Dnr

|  |
| --- |
| KI-Logo_pos_RGB(136-0-82) Datum |
|  |
|  |

# 

# Mall för konsekvensbedömning avseende dataskydd

Till denna mall finns Anvisningar för konsekvensbedömning avseende dataskydd. I anvisningarna beskrivs vad en konsekvensbedömning är, om och när en sådan ska göras och hur den ska genomföras.

**Projekt/ärende**

**Medverkande**

|  |  |  |
| --- | --- | --- |
| ***Namn*** | ***Kontaktuppgifter  (e-post/mobilnr)*** | ***Roll*** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Dataskyddsombudet har rådfrågats

Dataskyddsombudets eventuella kommentar:

**1. Beskriv personuppgiftsbehandlingen och dess syfte**

Fyll här i en kort beskrivning av personuppgiftsbehandlingen och syftet med den, dvs. vad ni vill uppnå med behandlingen, vilka personuppgifter som behandlas, var personuppgifterna kommer lagras/sparas och hur länge samt om någon person/organisation som inte hör till KI ska ta del av uppgifterna.

Klicka eller tryck här för att ange text.

**2. Beskriv omfattningen av personuppgiftsbehandlingen**

Redogör för vilka personuppgifter som kommer att behandlas, om det är känsliga personuppgifter eller personuppgifter som rör lagöverträdelser, hur många registrerade det är fråga om, hur länge behandlingen planeras pågå samt om det finns anledning anta att den registrerade är i ett underläge eller i beroendeställning och därmed mer sårbar.

Klicka eller tryck här för att ange text.

**3. Bedöm om personuppgiftsbehandlingen är nödvändig och proportionell i förhållande till syftet**

Ange den rättsliga grunden för behandlingen. Vid behandling för forskningsändamål är den rättsliga grunden *nödvändig behandling för att utföra en uppgift av allmänt* intresse. Beskriv om behandlingen är nödvändig för ändamålet eller om det finns andra sätt att nå syftet. Redogör också för hur kvaliteten i data och lagrings- och uppgiftsminimering säkerställs.

Klicka eller tryck här för att ange text.

## 4. Riskhantering

Dokumentera **risker** och vilka tekniska eller organisatoriska **åtgärder** som vidtas för att minimera respektive identifierad risk under detta steg. Tänk på att särskilt beakta risker som avser den registrerades integritetsintresse, förtroende och fri- och rättigheter.

Riskhanteringen kan dokumenteras här i mallen eller i separat bilaga. Om bilaga används, ange detta*.*

### Riskbedömning

Fundera kring vilka risker personuppgiftsbehandlingen innebär och vad som är acceptabel risknivå utifrån kombination av konsekvens och sannolikhet.

Exempel på risker:

Att personuppgifter röjs för obehöriga

Dataintrång

Oavsiktlig radering, förvanskning,

Översvämning

Exempel på konsekvenser:

Enskildas integritet blir kränkt

Förtroendet för KI skadas

### Konsekvens

| **Påverkansgrad** | **Värde** | **Definition** | **Ev. egen definition** |
| --- | --- | --- | --- |
| Allvarlig | 4 | Registrerade kan påverkas på ett allvarligt sätt. |  |
| Kännbar | 3 | Registrerade kan påverkas på ett kännbart sätt. |  |
| Lindrig | 2 | Eventuell påverkan bedöms vara lindrig |  |
| Försumbar | 1 | Konsekvensen bedöms vara försumbar för de registrerade. |  |

### Sannolikhet

| **Sannolikhetsgrad** | **Värde** | **Definition** | **Ev. egen definition** |
| --- | --- | --- | --- |
| Stor | 4 | Mycket troligt att det inträffar, bara en tidsfråga när. |  |
| Viss | 3 | Troligt att det inträffar. |  |
| Liten | 2 | Mindre troligt att det inträffar. |  |
| Mycket liten | 1 | Det är inte troligt att det inträffar. |  |

### Riskmatris

| **Konsekvens** |
| --- |
| **Allvarlig** | **4** |  |  |  |  |
| **Kännbar** | **3** |  |  |  |  |
| **Lindrig** | **2** |  |  |  |  |
| **Försumbar** | **1** |  |  |  |  |
|  |  | **1** | **2** | **3** | **4** |
| **Sannolikhet** |  | **Mkt liten** | **Liten** | **Viss** | **Stor** |

En specifik bedömning ska göras vid varje konsekvensbedömning avseende dataskydd men generellt kan risker i det gröna området accepteras men risker i det röda området måste elimineras innan KI kan utföra personuppgiftsbehandlingen.

| **Risk**   Beskrivning, orsak och konsekvens | Sannolikhet | Konsekvens | **Hantering av risk**  Acceptera  Begränsa  Eliminera |
| --- | --- | --- | --- |
| (1–4) | (1–4) |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| … |  |  |  |

### Åtgärder

Efter viktning av sannolikhet och konsekvens kan bedömningen bli att en risk inte kan accepteras men kan begränsas eller elimineras genom att åtgärder vidtas. Exempel på åtgärder (tekniska och organisatoriska) som kan användas för att hantera risker och skydda de registrerade.

* autentisering
* kryptering
* logg över vem som använder personuppgifter
* stöd för säkerhetskopiering
* pseudonymisering av personuppgifter
* minska antalet personer som har tillgång till uppgifterna
* begränsa sökbegreppen så att det inte går att söka på känsliga personuppgifter
* införa automatisk borttagning av personuppgifter som inte längre ska behandlas (om de inte ingår i allmänna handlingar som ska bevaras)
* utforma IT-systemen så att inte fler personuppgifter än nödvändigt behandlas, dvs. inbyggt dataskydd och dataskydd som standard.

| Risk | Åtgärd för att begränsa eller eliminera risken | Kvarstående risk efter åtgärd |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

**5. Sammanfattande konsekvensbedömning**

Gör en sammanfattande bedömning av personuppgiftsbehandlingen och dess risker utifrån vad som framkommit ovan. Ange om uppföljning av åtgärder eller förnyad bedömning behöver ske och i så fall när. (Till exempel vid införande av nytt system för hantering av personuppgifter som planeras att användas tills vidare.)

## Klicka eller tryck här för att ange text.

## 6. Dataskyddsombudet (DSO)

Enligt GDPR ska DSO rådfrågas vid genomförande av en konsekvens-bedömning. Det rekommenderas att DSO kontaktas tidigt i processen. Kontakt kan tas via [dataskyddsombud@ki.se](mailto:dataskyddsombud@ki.se).