# Mall för Konsekvensbedömning avseende dataskydd enligt art. 35 GDPR

(Ange system, tjänst, program eller art av personuppgiftsbehandling)

**Mallen**

En mall för konsekvensbedömning togs ursprungligen framtagen maj 2022 av Kompetenscenter välfärdsteknik på Sveriges Kommuner och Regioner (SKR), denna mall bygger på denna. Mallen får fritt användas och anpassas till verksamhetens egna rutiner för konsekvensbedömningar.

Innehåll

[Mall för Konsekvensbedömning avseende dataskydd enligt art. 35 GDPR 1](#_Toc158802661)

[1 Övergripande information om behandlingen 4](#_Toc158802662)

[1.1 Personuppgiftsansvarig(a) för personuppgiftsbehandlingen 4](#_Toc158802663)

[1.2 Kontaktuppgifter till dataskyddsombud 4](#_Toc158802664)

[1.3 Ansvarig(a) för konsekvensbedömningen 4](#_Toc158802665)

[**1.3.1** Genomförande 4](#_Toc158802666)

[**1.3.2** Förvaltning 4](#_Toc158802667)

[1.4 Projektinformation 4](#_Toc158802668)

[1.5 Systeminformation 4](#_Toc158802669)

[1.6 Kortfattad beskrivning av personuppgiftsbehandlingen 5](#_Toc158802670)

[1.7 Personuppgiftsbehandlingens effektmål 5](#_Toc158802671)

[1.8 Extern samverkan 5](#_Toc158802672)

[2 Systematisk beskrivning av personuppgiftsbehandlingen 6](#_Toc158802673)

[2.1 Beskrivning av behandlingar 6](#_Toc158802674)

[2.2 Översiktlig beskrivning av personuppgiftsflödet 7](#_Toc158802675)

[2.3 Ny, innovativ eller kontroversiell personuppgiftsbehandling 7](#_Toc158802676)

[2.4 Behandlingens omfattning 7](#_Toc158802677)

[**2.4.1** Känsliga personuppgifter 7](#_Toc158802678)

[**2.4.2** Mängd registrerade 7](#_Toc158802679)

[**2.4.3** Antalet personuppgifter 8](#_Toc158802680)

[**2.4.4** Behandlingens geografiska räckvidd 8](#_Toc158802681)

[**2.4.5** Nödvändiga informationstillgångar 8](#_Toc158802682)

[2.5 Finns uppförandekoder 8](#_Toc158802683)

[2.6 Den registrerades kontroll över sina personuppgifter 8](#_Toc158802684)

[3 Uppfyllnad av grundläggande dataskyddsprinciper 9](#_Toc158802685)

[3.1 Laglighet 9](#_Toc158802686)

[3.2 Ändamål 9](#_Toc158802687)

[**3.2.1** Andra lämpliga sätt att uppnå ändamålet 9](#_Toc158802688)

[**3.2.2** Nödvändighet 9](#_Toc158802689)

[**3.2.3** Ändamålsglidning 10](#_Toc158802690)

[3.3 Uppgiftsminimering 10](#_Toc158802691)

[3.4 Lagringsminimering 10](#_Toc158802692)

[4 Åtgärder som stärker den registrerades rättigheter 11](#_Toc158802693)

[4.1 Information till den registrerade (art. 12, 13 och 14 GDPR) 11](#_Toc158802694)

[4.2 Rätt till tillgång (registerutdrag) (art. 15 GDPR) 11](#_Toc158802695)

[4.3 Rätt till dataportabilitet (art. 20 GDPR) 11](#_Toc158802696)

[4.4 Rätt till rättelse (art. 16 och 19 GDPR) 11](#_Toc158802697)

[4.5 Rätt till radering (art. 17 och 19 GDPR) 11](#_Toc158802698)

[4.6 Rätt att göra invändningar och rätt till begränsning av personuppgiftsbehandling (art. 18, 19 och 21 GDPR) 12](#_Toc158802699)

[4.7 Tredjelandsöverföring (kap. 5 GDPR) 12](#_Toc158802700)

[**4.7.1** Beskrivning och skyddsåtgärder 12](#_Toc158802701)

[4.8 Medverkan från berörda parter 13](#_Toc158802702)

[**4.8.1** Synpunkter från registrerade 13](#_Toc158802703)

[**4.8.2** PERSONUPPGIFTSBITRÄDEN, specialister etc. 13](#_Toc158802704)

[5 Risker och riskreducerande åtgärder 14](#_Toc158802705)

[5.1 Riskdokumentation 14](#_Toc158802706)

[5.2 Kvarstående höga risker 14](#_Toc158802707)

[6 Rådfrågan, slutlig bedömning och godkännande 15](#_Toc158802708)

[6.1 Dataskyddssamordnarens (motsvarande) utlåtande 15](#_Toc158802709)

[6.2 Dataskyddsombudet bedömning och rekommendationer 15](#_Toc158802710)

[6.3 Sammantagen bedömning 15](#_Toc158802711)

# Övergripande information om behandlingen

## Personuppgiftsansvarig(a) för personuppgiftsbehandlingen

|  |
| --- |
|   |

## Kontaktuppgifter till dataskyddsombud

|  |
| --- |
|  |

## Ansvarig(a) för konsekvensbedömningen

### Genomförande

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

|  |
| --- |
|  |

### Förvaltning

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

|  |
| --- |
|  |

## Projektinformation

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

|  |
| --- |
|  |

## Systeminformation

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

|  |
| --- |
|  |

## Kortfattad beskrivning av personuppgiftsbehandlingen

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

|  |
| --- |
|  |

## Personuppgiftsbehandlingens effektmål

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

Beskriv vilka förväntade effekter behandlingen kommer att få för verksamheten och i ett bredare perspektiv, exempelvis för vård- och omsorg i ett regionalt eller nationellt perspektiv.

|  |
| --- |
|  |

## Extern samverkan

Om konsekvensbedömningen ska genomföras inom ramen för ett större projekt eller ett program ska ansvarig förvaltningschef (motsvarande) rådfrågas avseende genomförande, resurssättning och behov av externa resurser.

|  |  |
| --- | --- |
|  |  |
| Förvaltningschef (motsvarande) har rådfrågats | [ ]  |
| Ej tillämplig för denna konsekvensbedömning | [ ]  |
|  |  |

# Systematisk beskrivning av personuppgiftsbehandlingen

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

## Beskrivning av behandlingar

Att tänka på: Hur samlas personuppgifter in, används, lagras och raderas? Vad är källan till personuppgifterna? Är det ”personuppgifter” per definition enligt GDPR? Kommer personuppgifterna att delas med någon? Finns personuppgiftsbiträden? Är det en molntjänst? Det kan vara användbart att referera till ett flödesdiagram eller annat sätt att beskriva dataflöden (se nedan). Ändamål: Vad ska uppnås med behandlingen?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Personuppgifts-behandling (typ av behandlingar) | Ändamål | Personuppgifter | Person-uppgifts-biträde | Kategorier av registrerade | Insamling | Externa mottagare | Lagring/lagringstid | Radering/arkivering |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |

## Översiktlig beskrivning av personuppgiftsflödet

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

**[Bild]**

|  |
| --- |
| [Kommentar] |

## Ny, innovativ eller kontroversiell personuppgiftsbehandling

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

|  |
| --- |
|  |

## Behandlingens omfattning

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

### Känsliga personuppgifter

Utgå från svaren i avsnitt 5.1 och sammanfatta vilka känsliga personuppgifter (art. 9 GDPR) eller andra integritetskänsliga eller särskilt skyddsvärda personuppgifter (art. 10 och 87 GDPR) som behandlas**.[[1]](#footnote-1)**

|  |
| --- |
|  |

### Mängd registrerade

Uppskatta hur många registrerade som kommer att påverkas av personuppgiftsbehandlingen.

|  |
| --- |
|  |

### Antalet personuppgifter

Ange hur många personuppgifter som uppskattningsvis kommer att behandlas.

|  |
| --- |
|  |

### Behandlingens geografiska räckvidd

Beskriv personuppgiftbehandlingens geografiska räckvidd.

|  |
| --- |
|  |

### Nödvändiga informationstillgångar

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

|  |
| --- |
|  |

## Finns uppförandekoder

|  |
| --- |
|  |

## Den registrerades kontroll över sina personuppgifter

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

|  |
| --- |
|  |

# Uppfyllnad av grundläggande dataskyddsprinciper

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

Bedömningen innefattar en behovs- och proportionalitetsbedömning enligt följande:

Vilken är den rättsliga grunden för behandlingen?

Uppnår behandlingen faktiskt syftet?

Finns det ett annat sätt att uppnå samma resultat?

Hur undviks ”ändamålsglidningar”?

Hur säkerställs datakvalitet och uppgiftsminimering?

## Laglighet

Ange vilken rättslig grund som behandlingen stödjer sig på (art. 6 GDPR).[[2]](#footnote-2) Förekommer flera behandlingar med olika rättsliga grunder behöver det framgå tydligt vilken rättslig grund som gäller för respektive personuppgiftsbehandling.

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

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

## Ändamål

### Andra lämpliga sätt att uppnå ändamålet

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

|  |
| --- |
|  |

### Nödvändighet

Om behandlingen bygger på en annan rättslig grund än samtycke, beskriv varför den planerade behandlingen är nödvändig för att uppnå ändamålet samt varför man valt detta sätt att uppnå ändamålet snarare än något av de andra lämpliga sätten som beskrivits i 3.2.1.

Om den planerade behandlingen bygger på den rättsliga grunden samtycke, beskriv varför den planerade personuppgiftsbehandlingen har valts samt varför man valt detta sätt att uppnå ändamålet snarare än något av de andra lämpliga sätten som beskrivits i 3.2.1.

|  |
| --- |
|  |

### Ändamålsglidning

Beskriv hur ändamålsglidning motverkas**.**

|  |
| --- |
|  |

## Uppgiftsminimering

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

|  |
| --- |
|  |

## Lagringsminimering

Ange hur det tekniskt och organisatoriskt säkerställs att personuppgifter endast lagras så länge de behövs.**[[3]](#footnote-3)**

|  |
| --- |
|  |

# Åtgärder som stärker den registrerades rättigheter

I detta avsnitt ska effektiva åtgärder som vidtagits för att stärka den registrerades rättigheter dokumenteras (art. 12–23 och art. 34 GDPR). Åtgärderna kan vara organisatoriska, som framtagande av en rutin för handläggning och att utse ansvariga, och tekniska, t. ex. att alla personuppgifter i ett system går att utsöka.

För att åtgärderna ska kunna anses vara effektiva ska de utgå från behandlingen och dess ändamål (art. 35.7 b GDPR).

Avsnittet berör följande frågor:

Vilken information kommer personuppgiftsansvarig att ge individer?

På vilket sätt? Hur ska deras rättigheter främjas?

Vilka åtgärder ska vidtas för att säkerställa att personuppgiftsbiträden följer vidtagna åtgärder om dataskydd?

Hur ska överföringar av personuppgifter till andra länder skyddas?

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

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

|  |
| --- |
|  |

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

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

|  |
| --- |
|  |

## Rätt till dataportabilitet (art. 20 GDPR)

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

|  |
| --- |
|  |

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

Ange hur den registrerades rätt till rättelse säkerställs.

|  |
| --- |
|  |

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

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

|  |
| --- |
|  |

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

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

|  |
| --- |
|  |

## Tredjelandsöverföring (kap. 5 GDPR)

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

### Beskrivning och skyddsåtgärder

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| Personuppgifts-behandling | Beskrivning av tredjelandsöverföring | Överföringsmekanism  | Motivering av skyddsåtgärd(er) och tillämplighet[[4]](#footnote-4) |
| [Exempel: support, diagnostiska data, regulatoriska krav, marknadsföring etc] |  | Exempel: adekvansbeslut av kommissionen, standardavtalsklausuler, art. 49.1-undantag] |  |
|  |  |  |  |
|  |  |  |  |
|  |

## Medverkan från berörda parter

### Synpunkter från registrerade

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

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

|  |
| --- |
|  |

### PERSONUPPGIFTSBITRÄDEN, specialister etc.

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

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

|  |
| --- |
|  |

# Risker och riskreducerande åtgärder

## Riskdokumentation

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

|  |
| --- |
| [Hänvisning och kommentar] |

## Kvarstående höga risker

Dokumentera de risker från riskbedömningsdelen av konsekvensbedömningen som är fortsatt höga (riskvärde 8 eller högre om en tio-gradig skala används – 5 sannolikhet – 5 konsekvens) efter att riskreducerande åtgärder har vidtagits.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Riskscenario (hot, aktör och konsekvenser) | Riskens ursprung (sårbarhet, orsak) | Riskreducerande åtgärder | Eventuella krav fastställda av kommunen | Riskvärde efter åtgärder | Kommentar |
|  |  |  |  |  | [Hög alt. 8-10] |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |

# Rådfrågan, slutlig bedömning och godkännande

## Dataskyddssamordnarens (motsvarande) utlåtande

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

|  |
| --- |
|  |
|  |

## Dataskyddsombudet bedömning och rekommendationer

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

|  |
| --- |
|  |

## Sammantagen bedömning

De som genomfört konsekvensbedömningen ska skriva en sammantagen bedömning med rekommendationer (som också sammanfattas under avsnitt 1)

|  |
| --- |
| [Sammantagen bedömning och rekommendation] |

|  |  |  |
| --- | --- | --- |
| **Intressenter/saken**  | **Namn/datum** | **Anteckningar** |
| Dataskyddsombudet har rådfrågats: |  | [Dataskyddsombud ska rådfrågas om rättsliga krav, åtgärder som minskar risker och om behandlingen är tillåten.] |
| Dataskyddsombudets rekommendationer godtogs inte: |  | [Förklara nedan varför ansvarig chef, nämnd (motsvarande) gått emot dataskyddsombudets rekommendation/er.] |
| Motivering varför dataskyddsombudets rekommendationer inte godtagits: |
| Genomförare (se avsnitt 3.3.1): |  |  |
|  Genomförarnas rekommendationer: |
| Samråd med andra intressenter granskade och beaktade av: |  | [Om ett beslut avviker från t.ex. registrerades synpunkter ska skälen redovisas här.] |
| Skäl för beslut som avviker från intressenters synpunkter: |
| Gå vidare med personuppgiftsbehandlingen (JA/NEJ), beslutad av: |  | [Om kvarstående sannolika höga risker finns innebär ett JA att begära förhandssamråd hos IMY] |
| Motivering: |

1. I art. 9 GDPR definieras känsliga personuppgifter som följande: ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Med integritetskänsliga och särskilt skyddsvärda personuppgifter avses bland annat personnummer eller andra nationella identifikationsnummer, uppgifter om lagöverträdelser och uppgifter om någons privatliv. [↑](#footnote-ref-1)
2. Vägledning om de rättsliga grunderna finns på IMY:s webbplats: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/ [↑](#footnote-ref-2)
3. Se kommunens regelverk för bevarande och gallring eller kontakta arkivarie. [↑](#footnote-ref-3)
4. Se EDPB:s vägledning för val och bedömning av skyddsåtgärder för att uppnå lagenlig tredjelandsöverföring: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer\_en [↑](#footnote-ref-4)