Göteborgs Stad

Mallstöd konsekvensbedömning

Stöd i genomförande av konsekvensbedömning enligt dataskyddsförordningen

2022-08-31

Dataskyddsenhetens förord

Hej, ni som ska genomföra en konsekvensbedömning enligt GDPR har ett viktigt arbete framför er!

Eftersom ni har öppnat detta dokument har ni kommit fram till att den eller de behandlingar som ni ska påbörja eller förändra innebär en hög risk för de personer vars personuppgifter ni kommer att behandla. Kanske har ni kommit fram till detta genom att genomföra en så kallad tröskelanalys (se till exempel dataskyddsenhetens mall och mallstöd för detta). Kanske är behandlingens art, omfattning, sammanhang eller ändamål sådana att det för er har varit uppenbart att en konsekvensbedömning ska genomföras. Sannolikt har ni också rådgjort med er kontaktperson på dataskyddsenheten om en konsekvensbedömning bör genomföras (i alla fall om ni har för vana att följa Europeiska dataskyddsstyrelsens riktlinjer).

En konsekvensbedömning enligt GDPR är ett slags verktyg eller en systematisk process som hjälper den personuppgiftsansvarige att systematiskt beskriva behandlingen, identifiera och avhjälpa de risker som behandlingen medför för den vars personuppgifter behandlas, samt visa hur den personuppgiftsansvarige efterlever GDPR.

I en konsekvensbedömning är det fokus på den vars personuppgifter behandlas, den så kallade registrerade. I konsekvensbedömningen ska ni utgå ifrån riskerna som behandlingen kan medföra för den registrerade. En behandling kan såklart också innebära andra typer av risker. Det kan exempelvis handla om förtroendeskada eller om ekonomiska förluster för verksamheten på grund av att man påförs en sanktionsavgift för bristande följsamhet mot GDPR. Dessa risker är såklart viktiga för en verksamhet att beakta – men hör inte hemma i en konsekvensbedömning.

Vi på dataskyddsenheten har en viktig roll i ert arbete med konsekvensbedömningen. Den personuppgiftsansvarige har en skyldighet att rådfråga dataskyddsombudet vid en konsekvensbedömning och på förfrågan ska vi ge råd och övervaka ert konsekvensbedömningsarbete. Utöver detta, för att möta ett uppkommet behov och önskemål från flera verksamheter, har dataskyddsenheten tagit fram mallar för konsekvensbedömning och tröskelanalys tillsammans med mallstöd. Genom detta får ni som ska genomföra detta arbete såväl kunskap som praktiskt stöd i hur mallen fylls i, samt exempel på hur ni kan skriva.

Vi hoppas att detta ska underlätta ert arbete och vi ser fram emot att delta i ert konsekvensbedömningsarbete!

Förkortningar och vad de betyder

DSE: dataskyddsenheten

GDPR: dataskyddsförordningen/General Data Protection Regulation

IMY: Integritetsskyddsmyndigheten

PUA: personuppgiftsansvarig

PUB: personuppgiftsbiträde

PUB-avtal: personuppgiftsbiträdesavtal

Detta mallstöd utgör ett komplement till mallen ”Konsekvensbedömning enligt dataskyddsförordningen” och innehåller information om vad ni ska skriva var och hur det kan skrivas.

Varje avsnitt har ett motsvarande avsnitt i mallen. Om ni t.ex. vill ha information om hur ni fyller i avsnitt 1.1 Bakgrund och behov av behandlingen/behandlingarna i mallen går ni till avsnitt 1.1 i mallstödet.

Versionshantering

Datum	Version	Beskrivning	Ändrat av
20220429	0.1		Dataskyddsenheten
20220610	0.2	Ändringar efter inkomna synpunkter från arbetsgrupp	Dataskyddsenheten
20220831	1	Ändringar efter inkomna synpunkter från dataskyddskontakter m.fl.	Dataskyddsenheten

Innehåll

Versionshantering

Konsekvensbedömningsmallen inleds med en ruta för versionshantering. En konsekvensbedömning ska enligt GDPR vara ett ”levande dokument” och något som alltså uppdateras i takt med att behandlingen eller kunskapen om behandlingen förändras. För att göra det tydligt i vilket skede som konsekvensbedömningsarbetet befinner sig i, vilka ändringar som är gjorda och vem som har gjort dem rekommenderas verksamheterna att arbeta aktivt med att fylla i versionshanteringen. Detta underlättar också i samspelet mellan verksamheten och dataskyddsombudet eftersom det gör det enkelt att följa vilken version som dataskyddsombudet har fått kommentera och lämna rekommendationer på. Dataskyddsenheten rekommenderar Stadens förvaltningar och bolag att vid lämpliga tillfällen eller med jämna mellanrum (om arbetet med konsekvensbedömningen är konstant och pågående) fastställa versioner av konsekvensbedömningen och diarieföra underlaget.

Hur ni fyller i mallen

Datum	Version	Beskrivning	Ändrat av
20220227	0.1	Utkast upprättat	XX och YY
20220401	0.1	Utkast avstämt med handläggare på enhet Z	XX, YY och ZZ
20220515	0.1	Utkast granskat av DSO NN	YY
20220531	0.1	Ändringar gjorda i enlighet med kommentarer/rekommendationer från DSO	XX och YY
20220531	1	Version fastställd och diarieförd	XX

1 Inledning

1.1 Bakgrund och behov av behandlingen/behandlingarna

Hur ni fyller i mallen

I denna inledande del ska ni beskriva bakgrunden och ge kontext kring den behandling/de behandlingar som ni planerar att införa eller förändra. Syftet är att ge läsaren, som kan vara allt från en beslutande chef till tillsynsmyndigheten, möjlighet att förstå vad som har lett fram till det ni nu vill göra.

Exempel

- ✓ A-förvaltningen har genom A-nämndens reglemente fått uppgiften att samordna stadens arbete med X-bidrag. Detta innebär att A-förvaltningen kommer att behöva behandla personuppgifter tillhörande de som ansöker om X-bidraget.
- ✓ En ny lag innebär att alla arbetsgivare med över 50 anställda behöver inrätta ett visselblåsarsystem. Detta medför ett antal nya och förändrade personuppgiftsbehandlingar hos B-bolaget.
- ✓ C-förvaltningen har från kommunfullmäktige fått i uppdrag att rapportera in statistik om Y. Förvaltning C arbetar redan med att ta fram statistik om X och Z, men att ta fram statistik om Y är nytt och förvaltningen C bedömer att det innebär en ny personuppgiftsbehandling.

Exemplen i detta mallstöd är menade att ge vägledning till er som fyller i mallen för konsekvensbedömning. De ska inte kopieras rakt av utan måste alltid anpassas till omständigheterna i era specifika behandlingar.

1.2 Behov av konsekvensbedömning

Det är endast om en personuppgiftsbehandling sannolikt leder till en hög risk för registrerades friheter och rättigheter som en konsekvensbedömning behöver göras. I vissa fall kan det nästan vara uppenbart att en behandling innebär en hög risk och i vissa fall kan det vara mer oklart.

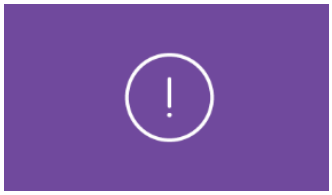
I artikel 35 GDPR finns det angivet tre situationer när en konsekvensbedömning alltid ska göras, nämligen:

1. Om behandlingen innefattar systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk

behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.
2. Om det kommer att ske personuppgiftsbehandling i stor omfattning av särskilda kategorier av uppgifter (känsliga personuppgifter, se artikel 9 GDPR) eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10 GDPR.
3. Om behandlingen innebär systematisk övervakning av en allmän plats i stor omfattning.

Utöver ovanstående tre situationer finns det även andra situationer som kan innebära att en konsekvensbedömning behöver genomföras. Nedanstående förteckning kommer från tillsynsmyndigheten och om er behandling passar in på **två eller fler** av dessa ska en konsekvensbedömning genomföras.

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



Obs! Även om er behandling bara passar in på en eller ingen av ovanstående punkter kan det finnas skäl att göra en konsekvensbedömning. Detta är dock mycket ovanligt. Glöm inte att rådfråga ert dataskyddsombud om ni är osäkra!

En behandling kan även uppfylla två eller flera av kriterier i förteckningen men den personuppgiftsansvarige kan ändå göra bedömningen att den ”sannolikt inte leder till en hög risk”. Detta bör vara aktuellt endast i absoluta undantagsfall. I sådana situationer bör den personuppgiftsansvarige motivera och dokumentera anledningarna till att en konsekvensbedömning inte utförs och inkludera dataskyddsombudets synpunkter.

I många fall är det hjälpsamt att göra en så kallad tröskelanalys för att bedöma behovet av en konsekvensbedömning. Detta är inget krav enligt GDPR men kan vara ett tydligt sätt att dokumentera sin bedömning på.

Dataskyddsenheten har tagit fram en mall och ett mallstöd även för tröskelanalys.

Hur ni fyller i mallen

Om en tröskelanalys har gjorts – hänvisa till aktuellt dokument (med angivet diarienummer om detta finns).

Om en tröskelanalys inte har gjorts, ange varför det finns behov av en konsekvensbedömning. Beskriv detta i fritext och hänvisa till de punkter som är relevanta i artikel 35 GDPR eller aktuella punkter i IMY:s förteckning.

Exempel

- ✓ Bedömning av om behov av konsekvensbedömning gjord i tröskelanalys, se underlag med diarienummer X123/22
- ✓ Eftersom den aktuella behandlingen behandlar hälsouppgifter som är en känslig personuppgift, samt behandlar personuppgifter tillhörande anställda, uppfyller behandlingen två kriterier från tillsynsmyndighetens förteckning. Behandlingen innebär alltså sannolikt en hög risk för registrerades friheter och rättigheter, varför en konsekvensbedömning behöver genomföras.
- ✓ Behandlingarna som bolaget B ska påbörja innebär en behandling av anställdas personuppgifter, inklusive personnummer och underlag från bedömningssamtal. Behandlingen omfattar ca 950 anställda. Behandlingen innefattar visserligen inga känsliga personuppgifter, men likväl extra skyddsvärda. Det rör också ett relativt stort antal registrerade. Bolaget B väljer att iaktta försiktighetsprincipen och beslutar därför att genomföra en konsekvensbedömning.

1.3 Deltagare och roller

Hur ni fyller i mallen

I detta avsnitt ska ni ange vilka personer som har deltagit i arbetet med konsekvensbedömningen och vilken roll som de har haft. Syftet med detta är att säkerställa att det finns en spårbarhet i arbetet och göra det möjligt att t.ex. i efterhand kontakta de personer som varit involverade om det uppstår frågor eller om konsekvensbedömningen behöver kompletteras. Tänk på att det är viktigt att samla rätt kompetenser i arbetet – såväl de som har kunskaper i dataskydd som de som har kunskaper om den praktiska verksamheten.

Exempel

- ✓ Ashkan Andersson, arkivare och dataskyddskontakt
- ✓ Berta Bertilsson, IT
- ✓ Christina Cadiz, systemförvaltare
- ✓ Daarun Davidsson, handläggare

1.4 Personuppgiftsansvar

Personuppgiftsansvarig är den som bestämmer för vilka ändamål som uppgifterna ska behandlas och hur behandlingen ska gå till. Om det är flera aktörer som kommer att behandla personuppgifterna behöver det utredas vem eller vilka som bestämmer över behandlingen. Vid en sådan utredning är det nödvändigt att identifiera de faktiska aktiviteterna och aktörernas förhållanden till varandra vid en behandling.

Genom att fastställa ansvaret mellan aktörerna klargörs det om det föreligger ett självständigt personuppgiftsansvar, ett gemensamt personuppgiftsansvar eller ett ansvar som personuppgiftsbiträde. Då kan även förhållandena mellan aktörerna regleras och dokumenteras, exempelvis genom ett datadelningsavtal eller ett personuppgiftsbiträdesavtal.

Vem som är personuppgiftsansvarig anges också i vissa fall i lag eller förordning, till exempel i särskilda registerlagar.

Gemensamt personuppgiftsansvar

Det huvudsakliga kriteriet för att ett gemensamt personuppgiftsansvar ska föreligga är att två eller flera parter gemensamt deltar i besluten om ändamål och medel för personuppgiftsbehandlingen. Kravet på gemensamt beslutande om ändamål och medel innebär dock inte att förvaltningarna måste ha lika stor inverkan på besluten om ändamålen och medel för behandlingen. Saknas koppling helt till ändamål och medel uppstår inte ett gemensamt ansvar.

Om personuppgiftsansvaret är gemensamt för en eller flera behandlingar ställer GDPR krav på de personuppgiftsansvariga att ingå ett ”inbördes arrangemang”. Kraven på ett inbördes arrangemang kan uppfyllas genom att ingå ett datadelningsavtal alternativt en överenskommelse om datadelning.

Bestämmelser om gemensamt personuppgiftsansvariga finns i artikel 26 GDPR.

Självständigt personuppgiftsansvar

När flera aktörer behandlar samma personuppgifter var och en för egna ändamål och utan att det finns ett nära samband mellan dessa ändamål handlar det normalt om självständiga personuppgiftsansvariga.

Om en självständig personuppgiftsansvarig avser att dela med sig av uppgifter till en annan part så rör det sig om ett utlämnande av personuppgifter. Det finns inte något krav i GDPR på att den här typen av situation behöver regleras i ett avtal.

Personuppgiftsbiträde

Om en aktör behandlar personuppgifter utan att ha något inflytande på ändamålet med behandlingen kan det röra sig om en biträdesrelation där aktören är personuppgiftsbiträde. Den personuppgiftsansvariga ger alltså i uppdrag till en annan aktör att behandla personuppgifter för sin räkning. Det kan till exempel röra sig om att en personuppgiftsansvarig inte har möjlighet att lagra data i någon större utsträckning ock köper därför en lagringstjänst i form av servrar från en IT-leverantör. Om aktuell data innehåller personuppgifter blir IT-leverantören personuppgiftsbiträde eftersom lagring räknas som en personuppgiftsbehandling. Ett annat exempel kan vara att en personuppgiftsansvarig köper in ett HR-system där leverantören bl.a. står för supporten. I och med att leverantören genom att ge support till personuppgiftsansvariga behandlar den personuppgiftsansvariges personuppgifter blir leverantören personuppgiftsbiträde.

Om en behandling innebär att en aktör behandlar personuppgifter för den personuppgiftsansvariges räkning måste den personuppgiftsansvarige och personuppgiftsbiträdet ingå ett personuppgiftsbiträdesavtal.

Bestämmelser om personuppgiftsbiträden finns i artikel 28 GDPR.

Hur ni fyller i mallen

I konsekvensbedömningen ska ni redogöra för vem som är personuppgiftsansvarig för behandlingen/behandlingarna. Om ni är flera aktörer som bestämmer ändamål och medel för behandlingen så behöver ni ange om personuppgiftsansvaret är gemensamt eller självständigt. Uppge också om detta gäller för hela behandlingen eller endast för delar av behandlingen.

Om en aktör i stället är personuppgiftsbiträde så ska detta anges under punkt 2.1.2 i konsekvensbedömningen.

Exempel

- ✓ Bolaget är personuppgiftsansvarig för den planerade behandlingen.
- ✓ Förvaltning A och förvaltning B är gemensamt personuppgiftsansvariga för hela den aktuella behandlingen. Förvaltningarna har reglerat

överföringen av personuppgifter i en överenskommelse om datadelning, diarienummer 12–34.

- ✓ Förvaltning C och förvaltning D är självständigt personuppgiftsansvariga för den del av behandlingen som avser utvärdering. I övriga delar av behandlingen är förvaltningarna gemensamt personuppgiftsansvariga och överföringen av personuppgifter i dessa delar har reglerats i en överenskommelse om datadelning, diarienummer 56–78.

2 Beskrivning av behandlingen/ behandlingarna

2.1 Översiktlig beskrivning av behandlingen/behandlingarna

En konsekvensbedömning ska innehålla en beskrivning av behandlingen (eller de behandlingar) som ingår. Detta är en viktig del av en konsekvensbedömning eftersom det är här ni redogör för hur behandlingen i sin helhet kommer att gå till. Utan en övergripande beskrivning av behandlingen är det svårt att pussla ihop de resterande delarna till en komplett bild. Det kan nog upplevas som att ni här beskriver delar som ni ändå kommer att behöva beskriva i efterföljande avsnitt men det är som sagt viktigt att få en ”ax till limpa”-beskrivning. En pedagogisk beskrivning i denna del visar också att ni själva är medvetna om och pålästa i det som ni kommer att göra. Glöm inte att tydligt skriva ut hur länge ni behandlar och sparar personuppgifterna.

För att tydligt illustrera personuppgifternas livscykel (var de kommer ifrån och var de sedan tar vägen) kan det vara bra att ha med ett flödesschema som illustrerar detta.

En konsekvensbedömning ska göras utifrån behandlingar, inte per system. En konsekvensbedömning kan innehålla en enda behandling eller en serie liknande behandlingar. Med detta menas personuppgiftsbehandlingar som liknar varandra och som alltså har gemensamma nämnare.

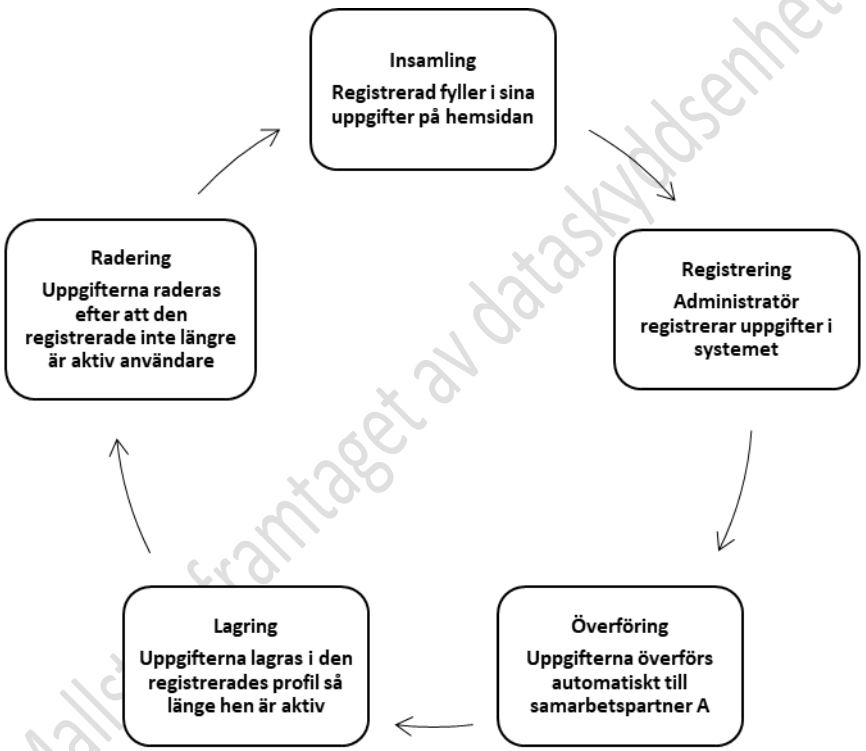
Exempel

- ✓ A-förvaltningen har fått uppdraget att ombesörja ansökningar och utbetalningar av X-bidraget. De registrerade skickar in sina ansökningar via en e-tjänst som tillhandahålls av Företag F AB. A-förvaltningens handläggare administrerar och behandlar de inkomna ansökningarna. Detta sker i systemstöd D hos A-förvaltningen. När handläggningen är klar och beslut om beviljande eller nekande av utbetalning har fattats

skickas beslutet via brev till den sökande. Av kommunfullmäktige har A-förvaltningen också fått uppdraget att föra statistik över X-bidraget. Detta sker genom en integration med system E. Endast antal beviljade och nekade ansökningar registreras och uppgifterna är helt anonymiserade. Det sker alltså ingen personuppgiftsbehandling i system E.

Ansökningarna gallras direkt ur e-tjänsten men finns kvar i systemstöd D. Stödet har en arkivfunktion men är inte ett arkiv. Vissa underlag innehållandes personuppgifter gallras efter x år och vissa ska bevaras. De skickas då till e-arkiv Z.

Nedan finns ett exempel på ett förenklat flödesschema som illustrerar personuppgifternas livscykel.



2.1.1 Tillgångar

En del i beskrivningen av behandlingen är att ange vilka tillgångar som är nödvändiga för personuppgifterna. Det kan exempelvis handla om maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper.

Hur ni fyller i mallen

I konsekvensvensbedömningen ska ni redogöra för vilka tillgångar som är aktuella för er behandling – helt enkelt vilka tillgångar som behövs för att möjliggöra behandlingen. Var tydlig och noggrann – det är lätt att glömma tillgångar som faktiskt behövs för att behandlingen ska vara möjlig.

Exempel

- ✓ **Mindre bra**: Treserva
- ✓ **Bra:** Behandlingen utförs i verksamhetssystemet Treserva. Verksamhetssystemet nås via dator och nätverk med VPN-tunnel. Inloggning kräver behörighet och är kopplat till medarbetarens AD-konto.

2.1.2 Personuppgiftsbiträden och underbiträden

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvarigas räkning. Det är den personuppgiftsansvarige som bestämmer hur behandlingen ska ske genom att ge instruktioner till personuppgiftsbiträdet. Ett personuppgiftsbiträde ska kunna garantera att behandlingen uppfyller kraven i GDPR och även säkerställa att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträde kan i vissa fall anlita ett så kallat personuppgiftsunderbiträde. Underbiträdet behandlar då personuppgifter på uppdrag av personuppgiftsbiträdet. Personuppgiftsbiträdet får inte anlita ett underbiträde utan att på förhand få ett skriftligt tillstånd av den personuppgiftsansvariga.

Bestämmelser om personuppgiftsbiträden finns i artikel 28 GDPR.

Hur ni fyller i mallen

I konsekvensbedömningen ska ni redogöra för om hela eller delar av behandlingen/behandlingarna utförs av ett eller flera personuppgiftsbiträden och/eller underbiträden. Tänk på att ange samtliga personuppgiftsbiträden och underbiträden. Vissa tjänster levereras som slutprodukt via en lång kedja av underleverantörer. Det är därför viktigt att identifiera alla underbiträden och vid behov illustrera hur personuppgifter behandlas/flödar genom ett flödesschema (se punkt 2.1).

Exempel

- ✓ För support av tjänsten anlitar bolag A leverantör B. I supporten behandlas användarnas personuppgifter. Eftersom uppgifterna behandlas å bolag A:s vägnar, blir leverantör B personuppgiftsbiträde.
- ✓ Personuppgiftsbiträdet använder leverantör C som underbiträde för teknisk support.

2.1.3 Mottagare

Med mottagare avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte. En mottagare kan till exempel vara ett personuppgiftsbiträde eller någon annan som får ta del av personuppgifterna.

Eftersom ni redan har angett personuppgiftsbiträde tidigare i mallen så behöver ni här enbart ange andra externa mottagare som får del av uppgifterna.

Mottagare skulle exempelvis kunna vara samarbetspartners, andra förvaltningar/bolag eller en aktör som samlar statistik. Tänk på att delningen av personuppgifter behöver ha en rättslig grund. Se avsnitt 2.5.

Offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare. Till exempel räknas inte Skatteverket som mottagare när personuppgiftsansvariga ska skicka över uppgifter om lön.

Bestämmelse om mottagare finns i artikel 4.9 GDPR.

Hur ni fyller i mallen

Ange samtliga externa mottagare och varför/i vilken kapacitet mottagaren får del av personuppgifterna.

Exempel

- ✓ **Mindre bra:** Ja.
- ✓ **Bra**: Y-skolan delar med sig av personuppgifter till den kulturella samarbetspartnern Z i syfte att eleverna vid skolan ska kunna delta i aktiviteter efter skoltid.
- ✓ **Bra**: A-förvaltningen delar med sig av personuppgifter med tänkbara arbetsgivare eller utbildningsanordnare och andra verksamheter som förvaltningen har avtal med för att på så vis få deltagare i arbetsmarknadsinsatser att komma i egen försörjning.

2.2 Översikt behandling/behandlingar

Som framgår under avsnitt 2.1 kan en konsekvensbedömning innehålla antingen endast en behandling eller en serie liknande behandlingar. Det är inte alltid självklart vad som utgör en behandling och när det ska ses som flera. Om behandlingar har olika ändamål och syften, eller olika rättsliga grunder kan det vara ett tecken på att ni nog har att göra med olika personuppgiftsbehandlingar. Om dessa liknar varandra kan de ändå ingå i samma konsekvensbedömning.

Syftet med detta avsnitt är att ni ska identifiera och namnge den eller de behandlingar som ingår i konsekvensbedömningen och ge er och läsaren en överblick över vilka personuppgifter som ingår i vilka behandlingar.

Vad är en personuppgift?

En personuppgift är varje form av upplysning som direkt eller indirekt kan hänföras till en fysisk levande person. Avgörande är om uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en person.

Vissa typer av personuppgifter är extra skyddsvärda. Exempel på uppgifter som är extra skyddsvärda är personnummer, löneuppgifter, uppgifter om lagöverträdelser och uppgifter om sociala förhållanden.

Det är bra att identifiera om extra skyddsvärda personuppgifter behandlas eftersom dessa uppgifter kan behöva skyddas av en högre säkerhetsnivå än mer ”harmlösa” personuppgifter. Eftersom uppgifterna är mer skyddsvärda kan det även vara av betydelse för bedömningen av risker som ni ska göra i samband med konsekvensbedömningen.

Det finns även personuppgifter som bedöms vara känsliga personuppgifter och dessa har ett starkare skydd i lagstiftningen. Det är uppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person. Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter, men det finns fall då det är tillåtet. (Läs mer om när det är tillåtet att behandla känsliga personuppgifter i avsnitt 2.4.1)

Definitionen av en personuppgift finns i artikel 4.1 GDPR. Bestämmelser om känsliga personuppgifter finns i artikel 9 GDPR.

Hur ni fyller i mallen

I mallen ska ni ange den behandling som konsekvensbedömningen omfattar. Det är detta som menas med ”namn på behandling”. Om konsekvensbedömningen omfattar fler än en behandling ska samtliga namn/behandlingar anges. Tänk också på att det ska vara samma namn på behandlingen som i ert personuppgiftsregister. Detta namn bör också i många fall vara samma som finns i verksamhetens klassificeringsstruktur.

Ni ska också beskriva vilka personuppgifter som hanteras i vilken behandling. Det är viktigt att kartlägga samtliga personuppgifter som behandlas och ange dessa i konsekvensbedömningen. Tänk på att det i vissa fall kan behövas kompletterande information om varför en uppgift är en personuppgift.

Det är även viktigt att ni bedömer om personuppgifterna är extra skyddsvärda eller känsliga och anger detta i konsekvensbedömningen.

Exempel

Namn på behandling	Person-uppgifter	Extra skyddsvärda person-uppgifter	Känsliga person-uppgifter
Bidragsansökan	Namn Hemadress Mobiltelefon-nummer E-postadress Tekniska metadata	Personnummer Löneuppgifter Uppgifter om arbetslöshets-ersättning Kontonummer	Hälsouppgifter Etniskt ursprung

		Familjestatus Uppgifter om närstående	
Behandling av personuppgifter om anställda för löne-administration	Förnamn och efternamn Hemadress E-postadress	Personnummer Löneuppgifter	

2.2.1 Personuppgifter om lagöverträdelser

Personuppgifter om lagöverträdelser räknas inte som känsliga personuppgifter enligt GDPR men har ändå ett starkt skydd. Som huvudregel är det bara myndigheter som får behandla denna typ av personuppgifter, men det finns vissa undantag. Om behandlingen till exempel är nödvändig för att kunna fastställa rättsliga anspråk eller fullgöra en rättslig förpliktelse enligt lag kan andra än myndigheter få behandla uppgifterna. I enskilda fall kan IMY också besluta om att andra än myndigheter i undantagsfall får behandla personuppgifter om lagöverträdelser. Personuppgiftsansvariga lämnar då in en ansökan om detta till IMY.

Uppgifter om lagöverträdelser kan vara information om att någon har begått ett brott eller lagöverträdelser som innefattar brott, har blivit dömd för ett brott i domstol, har varit föremål för till exempel häktning eller beslag, eller misstänks för ett konkret brott. Även om det inte finns en fällande brottmålsdom kan alltså en uppgift om att någon har eller kan ha begått en lagöverträdelse falla in i definitionen. En uppgift om att en person har brukat narkotika eller kört för fort kan exempelvis utgöra personuppgifter om lagöverträdelser.

Bestämmelser om personuppgifter om lagöverträdelser finns i artikel 10 GDPR samt i 3 kap. 8 – 9 §§ lag med kompletterande bestämmelser till EU:S dataskyddsförordning (dataskyddslagen).

Hur ni fyller i mallen

I denna del skriver ni ut om ni kommer att behandla personuppgifter om lagöverträdelser. Var så specifika som möjligt och förklara hur och varför personuppgifterna är personuppgifter om lagöverträdelser. Eftersom uppgifterna omfattas av ett starkt skydd behöver ni också ange varför ni får behandla dem. Om konsekvensbedömningen innefattar flera behandlingar och uppgifterna om lagöverträdelser är kopplad till en specifik behandling vore det bra om ni angav i vilken behandling som uppgifterna behandlas.

Exempel

- ✓ I ärendehanteringssystemet och den del som rör tjänsteanteckningar kommer det finnas anteckningar om kontakter med hyresgäster. I sällsynta fall förekommer det att hyresgäster uttalar hot mot anställda i bolaget vilket då polisanmäls. Bolaget gör anteckningar om detta vilket räknas som personuppgifter om lagöverträdelser. Bolaget får behandla uppgifterna eftersom de senare behövs för att framställa ett rättsligt anspråk om uppsägning av hyreskontraktet.

2.2.2 Kategorier av registrerade

Kategorier av registrerade betyder i vilken ”roll” eller i vilken egenskap som den registrerade får sina personuppgifter behandlade. Exempel på kategorier av registrerade är studenter, kunder eller leverantörer. Beroende på vilka kategorier av registrerade som ingår i behandlingen kan risken med behandlingen bli olika hög. Om behandlingen innefattar kategorier av registrerade som befinner sig i underläge eller beroendeställning och därmed räknas som sårbara kan t.ex. högre säkerhet behöva tillämpas. Dessa kategorier kan bl.a. vara barn, anställda, asylsökande, äldre eller patienter.

Anställda räknas som en sårbar kategori eftersom de befinner sig i beroendeställning i förhållande till sin arbetsgivare.

Bestämmelser om kategorier av registrerade finns i artikel 30.1 c GDPR.

Hur ni fyller i mallen

Här skriver ni ut vilken eller vilka kategorier av registrerade som ingår i behandlingen/behandlingarna

Exempel

Namn på behandling	Kategorier av registrerade
Elevadministration	Elever, lärare, vårdnadshavare
Rehabilitering för anställda	Anställda
Tillhandahålla daglig verksamhet enligt LSS	Brukare, anhöriga, anställda

2.2.3 Behandlingens/behandlingarnas omfattning

Att ange omfattningen av behandlingen/behandlingarna är en viktig del eftersom risken ofta ökar ju fler registrerade det är som omfattas.

Hur ni fyller i mallen

Här anger ni hur många registrerade som kommer att ingå i behandlingen. Om konsekvensbedömningen omfattar flera behandlingar får ni gärna ange hur

många registrerade per behandling. Om ni inte vet exakt antal får ni göra en uppskattning.

Exempel

- ✓ Behandlingen omfattar ca. 950 anställda

2.3 Ändamål

Ändamålet är anledningen till att ni behöver genomföra personuppgiftsbehandlingen. Inga personuppgiftsbehandlingar får genomföras utan att det finns ett tydligt avgränsat ändamål. Ändamålet ska vara formulerat och bestämt på förhand, alltså innan personuppgifterna samlas in och behandlas. Anledningen till att ett ändamål ska anges är att det ska vara möjligt att bedöma vilka personuppgifter som behöver behandlas och ifall en insamling av personuppgifter t.ex. är onödig eller för omfattande.

Bestämmelser om ändamål finns i artikel 5.1 b GDPR samt skäl 39.

Hur ni fyller i mallen

I denna del av mallen ska ni beskriva varför den aktuella personuppgiftsbehandlingen ska genomföras. Försök vara så specifik och konkret som möjligt. Det är viktigt att ändamålet inte är för allmänt hållet eller luddigt beskrivet.

Exempel

- ✓ **Luddigt och otydligt:** Behandlingens ändamål är att informera om verksamheten.
- ✓ **Avgränsat och specifikt:** Behandlingens ändamål är att genom broschyrer och annat tryckt material informera om verksamheten vid mässor och konferenser där verksamheten är representerad.
- ✓ **Luddigt och otydligt:** Behandlingens ändamål är att kamerabevaka verksamhetens entréer.
- ✓ **Avgränsat och specifikt:** Behandlingens ändamål är att öka tryggheten för personal/allmänheten och förebygga/förhindra störningar och brott på en brottsutsatt plats genom att använda kamerabevakning.

2.4 Rättslig grund

För att få behandla en personuppgift krävs det att man har giltig anledning - en rättslig grund för behandlingen. Detta gäller oavsett vilken typ av personuppgifter som man behandlar. Rättslig grund kallas också ibland för laglig grund, detta är alltså samma sak.

Ni måste välja en rättslig grund per behandling. Det är viktigt att identifiera den grund som är tillämplig och ange denna. Ni behöver också ha med er att i ett verksamhetssystem utförs det ofta många olika typer av behandlingar och det är

inte säkert att alla behandlingar har samma rättsliga grund. Det är bland annat därför som det är så viktigt att förstå vad som utgör en personuppgiftsbehandling och att ni på ett detaljerat sätt har kunnat klargöra vilka behandlingar av personuppgifter ni vill utföra och hur det ska gå till. Det är först när ni vet detta som ni kan hitta korrekta rättsliga grunder för era tilltänkta behandlingar. Det finns sex olika rättsliga grunder som en personuppgiftsansvarig kan använda sig av:

Samtycke: Ska vara frivilligt och specifikt för att vara giltigt. Det måste finnas genuin valmöjlighet och vara lika enkelt att samtycka som att återkalla samtycket. Om man inte samtycker får det inte innebära några negativa konsekvenser. Samtycke är inte en lämplig grund vid anställningsförhållande eller mellan en myndighet och en enskild eftersom det finns en betydande ojämlikhet i maktbalansen.

Artikel 6.1 a GDPR

Avtal: Är en giltig rättslig grund i fall där personuppgiftsansvarig är ena parten och den registrerade är andra parten. Personuppgifterna ska vara nödvändiga för att uppfylla villkoren i avtalet, t.ex. ett hyresavtal.

Artikel 6.1 b GDPR

Rättslig förpliktelse: Avser en skyldighet för den personuppgiftsansvarige som ska framgå i lag, författning eller kollektivavtal med tydligt definierat ändamål. Rättslig förpliktelse blandas ofta ihop med allmänt intresse men skillnaden mellan dessa är att grunden rättslig förpliktelse innebär att det uttryckligen ska framgå att man behöver genomföra en personuppgiftsbehandling. I lagen om sjuklön står t.ex. följande: Arbetsgivaren ska till Försäkringskassan anmäla sjukdomsfall som har gett arbetstagare hos honom rätt till sjuklön, om sjukperioden och anställningen fortsätter efter sjuklöneperiodens utgång. Här framgår det på ett direkt och uttryckligt sätt att arbetsgivare ska överlämna uppgifter till Försäkringskassan och den rättsliga grunden för en sådan personuppgiftsbehandling skulle därmed vara rättslig förpliktelse.

Artikel 6.1 c GDPR

Skydda grundläggande intresse: Denna grund kan bli aktuell i behandlingar som är direkt nödvändiga för att t.ex. rädda livet på någon som är medvetslös och som inte kan samtycka till en behandling. Det är mycket ovanligt att denna grund blir tillämplig, förutom för vissa enstaka behandlingar inom t.ex. vården.

Artikel 6.1 d GDPR

Allmänt intresse eller som ett led i myndighetsutövning: Denna rättsliga grund kan egentligen delas in i två delar, en som rör behandlingar som utgör en uppgift av allmänt intresse och en som rör behandlingar som ett led i myndighetsutövning.

Myndighetsutövning ska grundas på lagar, förordningar eller andra författningar. Personuppgiftsbehandlingar kopplade till att fatta beslut om

ekonomiskt bistånd, sätta betyg inom skolan eller lämna ut allmänna handlingar är exempel där myndighetsutövning kan användas som rättslig grund.

Den andra delen av denna rättsliga grund, behandling som är nödvändig för att utföra allmänt intresse, ska också den ha stöd i lagar, förordningar eller andra författningar. Det krävs att den rättsliga grunden är tydlig, precis och förutsägbar. Ju känsligare eller mer integritetsingripande som behandlingen är, desto mer preciserad behöver den rättsliga grunden vara. För att kunna använda denna grund för att behandla känsliga personuppgifter behöver det alltså tydligt framgå och genom till exempel lag vara förutsägbart för den registrerade att den personuppgiftsansvarige behöver behandla de aktuella uppgifterna. Allmänt hållna och generella formuleringar i en förvaltnings reglemente kan alltså många gånger inte ligga till grund för behandling av personuppgifter som ett led i att utföra uppgifter av allmänt intresse, eftersom de ofta är allt för opreciserade vilket gör personuppgiftsbehandlingarna oförutsägbara för de registrerade.

För att allmänt intresse och myndighetsutövning ska gå att använda som rättslig grund behöver personuppgiftsbehandlingen utöver att ha stöd i lag m.m., också vara nödvändig. Definitionen av nödvändig i dataskyddsrättlig mening har inte samma betydelse som det nog ofta kan ha i dagligt tal. För att nödvändighetskriteriet ska vara uppfyllt behöver det finnas ett tydligt samband mellan personuppgiftsbehandlingen och arbetsuppgiften av allmänt intresse eller myndighetsutövningen. Detta krav utgör ett skydd mot onödiga och omotiverade personuppgiftsbehandlingar som skulle innebära ett oproportionerligt stort intrång i de registrerades privatliv.

Artikel 6.1 e GDPR

Intresseavvägning: Denna rättsliga grund kan användas av den personuppgiftsansvarige om behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges berättigade intresse och dessa väger tyngre än den registrerades intressen. Myndigheter får inte stödja sin personuppgiftsbehandling på intresseavvägning för att utföra sina uppgifter.

Artikel 6.1 f GDPR

Hur ni fyller i mallen

I denna del av mallen ska ni beskriva vilken rättslig grund som den aktuella personuppgiftsbehandlingen stödjer sig på. Om konsekvensbedömningen omfattar fler än en behandling behöver det också framgå vilken rättslig grund som gäller för vilken behandling – såvida inte samma gäller för alla, men då behöver ni även ange det.

Om behandlingen/behandlingarna stödjer sig på allmänt intresse, myndighetsutövning eller rättslig förpliktelse behöver ni också ange vilken rättslig reglering det är som anger att den aktuella behandlingen är av allmänt intresse eller var det står att ni t.ex. måste rapportera in personuppgifter till Skatteverket eller Försäkringskassan.

Exempel

Namn på behandling	Rättslig grund	Motivering och hänvisning
Behandling av personuppgifter om anställda för löneadministration	Avtal (artikel 6.1 b GDPR)	Administration av lön är nödvändigt för att uppfylla villkoren i anställningsavtalet.
Behandling av personuppgifter i samband med bokföring för bolagets räkning	Rättslig förpliktelse (artikel 6.1 c GDPR)	Enligt xx § i lag om kommunal bokföring och redovisning är bolaget skyldig att…

2.4.1 Känsliga personuppgifter

Vissa typer av personuppgifter kallas för känsliga personuppgifter och har därför ett starkare skydd i lagstiftningen. Det är uppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person.

Här är det viktigt att komma ihåg att hälsouppgifter ska tolkas brett. En uppgift om att en anställd har sjukanmält sig räknas som en hälsouppgift även om det inte framgår detaljer om sjukdomen. Även en uppgift om att en anställd rehabiliteras eller har besökt en läkare räknas som en uppgift om hälsa som alltså är en känslig personuppgift enligt GDPR.

Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter men det finns fall då det är tillåtet. Några av undantagen när det är tillåtet att behandla känsliga personuppgifter framgår direkt av GDPR. Det finns även undantag i andra lagar, regler och kollektivavtal som innebär att det i vissa fall är tillåtet att behandla uppgifterna.

Bestämmelser om känsliga personuppgifter finns i artikel 9 GDPR och skäl 10, 34-35, 51-56 och 75.

Bra information om när det är tillåtet att behandla känsliga personuppgifter hittar ni på IMY:s hemsida, www.imy.se

Hur ni fyller i mallen

I mallen ska ni beskriva vilka känsliga personuppgifter som hanteras i behandlingen. Det är viktigt att kartlägga samtliga känsliga personuppgifter som behandlas och ange dessa i konsekvensbedömningen.

Tänk på att om känsliga personuppgifter behandlas behöver det finnas ett rättsligt stöd för behandlingen. Uppge i konsekvensbedömningen vilket stöd som finns för behandlingen. Detta innebär att det alltså måste finnas både en rättslig grund för behandlingen enligt artikel 6 GDPR och ett särskilt

undantag/rättsligt stöd för att få lov att behandla uppgifter av sådan känslig karaktär.

Den rättsliga grunden för behandlingen ska ni ange i punkt 2.4 i konsekvensbedömningen och under denna punkt anger ni tillämpligt undantag.

Ibland kan det krävas att ni utreder särskilt vilket eller vilka undantag som kan bli tillämpliga. Stäm gärna av med er förvaltnings-/bolagsjurist vid behov.

Exempel

Namn på behandling	Känslig personuppgift som behandlas	Tillämpligt undantag och motivering/ hänvisning
Bidragsansökan	Hälsouppgifter	Förvaltningen tillhandahåller social omsorg och uppgifterna kan därmed behandlas i enlighet med det undantag från förbudet som framgår av art 9.2 h GDPR. Det anges även i 7 § lag (2001:454) om behandling av personuppgifter inom socialtjänsten att förvaltningen kan behandla uppgifterna om de lämnats i ett ärende.

3 Behov/proportionalitet

En konsekvensbedömning avseende dataskydd ska innehålla en bedömning av om den planerade behandlingen av personuppgifter är nödvändig och proportionerlig för att nå de lagliga ändamålen med behandlingen. En del av detta är att säkerställa efterlevnaden av de grundläggande principerna i artikel 5 GDPR.

3.1 Ändamålsbegränsning

Personuppgifter får bara samlas in om det finns särskilda, uttryckligt angivna och berättigade ändamål. Detta kräver alltså att ändamålet eller ändamålen specificeras och motiveras innan behandlingen av personuppgifterna påbörjas. De registrerade ska utifrån beskrivningen av ändamålet kunna förstå hur deras personuppgifter kommer att användas. Personuppgifter som samlas in för ett specifikt ändamål får inte behandlas för ett annat ändamål.

Ändamålet påverkar även andra principer som gäller för behandlingen av personuppgifter, såsom uppgiftsminimering och lagringsminimering. Det är därför det är viktigt att specificera ändamålet med en behandling på förhand.

Bestämmelser om ändamålsbegränsning finns i 5.1 b GDPR samt skäl 39.

Hur ni fyller i mallen

Under punkt 2.3 i konsekvensbedömningen har ni beskrivit ändamålet med den aktuella behandlingen. Här ska ni beskriva vilka åtgärder som vidtas för att minska risken för att personuppgifterna behandlas på ett sätt som inte är förenligt med det ursprungliga ändamålet.

Exempel

- ✓ Verksamheten har tydligt definierat ändamålet med behandlingen och tagit fram rutiner för att säkerställa att ändamålet för varje personuppgift identifieras innan insamling. Av rutinen framgår även på vilket sätt uppgifterna ska dokumenteras.
- ✓ Inför införandet av den nya ansökningstjänsten har förvaltningen tagit fram anvisningar till medarbetarna för att förhindra att uppgifter samlas in enbart för att de är ”bra att ha”.

3.2 Uppgiftsminimering

Principen om uppgiftsminimering innebär att det inte är tillåtet att behandla fler uppgifter om den registrerade än vad som behövs för ändamålet. De uppgifter som samlas in ska vara både adekvata och relevanta.

För att veta om en personuppgift får behandlas måste orsaken till varför uppgiften behövs identifieras. Den personuppgift som behandlas ska vara tydligt kopplad till ändamålet. Om ändamålet, till exempel utförande av en tjänst, kan uppnås utan att vissa personuppgifter behandlas, så är dessa uppgifter inte nödvändiga och ska alltså inte användas. Det är inte heller tillåtet att samla in personuppgifter för obestämda framtida behov, bara för att de kan vara ”bra att ha”.

Bestämmelser om uppgiftsminimering finns i artikel 5.1 c GDPR samt skäl 39.

Hur ni fyller i mallen

Här ska ni fylla i på vilket sätt behandlingen uppfyller principen om uppgiftsminimering. Motivera varför de uppgifter som samlas in och behandlas är nödvändiga. Beskriv på vilket sätt det säkerställs att inte fler personuppgifter än vad som är nödvändigt behandlas.

Exempel

- ✓ På blanketten med kontaktuppgifter behöver vårdnadshavaren fylla i mobiltelefonnummer för att de ska kunna kontaktas vid nödsituationer.
- ✓ Verksamheten har genom att ta bort fritextfältet i formuläret begränsat möjligheten för brukaren att lämna personuppgifter som inte behövs för behandlingen.

- ✓ Verksamheten har säkerställt att det inte uppstår några tillfälliga filer i systemet i samband med att en ny ansökan skapas.
- ✓ Verksamheten har säkerställt att åtkomst- och användarbehörigheterna till personuppgifterna är begränsade till handläggarna vid ansökningsenheten.

3.3 Lagringsminimering

Personuppgifter får bara sparas så länge som de behövs för ändamålet med personuppgiftsbehandlingen. När uppgifterna inte längre behövs ska de raderas eller avidentifieras. I vissa fall framgår det av lagstiftningen hur länge uppgifter ska sparas eller att det är tillåtet att spara uppgifter för särskilda syften.

Om lagringstiden inte är reglerad i lag så måste den personuppgiftsansvarige bedöma hur länge det är nödvändigt att spara personuppgifterna i förhållande till ändamålet. Förvaltningar och bolag behöver ha rutiner för gallring av personuppgifter i vilka det anges tidsfrister för radering eller för regelbunden kontroll. Rutiner för gallring brukar därför ofta framgå av verksamhetens dokumenthanteringsplan.

Bestämmelser om lagringsminimering finns i artikel 5.1 e GDPR samt skäl 39.

Hur ni fyller i mallen

Här ska ni fylla i på vilket sätt behandlingen uppfyller principen om lagringsminimering. Redogör för om det finns bestämmelser i lag som avgör hur länge uppgifterna ska sparas eller om det är tillåtet att spara uppgifterna för ett särskilt syfte. Beskriv annars hur länge det är nödvändigt att spara personuppgifterna och vad det finns för rutiner för gallring av personuppgifter- Sker det till exempel automatiskt eller genom en manuell hantering. Ange också vad som framgår av förvaltningens/bolagets dokumenthanteringsplan. Här bör ni ange specifik hänvisning till dokumenthanteringsplanen och skriva ut hur länge personuppgifterna ska sparas/när de ska gallras. Beskriv även hur uppgifterna raderas eller avidentifieras och vem som ansvarar för det.

Exempel

- ✓ Underlaget som utgör räkenskapsinformation måste i enlighet med bokföringslagen sparas i sju år efter det kalenderår då räkenskapsåret avslutades. Därefter ansvarar arkivenheten för radering av uppgifterna. Rutiner för bevarande och radering framgår av verksamhetens dokumenthanteringsplan, se verksamhetsområde X, processgrupp X.1, process X.1.1.
- ✓ Verksamheten granskar regelbundet de personuppgifter som behandlas i systemet. De uppgifter som inte längre behövs raderas genom manuell hantering. Kontrollerna genomförs var sjätte månad och ansvarig för genomförandet är avdelningschef för avdelning X. Hur den praktiska hanteringen ska gå till framgår av rutin Z som finns tillgänglig på verksamhetens intranät. Rutiner för bevarande och radering framgår av

verksamhetens dokumenthanteringsplan, se verksamhetsområde Y, processgrupp Y.1, process Y.1.1.

- ✓ Verksamheten har rutiner för att säkerställa att när personuppgifter inte längre behövs ska de avidentifieras. Avidentifieringen sker genom att alla personuppgifter ersätts en slumpmässigt framtagen kod. Av rutinen framgår även vilka funktioner inom verksamheten som ansvarar för processen. När avidentifiering har skett raderas personuppgifterna i enlighet med verksamhetens dokumenthanteringsplan, se verksamhetsområde T, processgrupp T.1, process T.1.1.

3.4 Åtgärder som stärker de registrerades rättigheter

En viktig del i att bedöma behovet av och proportionaliteten hos en behandling utgörs av vilka åtgärder som har vidtagits för att stärka de registrerades rättigheter. Registrerades rättigheter och hur de har möjlighet att utöva dessa utgör en grundbult i dataskyddsförordningen och är således också en viktig del i en konsekvensbedömning. I detta avsnitt ska ni redogöra för konkreta åtgärder kopplat till den/de specifika behandlingen/behandlingarna, inte enbart redogöra för att de registrerade har vissa rättigheter.

3.4.1 Informationsplikt

När personuppgifter behandlas har den registrerade rätt att få information om det. Den som behandlar uppgifterna (den personuppgiftsansvarige) ska informera om det både när uppgifterna samlas in och när den registrerade begär det.

Den registrerade har bland annat rätt att få veta varför personuppgifterna samlas in, hur länge uppgifterna kommer att sparas, vilka som kommer att ha tillgång till uppgifterna, vilka rättigheter hen har enligt GDPR och kontaktuppgifter till den personuppgiftsansvarige.

Bestämmelser om den registrerades rätt till information finns i artikel 13–14 GDPR.

Hur ni fyller i mallen

Här ska ni ange på vilket sätt den registrerade får information om behandlingen. Tänk på att informationen måste uppfylla kravet på att vara lättillgänglig för den registrerade. Informationen ska ges i skriftlig form (digital information går bra) och språket ska vara klart och tydligt.

Exempel

- ✓ Bolaget har en integritetspolicy som finns tillgänglig för alla på verksamhetens hemsida. Integritetspolicyn är uppdaterad med information om den aktuella behandlingen. Hemsidan är utformad så att

informationen är lätt att hitta för de registrerade som omfattas av behandlingen, genom en väl utmärkt länk på startsidan.
- ✓ Förvaltningens medarbetare informerar om verksamhetens personuppgiftsbehandling via en länk i e-postsignaturen.
- ✓ I systemet som behandlingen sker i finns speciellt framtagen information om den aktuella behandlingen som är lätt att nå via menyn när den anställde/medborgaren loggar in i systemet.

3.4.2 Tillgång och dataportabilitet

Den registrerade har rätt att vända sig till en personuppgiftsansvarig och få svar på om hens personuppgifter behandlas eller inte. Om personuppgifter behandlas så ska den registrerade få en kopia av de uppgifter som behandlas, ett s.k. registerutdrag. Dessutom ska den registrerade få information om behandlingen av personuppgifterna. På detta sätt kan den registrerade kontrollera att behandlingen är laglig.

Den registrerade har rätt att i vissa situationer få ut sina personuppgifter och överföra dessa till en annan personuppgiftsansvarig, s.k. rätt till dataportabilitet. Detta gäller dock bara sådana personuppgifter som den registrerade själv har lämnat och som behandlats med stöd av ett samtycke eller för att uppfylla ett avtal.

Bestämmelser om den registrerades rätt till tillgång finns i artikel 15 GDPR. Rätten till dataportabilitet behandlas i artikel 20 GDPR.

Hur ni fyller i mallen

Här ska ni ange på vilket sätt det säkerställs att den registrerade kan få ta del av begärda uppgifter och att det sker inom gällande tidsfrist. Beskriv exempelvis om verksamheten har en rutin för att hantera en begäran om registerutdrag eller en begäran om att få använda uppgifterna på annat håll.

Exempel

- ✓ Förvaltningen har lättillgänglig information på hemsidan om de registrerades rätt till tillgång och på sidan finns även en blankett att fylla i för att begära ett registerutdrag.
- ✓ Verksamheten har en rutin för hur en begäran om att överföra personuppgifter till en annan personuppgiftsansvarig ska hanteras. Av rutinen framgår bland annat på vilka behandlingar rätten till dataportabilitet kan tillämpas och för vilka uppgifter den gäller.

3.4.3 Rättelse och radering

Uppgifterna om den registrerade ska vara riktiga och korrekta. Är uppgifterna felaktiga eller bristfälliga så ska de rättas. En registrerad har rätt att vända sig till den personuppgiftsansvarige och begära att uppgifterna rättas utan onödigt dröjsmål. Den registrerade får även komplettera med sådana personuppgifter som saknas.

Den registrerade har i vissa situationer rätt att begära att den personuppgiftsansvarige utan dröjsmål raderar personuppgifterna. Uppgifterna måste raderas bland annat när uppgifterna inte längre behövs för de ändamål som de samlades in för, när behandlingen grundar sig på ett samtycke och den registrerade återkallar samtycket, om personuppgifterna har behandlats olagligt och om radering krävs för att uppfylla en rättslig skyldighet. Det finns undantag från rätten till radering när det är nödvändigt att tillgodose andra viktiga rättigheter, exempelvis att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Bestämmelser om den registrerades rätt till rättelse finns i artikel 16 GDPR. Rätten till radering och i vilka situationer denna rättighet kan användas framgår av artikel 17 GDPR.

Hur ni fyller i mallen

Här ska ni ange på vilket sätt det säkerställs att den registrerade kan få sina uppgifter rättade eller raderade och att det sker inom gällande tidsfrist. Beskriv exempelvis om verksamheten har en rutin för att hantera en begäran om rättelse eller radering.

Exempel

- ✓ I det aktuella systemet finns inbyggda funktioner för att utföra rättelse och radering. Dessa funktioner kompletteras i den aktuella behandlingen av instruktioner för hur handläggare går till väga om en begäran om rättelse eller radering skulle inkomma. Rätten till radering är begränsad pga. arkivbestämmelser.
- ✓ Verksamheten har en rutin för raderingsprocessen om den registrerade återkallar sitt samtycke till behandling av personuppgifter.
- ✓ Verksamheten har en tydlig och detaljerad rutin för hur radering av uppgifter utförs i praktiken, avseende både manuell och automatiserad radering. Rutinen innehåller även instruktioner för att säkerställa att uppgifter i säkerhetskopior raderas.

3.4.4 Invändningar och begränsning av behandling/behandlingar

Den registrerade har i vissa situationer rätt att invända mot behandlingen av sina personuppgifter, alltså att be att de inte behandlas alls. Rätten att invända gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning.

Den registrerade har även i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Personuppgifterna får då bara behandlas i vissa specifika fall.

Bestämmelser om den registrerades rätt att göra invändningar finns i artikel 21 GDPR. Rätten till begränsning av behandling framgår av artikel 18 GDPR.

Hur ni fyller i mallen

Här ska ni ange på vilket sätt det säkerställs att den registrerade har möjlighet att invända mot behandlingen eller begära begränsning av behandlingen. Beskriv exempelvis om verksamheten har en rutin för att underlätta för de registrerade att utöva sina dataskyddsrättigheter.

Exempel

- ✓ Förvaltningen har en arbetsrutin för att säkerställa att de registrerades rättigheter tillgodoses. Den rättsliga grunden för den aktuella personuppgiftsbehandlingen är att utföra en uppgift av allmänt intresse och därmed kan en registrerad invända mot behandlingen. Vid en sådan begäran ska förvaltningen följa gällande rutin för att bland annat avgöra om rätten att göra invändningar ska tillämpas på den behandling som bedöms.
- ✓ Bolaget har en arbetsrutin för att säkerställa att de registrerades rättigheter tillgodoses. Vid en begäran om begränsning av behandling ska verksamheten följa gällande rutin för att bland annat bedöma om rätten till begränsning är tillämplig. Av rutinen framgår även hur begränsningen genomförs i praktiken.

3.4.5 Personuppgiftsbiträdesavtal och instruktioner

Om personuppgiftsbiträden används är det viktigt att det upprättas personuppgiftsbiträdesavtal med dessa och att den personuppgiftsansvarige lämnar instruktioner till biträdet. I instruktionerna ska det anges hur personuppgiftsbiträdet får behandla den personuppgiftsansvariges personuppgifter, t.ex. vilka tekniska och administrativa säkerhetsåtgärder som ska finnas. Om biträdet går utöver vad som framgår av avtalet och instruktionerna kan biträdet själv komma att betraktas som personuppgiftsansvarig för denna behandling.

Det kanske inte upplevs som att denna del hör hemma i avsnitt 3.4, som behandlar åtgärder som stärker de registrerades rättigheter, men att ha avtal och instruktioner på plats är en viktig del av skyddet för de registrerade. Om det inte finns upprättat korrekta avtal med tillhörande instruktioner kan den personuppgiftsansvarige inte vara säker på att biträdet enbart behandlar personuppgifterna på det sätt som man har kommit överens om.

I mallen används också begreppet ”underbiträdesavtal”, detta avtal tecknas mellan personuppgiftsbiträdet och underbiträdet. Det är viktigt att ni som personuppgiftsansvariga har kontrollerat hela kedjan av biträden och underbiträden varför det kan vara aktuellt att även ha med hänvisningar till detta avtal.

Bestämmelser om personuppgiftsbiträdesavtal och instruktioner finns i artikel 28 GDPR.

Hur ni fyller i mallen

I denna del av mallen ska ni ange specifika hänvisningar till de personuppgiftsbiträdesavtal som ska finnas om det är så att behandlingen utförs helt eller delvis av ett personuppgiftsbiträde.

I vissa fall kan det bli aktuellt att också ha med specifika hänvisningar till de avtal som personuppgiftsbiträdet kan ha med ett underbiträde (underbiträdesavtal). Detta kan t.ex. vara fallet om Intraservice agerar som personuppgiftsbiträde. Då kan det vara lämpligt att ange en specifik hänvisning till det avtal som Intraservice har tecknat med underbiträdet.

Exempel

- ✓ Personuppgiftsbiträdesavtal med IT-företaget Q AB, diarienummer 1234/22. Specifika instruktioner har lämnats till företaget.
- ✓ Personuppgiftsbiträdesavtal med Intraservice, diarienummer X5678/22. Specifika instruktioner har lämnats. Intraservice har i sin tur upprättat avtal med IT-företaget Z AB och lämnat tillhörande instruktioner, detta avtal har diarienummer XXXX/22 i Intraservices diarium.

3.5 Samlad bedömning av behovet av och proportionaliteten hos behandlingen/behandlingarna

I detta avsnitt ska ni ange en samlad bedömning av behovet av och proportionaliteten med behandlingen/behandlingarna. Detta innebär att ni, utifrån det som ni har angett ovan, sammanfattar varför behandlingen är nödvändig utifrån verksamhetens uppdrag. Ni anger i detta avsnitt också de åtgärder ni har vidtagit och de avvägningar som ni har gjort för att säkerställa att behandlingen inte innebär mer av ett integritetsintrång än vad den absolut måste vara. Ni ska också beskriva varför behandlingen som utförs är proportionerlig, alltså varför fördelarna med behandlingen och det integritetsintrång som den innebär överväger nackdelarna.

Exempel

- ✓ **Mindre bra:** Behandlingen är nödvändig och proportionerlig.
- ✓ **Bra:** H-förvaltningen har ett behov av att utföra behandlingen eftersom den manuella hantering som nu används kan ersättas med en digital. Behandlingen bedöms vara nödvändig eftersom det ändrade arbetssättet kommer att innebära stora effektivitetsvinster vilket gynnar invånarna i kommunen i form av förbättrat stöd och service. Under avsnitt 3.1, 3.2, och 3.3 anges flera åtgärder som vidtagits för att bland annat säkerställa att insamlingen av personuppgifter är begränsad och att tillgången till dem regleras genom behörighetsstyrning. Behandlingen medför visserligen att de registrerades personuppgifter behandlas digitalt vilket öppnar upp för fler risker än den tidigare manuella hanteringen innebar,

men fördelarna bedöms överstiga nackdelarna och behandlingen anses alltså vara proportionerlig.

4 Överföring av personuppgifter utanför EU/EES

4.1 Sker det en överföring av personuppgifter utanför EU/EES?

Så kallade tredjelandsöverföringar, alltså överföring av personuppgifter till länder utanför EU/EES, är noggrant reglerade i GDPR. Anledningen till detta är att ett av syftena med GDPR är att säkerställa en likvärdig nivå av skydd för personuppgifterna likt den som finns inom EU/EES även i det fall personuppgifterna blir tillgängliga för någon i ett land utanför EU/EES-området. Därför måste den som vill överföra personuppgifter utanför detta område vidta flera steg för att på så vis upprätthålla en likvärdig skyddsnivå som den inom EU/EES.

I detta är det viktigt att beakta vad som anses utgöra en överföring. Ofta är det trots allt ganska lätt att bedöma att något är en överföring. Om personuppgifterna lagras på en server i Kina är det exempelvis en solklar tredjelandsöverföring. Däremot tänker kanske inte de flesta på att om supporten för exempelvis ett system är placerad i Indien och supporten kan komma att se personuppgifter i systemet så räknas också detta som en överföring (trots att tillgången sker ”remote”).

Tänk också på att vissa tredjeländer har en lagstiftning som innebär att uppgifter kan komma att behöva lämnas ut till det tredjelandets myndigheter oavsett om all behandling under vanliga omständigheter sker inom EU/EES. I dessa fall föreligger det alltså en risk för tredjelandsöverföring.

Bestämmelser om överföring av personuppgifter till tredjeländer eller internationella organisationer finns i kapitel 5 GDPR.

Hur ni fyller i mallen

När ni noggrant har kontrollerat alla personuppgiftsbiträden och underbiträden anger ni här om någon tredjelandsöverföring förekommer eller inte, samt om det finns risk för tredjelandsöverföring.

Vid risk för tredjelandsöverföring ska ni ange skälen till att sådan risk föreligger och hur ni har kommit till den insikten.

4.2 Översikt överföringar

Man kan lite slarvigt säga att överföringar av personuppgifter till tredjeland som huvudregel är förbjudna om man inte kan säkerställa ett tillräckligt skydd för personuppgifterna. Som framgår under avsnitt 4.1 behöver det här skyddet vara lika bra som det som hade funnits om personuppgifterna hade stannat inom EU/EES. Detta är högt ställda krav och ställer i sin tur krav på att personuppgiftsansvariga har koll på sina behandlingar och sina personuppgiftsbiträden. För att få överföra personuppgifter behöver det finnas ett tillämpligt överföringsverktyg (detta kallas också ibland för överföringsmekanism, men betyder alltså samma sak). Verktyget kan utgöras av adekvansbeslut eller lämpliga skyddsåtgärder som t.ex. standardavtalsklausuler eller bindande företagsbestämmelser, som ibland behöver kombineras med andra skyddsåtgärder för att anses vara tillräckliga.

Adekvansbeslut (ibland även kallat artikel 45-beslut) finns för flera länder och gäller för överföringar av personuppgifter från EU/EES. Dessa beslut fattas av EU-kommissionen som endast utfärdar dem efter att noga ha gått igenom bland annat mottagarlandets lagstiftning och om landet respekterar mänskliga rättigheter. Listan över länder som har sådana här beslut är föränderlig eftersom nya beslut fattas och beslut ibland ogiltigförklaras.

Vi råder er därför att dubbelkolla listan över aktuella adekvansbeslut som finns hos EU-kommissionen här.

Bestämmelser om överföring av personuppgifter på grundval av ett beslut om adekvat skyddsnivå finns i artikel 45 GDPR.

Frågan om tredjelandsöverföringar och hur skyddet för personuppgifter garanteras är i vissa fall mycket komplicerad. Glöm inte att utnyttja den kompetens ni har inom er egen verksamhet och att involvera dataskyddsombudet i god tid.

Hur ni fyller i mallen

Om behandlingen innefattar en tredjelandsöverföring behöver detaljerna kring detta framgå av konsekvensbedömningen. I mallen finns denna tabell som ni ska fylla i.

Namn på behandlingen: Här anger ni i vilken behandling som överföringen äger rum. Är det t.ex. i supportärenden? Eller sker hela behandlingen i ett land utanför EU/EES?

Vilka personuppgifter överförs: Det är kanske så att den del av behandlingen som är en tredjelandsöverföring bara innefattar ett visst antal personuppgifter, ange då bara de personuppgifter som faktiskt överförs.

Till vilket land överförs personuppgifterna: Här anger ni specifikt land.

Finns det ett adekvansbeslut för mottagarlandet? Ja eller nej? Om svaret är Ja, kan ni sedan fortsätta direkt till avsnitt 5. Om svaret däremot är Nej, behöver ni fortsätta till avsnitt 4.3.

Exempel

Namn på behandling	Vilka person-uppgifter överförförs?	Till vilket land överförs person-uppgifterna?	Finns det ett adekvansbeslut för mottagar-landet?
Support för e-post	För- och efternamn Arbetsplats och titel E-postadress	USA	Nej

4.3 Lämpliga skyddsåtgärder

Även om det inte finns ett adekvansbeslut kan överföringar av personuppgifter till ett land utanför EU/EES ändå vara tillåtna. Då behöver den personuppgiftsansvarige hitta ett annat överföringsverktyg, till exempel lämpliga skyddsåtgärder i form av standardavtalsklausuler.

Beroende på hur lagstiftningen ser ut i mottagarlandet och om utländska medborgare till exempel ges rätt till effektiva rättsmedel är det inte säkert att standardavtalsklausuler eller bindande företagsbestämmelser är tillräckligt som garanti. Då kan personuppgiftsansvariga också behöva vidta extra skyddsåtgärder, dessa anges (om de bedöms nödvändiga) i avsnitt 4.3.1.

Läs mer om lämpliga skyddsåtgärder hos IMY.

Bestämmelserna om lämpliga skyddsåtgärder finns i artikel 46 GDPR.

Hur ni fyller i mallen

Namn på behandling	Lämpliga skyddsåtgärder	Motivering av lämpliga skyddsåtgärder

Namn på behandling: Ange vilken behandling som överföringen rör.

Lämpliga skyddsåtgärder: Om överföringsverktyget adekvansbeslut inte finns tillgängligt behöver lämpliga skyddsåtgärder användas i stället. Ange vilka skyddsåtgärder som ni lutar er mot, t.ex. standardavtalsklausuler eller bindande företagsbestämmelser.

Motivering av lämpliga skyddsåtgärder: Här ska ni ange om den skyddsåtgärd ni angett i föregående fält bedöms som tillräcklig eller inte. Som framgår ovan behöver de här skyddsåtgärderna ibland kombineras med ytterligare skyddsåtgärder beroende på vilket mottagarland ni har att göra med.

Exempel

Namn på behandling	Lämpliga skyddsåtgärder	Motivering av lämpliga skyddsåtgärder
Support i e-postärenden	Standardavtalsklausuler (SCC:er)	Standardavtals-klausuler för tredjelandsöverföringar från den 4 juni 2021

4.3.1 Andra/extra skyddsåtgärder

Som nämnt ovan i avsnitt 4.3 kan de valda skyddsåtgärderna behöva kompletteras med ytterligare skyddsåtgärder för att säkerställa skyddsnivån för de registrerades personuppgifter i mottagarlandet. Det kan handla om både tekniska och administrativa åtgärder. EDPB, Europeiska dataskyddsstyrelsen, har tagit fram rekommendationer och vägledningar för hur man som personuppgiftsansvarig ska tänka vid valet av extra skyddsåtgärder. I vissa fall räcker det inte med enbart administrativa åtgärder utan det kan krävas även tekniska åtgärder. Se följande dokument från EDPB:

Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter.

Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder.

Ni hittar rekommendationerna via EDPB:s hemsida:
https://edpb.europa.eu/edpb_sv

Hur ni fyller i mallen

Om ni bedömer att överföringen kräver andra/extra skyddsåtgärder, ska ni ange vilka skyddsåtgärder som valts och varför. Motivera varför ni bedömer att skyddsåtgärderna är tillräckliga för att säkerställa skyddsnivån.

Exempel

- ✓ Förvaltningen har ett personuppgiftsbiträde (Z) för system Y och har kontrollerat hela kedjan av underbiträden och konstaterar att ett underbiträde är amerikanskt. Personuppgiftsbiträde Z uppger att de tecknat standardavtalsklausuler med underbiträde som ska garantera

överföringen. Förvaltningen kräver att personuppgiftsbiträdet vidtar kompletterande åtgärder för att säkerställa likvärdig skyddsnivå vilket görs genom att kryptering av uppgifterna sker på ett säkert sätt som håller över tid. Åtgärderna finns dokumenterade tillsammans med personuppgiftsbiträdesavtalet hos förvaltningen.

4.4 Undantag i särskilda situationer

Om den planerade överföringen inte omfattas av något adekvansbeslut (beslut om adekvat skyddsnivå) eller om lämpliga skyddsåtgärder samt kompletterande åtgärder inte är tillräckliga, finns det i GDPR ett antal undantag för överföringar i särskilda situationer. Det kan till exempel handla om att den registrerade uttryckligen har samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med överföringen när det saknas beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder. Överföringen kan också genomföra om den är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige.

Undantagen är noggrant reglerade och i artikel 49 GDPR finns det en uttömmande lista på när det skulle kunna vara möjligt att i undantagsfall göra en överföring. EDPB har tagit fram en vägledning för när undantagen enligt artikel 49 får användas som kan vara bra att titta på. Det är viktigt att komma ihåg att undantagen ska tolkas restriktivt. Detta eftersom riskerna för de registrerades fri- och rättigheter ökar med sådana oreglerade överföringar. Vägledningen förtydligar också att ett övergripande villkor för användning av flera av undantagen är att överföringen av uppgifter måste vara nödvändig för ett visst ändamål. En nödvändighetsprövning bör därför göras innan överföringen grundas på ett undantag.

En överföring enligt artikel 49 får inte göras innan ni först har prövat möjligheterna att överföra personuppgifterna med någon av mekanismerna i artikel 45 och 46, och endast om det inte går kan något av undantagen tillämpas.

Om inget av undantagen är tillämpliga finns det en liten möjlighet att trots det göra en överföring. Det gäller om överföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges berättigade intressen och att den registrerades intressen eller rättigheter och friheter inte väger tyngre. Ni (den personuppgiftsansvarige) ska också ha bedömt samtliga omständigheter kring överföringen av personuppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifterna. I sådana fall ska ni informera tillsynsmyndigheten om överföringen och den registrerade ska få information.

Hur ni fyller i mallen

Om ni bedömer att det finns ett tillämpligt undantag, ange vilket och förklara varför ni bedömer det vara lämpligt för den aktuella behandlingen.

Exempel

- ✓ Bolagets representant har inför en resa till samarbetspartner i USA skickat en bild på en medarbetare. Genom en samtyckesblankett har bolaget säkerställt att medarbetaren godkänner bilden samt överföringen av personuppgifter till USA i det enskilda fallet.

4.5 Samlad bedömning

En överföring av personuppgifter får bara ske under förutsättning att villkoren i kapitel 5 GDPR uppfylls. En bedömning behöver göras om den aktuella överföringen är möjlig.

Hur ni fyller i mallen

Sammanfatta valt överföringsverktyg och motivering för att beskriva varför eller varför inte överföringen till tredjeland går att genomföra.

Exempel

- ✓ Eftersom det finns tillämpliga standardavtalsklausuler ingångna mellan leverantören och underleverantören och inga kompletterande skyddsåtgärder krävs, bedöms överföringen uppfylla kraven enligt GDPR och säkerställer en likvärdig skyddsnivå.

5 Risker och åtgärder

5.1 Generella risker och åtgärder

Bedömningen av risker och åtgärder är en avgörande del i att behandla personuppgifter och utgör en viktig komponent i en konsekvensbedömning. En analys av riskerna redan i planeringsskedet (en konsekvensbedömning ska ju genomföras före det att en behandling påbörjas) gör det möjligt att redan från start trygga en säker och ändamålsenlig behandling av personuppgifter.

I de flesta fall finns det både tekniska och administrativa åtgärder inom en verksamhet som minskar risker och stärker skyddet för såväl den fysiska säkerheten som för informationen som verksamheten hanterar. Dessa åtgärder av mer generell karaktär skyddar alltså ofta alla eller i vart fall de flesta av de personuppgifter som behandlas, oavsett vilken typ av behandling det är som utförs. Grundskyddet som en verksamhet har kan dock skilja sig åt, vilket alltså kan påverka bedömningen av risken för de personuppgifter som behandlas. Om det t.ex. finns riktlinjer för datoranvändning är det ju en del av skyddet för alla personuppgiftsbehandlingar som äger rum via en dator. Avsnitt 5.1.1 och 5.1.2 syftar alltså till att underlätta för er att ange hur skyddet för personuppgifterna i era behandlingar ser ut.

5.1.1 Generella tekniska åtgärder

Generella tekniska åtgärder syftar till de allmänna och grundläggande tekniska åtgärder som en verksamhet har vidtagit som kanske inte är kopplade till en specifik behandling eller en specifik risk. Vissa åtgärder kan alltså skydda olika uppgifter samtidigt.

Hur ni fyller i mallen

Här kryssar ni i de åtgärder som ni har vidtagit, håller på att införa eller planerar att införa. Om de inte är aktuella för den/de aktuella behandlingarna kryssar ni i ”ej tillämplig”. Kommentera gärna ert svar om ni har kompletterande information att lämna eller vill motivera hur ni har kryssat i. Kom ihåg att det kan finnas relevanta generella åtgärder inom er verksamhet som inte är med i listan i mallen. I så fall kan dessa läggas till i raden ”Annat”.

Är ni osäkra på vilket grundskydd som finns i er verksamhet? Glöm inte att involvera och fråga t.ex. er säkerhets/IT-avdelning!

5.1.2 Generella administrativa åtgärder

Med generella administrativa åtgärder menas de åtgärder i form av t.ex. rutiner, riktlinjer och beslutade arbetssätt som fungerar som ett skydd för den information som en verksamhet hanterar. Likt de generella tekniska åtgärderna kan ett arbetssätt eller en rutin skydda olika uppgifter på samma gång.

Hur ni fyller i mallen

Här kryssar ni i de åtgärder som ni har vidtagit, håller på att införa eller planerar att införa. Om de inte är aktuella för den/de aktuella behandlingarna kryssar ni i ”ej tillämplig”. Kommentera gärna ert svar om ni har kompletterande information att lämna eller vill motivera hur ni har kryssat i. Kom ihåg att det kan finnas relevanta generella åtgärder inom er verksamhet som inte är med i listan i mallen. I så fall kan dessa läggas till i raden ”Annat”.

5.2 Bedömning av specifika risker

Den personuppgiftsansvarige ska bedöma de risker som förknippas med personuppgiftsbehandlingen ur den registrerades perspektiv. Riskerna ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter som yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion. Det krävs dock att det finns en koppling till behandlingen av personuppgifter för att rättigheten ska bedömas i en konsekvensbedömning.

Vid riskbedömningen måste den personuppgiftsansvarige först identifiera de risker som uppkommer till följd av behandlingen av personuppgifter och konsekvenserna som riskerna kan leda till för de registrerade. Nästa steg är att bedöma hur allvarliga konsekvenserna är för de registrerade och hur sannolikt det är att de identifierade riskerna inträffar. Avsikten med riskbedömningen är att sedan att kunna hantera de höga risker som har identifierats genom att välja ändamålsenliga skyddsåtgärder.

När risker med behandlingen av personuppgifter ska identifieras är det viktigt att beakta att riskerna kan finnas både inom organisationen och utanför den. Riskerna kan bero både på människors verksamhet och icke-mänskliga orsaker samt uppkomma både genom medvetet agerande och oaktsamt agerande. Det är även av vikt att ha i åtanke att konsekvenserna av de risker som uppkommer för de registrerade kan vara av väldigt olika karaktär. Skadorna kan vara fysiska, materiella eller immateriella/moraliska.

När ni ska bedöma hur allvarliga konsekvenser som riskerna kan leda till måste ni ta hänsyn till samtliga omständigheter kring behandlingen. Omständigheter som kan påverka allvarligheten är bland annat personuppgifternas art. Konsekvenserna för de registrerade blir i regel allvarligare om behandlingen avser exempelvis extra skyddsvärda personuppgifter, känsliga personuppgifter eller uppgifter om lagöverträdelser. Ett annat exempel då allvarligheten ökar är när det rör sig om sårbara personer, vilket kan vara fallet när uppgifter om barn behandlas.

I samband med riskbedömningen krävs det också att ni bedömer hur sannolikt det är att de identifierade riskerna inträffar. Vid bedömningen av hur troligt det är att exempelvis en viss händelse inträffar kan hänsyn tas till bland annat redan tillgängliga skyddsåtgärder och hur vanligt förekommande det är att den aktuella risken inträffar.

Kort sammanfattat ska ni här alltså fundera på vad det är som kan hända och hur sannolikt det är att det faktiskt händer. I detta är det viktigt att ni tänker och vitt och brett och låter fantasin flöda fritt. Alla tänkbara risker bör inledningsvis beaktas. Därefter kan ni gå igenom och rensa bort de risker som eventuellt ligger utanför behandlingens omfattning.

Excelfilen ”DSE Riskbedömningsmall”

Hur ni fyller i excelfilen ”DSE Riskbedömningsmall”

När riskbedömningen ska genomföras ska riskerna både identifieras och bedömas. Det är betydelsefullt att kunna säkerställa att eventuella risker kan identifieras på ett heltäckande sätt ur olika perspektiv. Tänk därför på att det är av stor vikt att ni som genomför riskbedömningen tillsammans har relevanta sakkunskaper inom bl.a. dataskydd, informationssäkerhet och riskhantering, samt har kunskaper om den praktiska verksamheten. Det är också viktigt att ni tar del av relevant dokumentation, exempelvis tekniskt underlag, inför riskbedömningen.

När ni genomför riskbedömningen ska ni ange relevanta uppgifter för bedömningen i excelfilen ”DSE Riskbedömningsmall”. Detta dokument ska sedan utgöra bilaga 1 till konsekvensbedömningen. Risker med medelhöga och höga riskvärde ska även anges direkt i konsekvensbedömningen under avsnitt 5.2. Se nedan för vidare instruktioner.

I excelfilen ”DSE Riskbedömningsmall” första bladet, ”Riskbedömning”, ska ni ange följande uppgifter:

Risk-ID	Namn på behandling	Risk *Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter, förlust av personuppgifter eller annan form av risk*	Beskrivning av risk
1			Exempel 1
2			Exempel 2

Risk-ID: Varje identifierad risk får ett eget nummer.

Namn på behandling: Ange vilken behandling som risken rör.

Risk: Ange om risken innebär obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter, förlust av personuppgifter eller annan form av risk.

Med *obehörig åtkomst* avses situationer när någon inom eller utanför organisationen har tagit del av personuppgifter som den inte har behörighet till, exempelvis vid ett dataintrång eller när e-post skickas till fel mottagare.

Med *oönskad ändring av personuppgift* avses situationer när exempelvis någon ändrar personuppgifter i ett verksamhetssystem utan tillstånd.

Med *förlust av personuppgift* avses situationer när personuppgifter går förlorade, exempelvis när en tjänstedator eller tjänstemobil stjäls eller förloras på annat sätt.

Även i det fall det är någon annan slags risk som har identifierats så ska detta anges.

Beskrivning av risk: Beskriv risken som ni har identifierat. Beskrivningen ska inkludera riskens bakgrund, alltså varför den uppstår.

Konsekvenserna av risken för den registrerade: Beskriv hur de registrerade drabbas om risken inträffar. Skadan för den registrerade kan vara fysisk, materiell eller immateriell/moralisk.

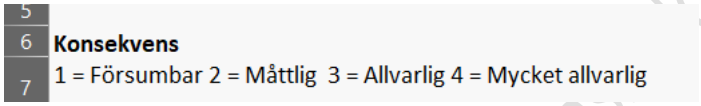
Konsekvens: Ange om ni bedömer att konsekvensen av risken är försumbar (=1), måttlig (=2), allvarlig (=3) eller mycket allvarlig (=4). Tänk på att konsekvensen för den registrerade i regel blir allvarligare om behandlingen avser exempelvis känsliga eller extra skyddsvärda personuppgifter.

Med *försumbar* risk avses att konsekvensen är sådan att de registrerade inte är påverkade eller att de kan stöta på problem som de lätt klarar sig igenom. Exempelvis tillfällig huvudvärk (fysisk skada), mottagande av skräppost (materiell skada) eller smärre tidsförlust t.ex. genom att behöva lägga ner tid på att skriva in information (moralisk skada).

Med *måttlig* risk avses att konsekvensen är sådan att de registrerade kan påverkas med tydliga besvär men som de kan komma över trots vissa svårigheter. Exempelvis mindre fysiska besvär eller stress (fysisk skada), nekad tillgång till digitala administrativa tjänster eller extra kostnader (materiell skada), eller känsla av intrång i privatlivet eller rädsla (moralisk skada).

Med *allvarlig* risk avses att konsekvensen är sådan att de registrerade kan stöta på betydande problem/konsekvenser men som de bör kunna klara sig igenom, även om det sker med betydande svårigheter. Exempelvis allvarlig fysisk påverkan som orsakar långvariga problem (fysisk skada), förlust av bostad eller arbete eller skador på egendom (materiell skada), eller allvarliga psykiska problem såsom depression och fobier (moralisk skada).

Med *mycket allvarlig* risk avses att konsekvensen är sådan att de registrerade kan stöta på betydande eller till och med bestående konsekvenser som de inte nödvändigtvis klarar sig igenom. Exempelvis permanent funktionsnedsättning (fysisk skada), förlust av vital infrastruktur såsom vatten eller el (materiell skada) eller förlust av familjeband, ekonomisk oro, långsiktiga psykologiska besvär etc. (moralisk skada).



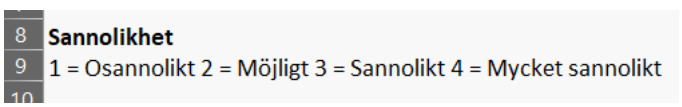
Sannolikhet: Ange om ni bedömer att det är osannolikt (=1), möjligt (=2), sannolikt (=3) eller mycket sannolikt (=4) att den identifierade risken inträffar.

Med en *osannolik* risk avses situationer när det verkar mycket osannolikt att den identifierade risken skulle förverkligas i den aktuella situationen. Exempelvis när åtkomst till en databas via det öppna nätet är möjlig men kräver stark autentisering, eller stöld av dokument förvarade i ett rum som skyddas av både kortläsare och åtkomstkod.

Med en *möjlig* risk avses situationer när det verkar osannolikt att den identifierade risken skulle förverkligas i den aktuella situationen. Exempelvis när åtkomst till databasen via det öppna nätet är möjlig men lösenordet är svagt, eller stöld av dokument som är förvarade i ett rum skyddat av en kortläsare.

Med *sannolik* risk avses situationer när det verkar sannolikt att den identifierade risken kommer att förverkligas i den aktuella situationen. Exempelvis när databasen är helt öppen i det öppna nätet men databasen kan inte hittas med sökmotorer, eller stöld av dokument förvarade på kontor som inte kan nås utan att först ha passerat och kontrollerats i receptionen.

Med *mycket sannolik* risk avser situationer när det verkar mycket sannolikt att den identifierade risken kommer att förverkligas i den aktuella situationen. Exempelvis när databasen är helt öppen i det öppna nätet och hittas med sökmotorer, eller stöld av dokument som förvaras i en lobby.



Riskvärde: Multiplicera sannolikheten med konsekvensen och det resultat som ni får är riskvärdet.

Vidtagna skyddsåtgärder: Beskriv den eller de åtgärder som vidtas för att minimera risken.

Konsekvens efter åtgärd: Beakta vidtagna skyddsåtgärder och bedöm på nytt om ni anser att konsekvensen av risken är försumbar (=1), måttlig (=2), allvarlig (=3) eller mycket allvarlig (=4).

Sannolikhet efter åtgärd: Beakta vidtagna skyddsåtgärder och bedöm på nytt om ni anser att det är osannolikt (=1), möjligt (=2), sannolikt (=3) eller - mycket sannolikt (=4) att den identifierade risken inträffar.

Riskvärde efter åtgärd: Multiplicera sannolikheten efter åtgärd med konsekvensen efter åtgärd och det resultat som ni får är riskvärdet efter åtgärd.

Uppföljning av vidtagna åtgärder ska göras: Ange hur ni planerar att följa upp vidtagna åtgärder för att säkerställa att åtgärderna ger önskat resultat.

Riskvärde	Vidtagna skyddsåtgärder	Konsekvens efter åtgärd	Sannolikhet efter åtgärd	Riskvärde efter åtgärder	Uppföljning av vidtagna åtgärder ska göras
2		2	1	2	
4		3	1	3	
9		3	2	6	
12		3	3	9	

Sammanställning av risker och Fortsatta åtgärder i ”DSE Riskbedömningsmall”

Sammanställning av risker: De risker som ni har beskrivit och bedömt i filens första blad ”Riskbedömning” sammanställs här för att tydliggöra vilka risker som sedan ska flyttas över till mallen (se mer information nedan under ”*Hur ni fyller i mallen”)*

Fortsatta åtgärder: Detta blad kan ni använda för att sammanställa och tydliggöra den konkreta plan som behöver vidtas för att genomföra de åtgärder som ni har identifierat är nödvändiga för att minska riskerna. Denna del är frivillig att fylla i och utgör alltså inte en obligatorisk del av själva konsekvensbedömningen. Det är dock obligatoriskt att genomföra de åtgärder som ni har bedömt vara nödvändiga, varför detta kan vara ett hjälpsamt verktyg i den processen. Här kan ni tydliggöra tidplan för åtgärderna, fördela ansvar och ange hur uppföljningen ska ske.

Hur ni fyller i mallen

I detta avsnitt ska ni utgå från de uppgifter som ni dokumenterat i excelfilen ”DSE Riskbedömningsmall” och i tabellen ange samtliga medelhöga och höga risker som har ett riskvärde mellan 6–16 efter åtgärder. En sammanställning av identifierade risker finns i bladet ”**Sammanställning av risker**” i excelfilen.

Förslagsvis kan ni kopiera den text som ni skrivit in i excelfilen avseende beskrivning av risk och vidtagna skyddsåtgärder.

Exempel

Risk-ID	Beskrivning av risk	Vidtagna skyddsåtgärder	Nytt risk-värde
R8	Risk för obehörigt röjande av personuppgifter pga. otillräckliga organisatoriska säkerhetsåtgärder när e-postmeddelande används.	Organisatoriska åtgärder i form av rutiner för hantering av känsliga personuppgifter, extra skyddsvärda personuppgifter eller sekretesskyddade uppgifter i e-post införs. Rutinen kompletteras med utbildning till aktuella befattningar.	6
R9	Risk för obehörigt röjande av personuppgifter pga. otillräckliga tekniska säkerhetsåtgärder när e-postmeddelande används.	Standardkryptering i form av TLS 1.2 kompletteras med extra kryptering vid e-postmeddelande innehållande känsliga personuppgifter, extra skyddsvärda personuppgifter eller sekretesskyddade uppgifter.	8
			Lägg till fler rader vid behov

5.2.1 Riskmatris

En riskmatris används för att illustrera och synliggöra risker, i det här fallet med en personuppgiftsbehandling. I riskmatrisen ger sannolikheten multiplicerat med konsekvensen riskvärdet. När risken är placerad på en nivå som anges med röd färg är risknivån mycket hög. När risknivån anges med orange färg är den hög. Risknivån minskar stegvis och när risknivån anges med grön färg är den låg.

I de fall risken, även efter det att skyddsåtgärder vidtagits, fortfarande ligger på en nivå som anges med röd eller orange färg finns det skäl att inleda förhandssamråd.

I detta avsnitt finns det alltså inget för er att fylla i utan matrisen illustrerar risknivå och riskvärde beroende på hur ni bedömer riskerna med behandlingen.

KONSEKVENS	Mycket allvarlig	4	8	12	16
	Allvarlig	3	6	9	12
	Måttlig	2	4	6	8
	Försumbar	1	2	3	4
		Osannolikt	Möjligt	Sannolikt	Mycket sannolikt
SANNOLIKHET					

5.3 Samlad bedömning av risker och åtgärder

Hur ni fyller i mallen

I detta avsnitt ska ni ge en samlad bedömning av risker och åtgärder för behandlingen/behandlingarna. Syftet är att ge en samlad och översiktlig bild över de risker som har identifierats med behandlingen/behandlingarna och de åtgärder som ni har vidtagit eller beslutat er för att vidta. Vid behov motivera gärna de valda åtgärderna.

Exempel

- ✓ Riskbedömning visar att endast två risker kvarstår med högt riskvärde efter vidtagna skyddsåtgärder. Övriga risker har ett lågt riskvärde mellan 1–3. De två risker som kvarstår trots vidtagna skyddsåtgärder har båda fått ett riskvärde på 6. Avsaknaden av möjligheten att pseudonymisera personuppgifter i det system där behandlingen sker medför att risken för de registrerade är fortsatt hög vid ett eventuellt dataintrång trots införande av tvåfaktorsautentisering. Då det inte heller finns möjlighet att införa automatiserad säkerhetskopiering i systemet riskerar personuppgifter att gå förlorade vid oförutsedda avbrott om den manuella säkerhetskopieringen glöms bort. Även om riskvärdet sänkts genom åtgärden att införa en rutin om manuell säkerhetskopiering bedöms fortfarande risken vara relativt hög.

5.3.1 Kvarstående höga risker?

Hur ni fyller i mallen

I detta avsnitt ska ni ange om det finns kvarstående höga risker med behandlingen trots att åtgärder vidtagits. Hänvisa även till risk-id. Syftet med att ange eventuella kvarstående risker här är att det ska bli extra tydligt vilka risker som ska beaktas vid bedömningen av vilket steg som ska tas härnäst (punkt 7.2 i konsekvensbedömningen).

Exempel

- ✓ R4 Avsaknaden av möjligheten att pseudonymisera personuppgifter.
- ✓ R7 Avsaknaden av möjligheten att införa automatiserad säkerhetskopiering.

5.3.2 Förhandssamråd

Om höga risker kvarstår för de registrerade (riskvärde 8 – 16), trots att åtgärder för att avhjälpa dessa har vidtagits, ska den personuppgiftsansvarige begära förhandssamråd hos IMY innan behandlingen/behandlingarna kan påbörjas. Ett beslut om att begära förhandssamråd eller att inte begära förhandssamråd behöver fattas av behörig person i förvaltningen/bolaget, se avsnitt 7.1.

Den personuppgiftsansvarige ska i sin begäran om förhandssamråd beskriva de kvarstående höga riskerna i behandlingen och varför dessa inte har kunnat åtgärdas. Därefter kan IMY antingen välja att ge skriftliga råd om hur den personuppgiftsansvarige kan gå vidare med behandlingen eller förbjuda behandlingen.

Bestämmelser om förhandssamråd finns i artikel 36 GDPR. Tillvägagångssätt för att begära förhandssamråd finns på IMY:s hemsida.

Hur ni fyller i mallen

I denna del ska ni bedöma om ni behöver begära förhandssamråd med IMY eller inte. Bedömningen gör ni utifrån om de höga riskerna för de registrerade har kunnat avhjälpas och därmed minskas till en acceptabel nivå eller om de kvarstår trots de åtgärder ni vidtagit. Var tydliga i er bedömning, så att läsaren förstår hur ni har resonerat. Beslut fattas i avsnitt 7.1.

Exempel

- ✓ Eftersom det kvarstår höga risker för de registrerade, trots att åtgärder för att avhjälpa dessa har vidtagits, görs bedömningen att förhandssamråd med tillsynsmyndigheten bör begäras.
- ✓ Eftersom riskerna med behandlingen har kunnat avhjälpas genom vidtagna åtgärder, görs bedömningen att förhandssamråd med tillsynsmyndigheten inte behöver begäras.

6 Medverkan från berörda parter

6.1 Kommentarer/rekommendationer från dataskyddsombudet

Vid genomförandet av en konsekvensbedömning ska den personuppgiftsansvarige alltid rådfråga sitt dataskyddsombud. Dataskyddsombudet ska även som en del i sitt arbete övervaka genomförandet av konsekvensbedömningen på förfrågan av den personuppgiftsansvarige.

Bestämmelser om involverande av dataskyddsombud finns i artikel 35.2 och 39.1 c GDPR.

Hur ni fyller i mallen

Vid genomförandet av konsekvensbedömningen ska ni involvera och rådfråga dataskyddsombudet. De råd som dataskyddsombudet ger ska biläggas till det här avsnittet. Om dataskyddsombudet skrivit en sammanfattning i sin rekommendation kan ni med fördel klippa in sammanfattningen under den här punkten.

Exempel

- ✓ I bilaga X finns dataskyddsombudets rekommendation i sin helhet. Nedan är dataskyddsombudets sammanfattning inklippt från rekommendationen i bilaga X:

  Dataskyddsombudets sammanfattade rekommendationer:
  Säkerställ laglig grund för tredjelandsöverföring till USA.
  Utred kvarstående risker kopplat till X.

6.2 Synpunkter från de registrerade

När det är lämpligt ska den personuppgiftsansvariga inhämta synpunkter från de registrerade eller deras företrädare om behandlingen. Detta kan ske t.ex. genom att tillfråga facket om behandlingen rör anställda, enkät till kunder eller relevanta intresseorganisationer.

Genom inhämtande av synpunkter från de registrerade är det möjligt för er som personuppgiftsansvariga att bedöma eventuella risker och konsekvenser som de registrerade ser med den planerade behandlingen. Det är en möjlighet för den personuppgiftsansvarige att på förhand undvika missförstånd gällande behandlingen. Om den personuppgiftsansvariges beslut skiljer sig från de registrerades synpunkter ska skälen för att gå vidare med behandlingen, alternativt stoppa påbörjandet av behandlingen, dokumenteras.

Om ni som personuppgiftsansvarig inte inhämtar synpunkter från registrerade ska det dokumenteras och motiveras i konsekvensbedömningen.

Bestämmelse om inhämtande av registrerades synpunkter finns i artikel 35.9 GDPR.

Hur ni fyller i mallen

Under den här punkten ska ni redogöra för de registrerades synpunkter. Om den personuppgiftsansvariges beslut gällande att gå vidare med behandlingen skiljer sig från de registrerades synpunkter ska skälen för ert beslut redogöras för under den här punkten.

Om ni valt att inte inhämta synpunkter från de registrerade ska skälen för det dokumenteras under den här punkten.

Exempel

- ✓ I bilaga Z ser ni sammanställningen av de registrerades synpunkter. De registrerades synpunkter avviker inte i någon större omfattning från bolagets.

7 Avslut

7.1 Beslut

Hur ni fyller i mallen

Här beskriver ni det beslut som fattats gällande behandlingen/behandlingarna utifrån det underlag som presenterats i konsekvensbedömningen. Ni ska även ange vem som fattat beslutet och i vilken roll som denne har gjort det.

Exempel

- ✓ Bolaget B beslutar att behandlingen/behandlingarna kan genomföras då några kvarstående höga risker inte föreligger. Beslutat av Anna Andersson, HR-chef xxxx-xx-xx
- ✓ A-förvaltningen beslutar att begära förhandssamråd eftersom höga risker kvarstår, trots vidtagna åtgärder. Beslutet fattas av Kim Karlsson, avdelningschef, xxxx-xx-xx

7.2 Nästa steg

Hur ni fyller i mallen

När ni fattat ett beslut ska ni förklara hur ni går vidare. Om ni under avsnitt 7.1 har beslutat att ett förhandssamråd ska genomföras beskriver ni här de nästa

stegen ni vidtar i form av ifyllande begäran av förhandssamråd och vem som ansvarar för det.

Om beslutet i 7.1 innebär att behandlingarna kan genomföras efter åtgärder ska konsekvensbedömningen diarieföras. En handlingsplan för de identifierade åtgärderna som ska vidtas bör även tas fram.

Exempel

- ✓ Denna version av konsekvensbedömningen diarieförs med diarienummer xx/xxxx. En handlingsplan för identifierade åtgärder tas fram innan behandlingen påbörjas. Ansvarig för detta är Anna Andersson.

8 Bilagor

Hur ni fyller i mallen

Om er konsekvensbedömning innehåller flera bilagor rekommenderas ni att under den här punkten skriva en förteckning över samtliga bilagor för att undvika att någon bilaga faller bort. Glöm sedan inte att bilägga dokumenten!

Exempel

Bilaga 1 – Personuppgiftsbiträdesavtal Företag X
Bilaga 2 – Dataskyddsombudets rekommendation
Bilaga 3 – Synpunkter från de registrerade

Glöm inte att uppdatera innehållsförteckningen i konsekvensbedömningen efter att ni har fyllt i mallen.

Mallstöd framtaget av dataskyddsenheten
Telefon: 031-365 00 00 (kontaktcenter)
E-post: dso@intraservice.goteborg.se