataportabilitet säkerställs.**

|  |
| --- |
|  |

## Rätt till rättelse (art. 16 och 19 DSF)

*Felaktiga eller ofullständiga personuppgifter ska gå att rätta eller komplettera. Vissa registerlagstiftningar reglerar hur denna rättighet ska tillämpas. Personuppgifter som behandlas i enlighet med patientdatalagen (2008:355) får till exempel endast justeras under vissa förutsättningar. Det innebär att en tjänsteanteckning kan behöva göras i stället för en rättelse om personuppgifterna förekommer i en allmän handling.*

*i*

**Ange hur den registrerades rätt till rättelse säkerställs.**

|  |
| --- |
|  |

## Rätt till radering (art. 17 och 19 DSF)

*Region Skåne har en rättslig skyldighet att registrera och bevara allmänna handlingar i enlighet bestämmelserna i offentlighets- och sekretesslagen (2009:400) och arkivlagen (1990:782). Rätten till radering är därför inte aktuell för personuppgifter i handlingar som inkommit till, upprättats vid, och/eller finns förvarade hos Region Skåne eftersom dessa utgör allmänna handlingar vid myndigheten.*

*i*

**I de fall den är tillämplig, ange hur den registrerades rätt till radering säkerställs samt hur det säkerställs att personuppgifterna som raderas inte går att återskapa.**

|  |
| --- |
|  |

## Rätt att göra invändningar och rätt till begränsning av personuppgiftsbehandling (art. 18, 19 och 21 DSF)

*Den registrerade har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas, exempelvis när hen begär rättelse och vill att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds. Exempel på begränsning är att tillfälligt flytta uppgifterna till en annan plats, att göra uppgifterna otillgängliga för användare eller att tillfälligt avpublicera dem om de till exempel publicerats på en hemsida. Uppgifterna ska sitta i ”karantän” och får inte ändras medan begränsningen är aktiv.*

*i*

**Ange hur den registrerades rätt att göra invändningar och rätt till begränsning av personuppgiftsbehandlingen säkerställs.**

|  |
| --- |
|  |

## Tredjelandsöverföring (kap. 5 DSF)

*Med tredjeland avses ett land utanför EU/EES. Begreppet ”överföring” som det definieras i dataskyddsförordningen innefattar all form av åtkomst till personuppgifter. Även överföringar av Region Skånes uppgifter utanför EU/EES som görs av Region Skånes personuppgiftsbiträden och deras underbiträden är tredjelandsöverföringar som vi ansvarar för eftersom det är våra uppgifter som överförs.*

*Ett exempel på överföring till tredjeland är att ett av Region Skånes personuppgiftsbiträden inom EU/EES har anlitat ett underbiträde i Indien som sköter Region Skånes supportärenden och i samband med detta ges åtkomst till personuppgifter i klartext.*

*Vid tredjelandsöverföring måste den personuppgiftsansvarige (Region Skåne) säkerställa att rätt, rättspraxis och administrativa metoder/rutiner hos myndigheter och domstolar i mottagarlandet möjliggör en väsentligen likvärdig skyddsnivå med den som garanteras inom EU.*

*i*

|  |  |  |
| --- | --- | --- |
|  | Ja | Nej |
| Överförs personuppgifter till tredjeland i samband med behandlingen? |  |  |

### Beskrivning och skyddsåtgärder

**Om personuppgifter överförs till tredjeland, beskriv vilka tredjelandsöverföringar som görs i och med behandlingen.**

**Ange även vilka överföringsmekanismer (land med adekvat skyddsnivå eller lämpliga skyddsåtgärder) som har använts för tredjelandsöverföringarna samt motivera varför dessa mekanismer är tillämpliga.**

|  |  |  |  |
| --- | --- | --- | --- |
| Personuppgifts-behandling | Beskrivning av tredjelandsöverföring | Överförings-mekanism | Motivering av skyddsåtgärd(er) och tillämplighet[[7]](#footnote-8) |
| [*Support*] | [*Överförs till Storbritannien* *i* *samband med skärmdelning vid supportärenden*] | [*Standard-avtalsklausuler*] | [*Motivera utifrån bland annat tredjelandets lagstiftning/skydd för personuppgifter.*] |
|  |  |  |  |
|  |  |  |  |
|  | | | |

## Medverkan från berörda parter

### Synpunkter från registrerade

*När så är lämpligt ska synpunkter inhämtas från de registrerade eller deras företrädare (art. 35.9 DSF).*

*i*

**Har ni rådgjort med registrerade eller deras företrädare? Om ja: Redogör för dessa synpunkter. Om nej: Motivera varför ni bedömer att det inte är lämpligt att inhämta eller följa synpunkter från de registrerade.**

|  |
| --- |
|  |

### BIträden, specialister etc.

*Om utlåtanden från relevanta intressenter finns i annan bifogad dokumentation såsom en riskbedömning kan man hänvisa dit.*

*i*

**Redogör för synpunkter från relevanta intressenter, exempelvis personuppgiftsbiträden eller informationssäkerhetsspecialister.**

|  |
| --- |
|  |

# Risker och mitigerande åtgärder

Målet med en konsekvensbedömning avseende dataskydd är att minimera risker för den registrerades rättigheter och friheter (art. 35.7 c DSF). För att möjliggöra detta ska en riskbedömning där man hanterar risker för kränkningar av den registrerades rättigheter och friheter genomföras i samband med konsekvensbedömningen, det vill säga informationssäkerhetsrisker som kan resultera i negativa konsekvenser för enskilda individer. Konsekvenserna kan vara av materiell, fysisk eller psykisk karaktär.

Endast risker för den registrerade ska vara i fokus under riskbedömningsdelen av konsekvensbedömningen eftersom det bara är den registrerades perspektiv som är av relevans i en konsekvensbedömning. Risker ur ett bredare perspektiv, såsom risker för Region Skåne som organisation, hanteras i stället i en riskbedömning avseende informationssäkerhet.[[8]](#footnote-9)

Riskbedömningsdelen av en konsekvensbedömning ska innehålla[[9]](#footnote-10):

* Riskens ursprung (orsak/sårbarhet) (skäl 90 DSF).
* Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av personuppgifter (personuppgiftsincidenter).
* Identifiering av möjliga konsekvenser för den registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
* Uppskattning av sannolikhetsgrad och konsekvensgrad (värdering av risker) (skäl 90 DSF).
* Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d DSF och skäl 90 DSF)

Riskbedömningsdelen av en konsekvensbedömning kan av praktiska skäl genomföras samtidigt som en riskbedömning avseende informationssäkerhet. Dokumentationen görs i Region Skånes riskhanteringsverktyg.[[10]](#footnote-11) Det är dock viktigt att värdera och dokumentera de risker som tillhör konsekvensbedömningen separat. Detta för att konsekvensbedömnings-riskerna endast ska bestå av risker för den registrerade och inte Region Skåne som organisation.

Tillsammans utgör en komplett ifylld mall för konsekvensbedömning samt tillhörande riskhanteringsdokument en komplett konsekvensbedömning.

## Riskdokumentation

**Hänvisa till aktuellt riskbedömningsdokument (diarienummer eller motsvarande beständigt referensnummer) eller bifoga riskerna och de mitigerande åtgärderna i sin helhet till detta dokument.**

|  |
| --- |
|  |

## Kvarstående höga risker

**Dokumentera de risker från riskbedömningsdelen av konsekvensbedömningen som är fortsatt höga (riskvärde 8 eller högre) efter att mitigerande åtgärder har vidtagits.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Riskscenario (hot, aktör och konsekvenser) | Riskens ursprung (sårbarhet, orsak) | | Vidtagna åtgärder | | Sannolikhets-värde efter åtgärder (1–4) | Konsekvens-värde efter åtgärder (1–4) | Riskvärde efter åtgärder (1–16) |
|  | [*Intern obehörig åtkomst vilket resulterar i att den registrerades personuppgifter röjs för en stor mängd obehöriga.*] | [*För bred behörighetstilldelning. Incidenter har redan inträffat och dessutom är det möjligt att nya sådana inträffar p.g.a. systemets utformning.*] | | [\**Översyn av behörighetsstrukturen i systemet* \**Logguppföljning*] | | [*3*] | [*3*] | [*9*] |
|  |  |  | |  | |  |  |  |
|  |  | |  | |  | | | |

# Rådfrågan och granskning

## Dataskyddssamordnarens utlåtande

Vid behov kan dataskyddssamordnaren som rådfrågats i denna ruta ge ett samlat utlåtande om konsekvensbedömningen. Rutan får endast fyllas i av dataskyddssamordnaren.

|  |
| --- |
|  |

## Rådfrågan av dataskyddsombud

Om krav på en konsekvensbedömning föreligger enligt avsnitt 2 i denna mall (om det sannolikt föreligger en hög risk för den registrerades rättigheter och friheter) ska Region Skånes dataskyddsombud rådfrågas om konsekvensbedömningen (art. 35.2 DSF), vilket ska dokumenteras i denna ruta. Rutan får endast fyllas i av dataskyddsombudet.

|  |
| --- |
|  |

1. Kontaktuppgifter till Region Skånes dataskyddssamordnare: <https://intra.skane.se/hemvister/informationsstyrning/djupa-textsidor/dataskydd/kontaktuppgifter> [↑](#footnote-ref-2)
2. Kriterierna definieras i dataskyddsförordningen art. 35.3. [↑](#footnote-ref-3)
3. Kontrollfrågorna utgår från Integritetsskyddsmyndighetens publicerade lista över när konsekvensbedömningar behöver göras: <https://www.imy.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/forteckning-konsekvensbedomning/> [↑](#footnote-ref-4)
4. I art. 9 DSF definieras känsliga personuppgifter som följande: ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

   Med integritetskänsliga och särskilt skyddsvärda personuppgifter avses bland annat personnummer eller andra nationella identifikationsnummer, uppgifter om lagöverträdelser och uppgifter om någons privatliv. [↑](#footnote-ref-5)
5. Vägledning om de rättsliga grunderna finns i *Instruktion för Region Skånes behandling av personuppgifter* och på IMY:s webbplats: <https://www.imy.se/lagar--regler/dataskyddsforordningen/rattslig-grund/> [↑](#footnote-ref-6)
6. Regelverk för bevarande och gallring inom Region Skåne finns på Vårdgivare Skåne: <https://vardgivare.skane.se/uppdrag-avtal/arkiv-och-informationshantering/#50287> [↑](#footnote-ref-7)
7. Se EDPB:s vägledning för val och bedömning av skyddsåtgärder för att uppnå lagenlig tredjelandsöverföring: <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en> [↑](#footnote-ref-8)
8. Mer information om riskbedömningar avseende informationssäkerhet: <https://intra.skane.se/sidor/min-forvaltning-region-skane/katastrof-sakerhet/sakerhet/informationssakerhet/riskanalys-informationssakerhet> [↑](#footnote-ref-9)
9. Se den franska dataskyddsmyndigheten CNIL:s vägledning för stöd i riskbedömningen:

   <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> [↑](#footnote-ref-10)
10. <https://intra.skane.se/sidor/min-forvaltning-region-skane/katastrof-sakerhet/sakerhet/informationssakerhet/riskanalys-informationssakerhet> [↑](#footnote-ref-11)