# Anvisningar för konsekvensbedömning avseende dataskydd

Dnr 1-282 /2022

Gäller fr.o.m. 2022-03-11

Karolinska Institutet

**Anvisningar för konsekvensbedömning avseende dataskydd**

Dnr 1-282/2022

# INNEHÅLL



| **Diarienummer:** 1-282/2022 | **Dnr föregående version:** - | **Beslutsdatum:** 2022-03-11 | **Giltighetstid:** Fr.o.m. 2022-03-11 och tills vidare |
|---|---|---|---|
| **Beslut:** Avdelningschefen för juridiska avdelningen | | **Dokumenttyp:** Anvisningar | |
| **Handläggs av avdelning/enhet:** Juridiska avdelningen, dataskyddsombudet | | **Beredning med:** Juridiska enheten och informationssäkerhetsfunktionen | |
| **Revidering med avseende på:** Nytt styrdokument | | | |

# 1 Inledning

En konsekvensbedömning ska alltid göras om en behandling av personuppgifter sannolikt leder till en hög risk för enskilda personers fri- och rättigheter[1].

Syftet med en konsekvensbedömning är att förebygga risker innan de uppkommer.

Konsekvensbedömningen är en process för att

- ta reda på vilka risker som finns med att behandla personuppgifterna,
- ta fram rutiner och åtgärder för att bemöta dessa risker,
- visa att KI uppfyller dataskyddsförordningens krav.

# 2 Syfte

Syftet med denna anvisning är att stödja KI:s verksamheter vid genomförandet av en konsekvensbedömning. I anvisningarna beskrivs vad en konsekvensbedömning innebär, om och när en sådan ska göras samt hur den ska genomföras.

Anvisningarna vänder sig till alla som behandlar personuppgifter. I samband med en personuppgiftsbehandling ska verksamheten ta ställning till om en konsekvensbedömning måste göras.

Anvisningarna kompletteras med en mall som kan användas som underlag vid bedömningen.

# 3 Konsekvensbedömning

Börja med att bedöma om behandlingen kan innebära en hög risk för enskilda personers fri- och rättigheter (riskanalys). Bedöms risken vara hög måste en konsekvensbedömning genomföras. I tveksamma fall ska alltid en konsekvensbedömning göras.

Om den som ansvarar för den faktiska personuppgiftsbehandlingen, dvs. den som ansvarar för projektet eller ärendet, anser att riskerna inte är så pass stora att en konsekvensbedömning måste göras, ska det motiveras och dokumenteras på lämpligt sätt.

Risker ska i första hand bedömas utifrån data- och integritetsskyddsaspekter men också från andra grundläggande mänskliga rättigheter såsom yttrande- och åsiktsfrihet, fri rörlighet och förbud mot diskriminering.

[1] Artikel 35 dataskyddsförordningen (GDPR)

Konsekvensbedömningen ska innehålla

- en beskrivning av den planerade personuppgiftsbehandlingen och dess syfte,
- en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftet med behandlingen,
- en bedömning av identifierade risker för de registrerades fri- och rättigheter,
- en beskrivning av de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att dataskyddsförordningen efterlevs, med hänsyn till de registrerade och andra berörda personers rättigheter och berättigade intressen,
- hur en uppföljning av åtgärderna ska göras för att säkerställa att de över tid är effektiva och ändamålsenliga.

En konsekvensbedömning ska dokumenteras. Av dokumentationen ska framgå de ställningstaganden man gjort som motiverar att personuppgiftsbehandlingen kan utföras och eventuella åtgärder som vidtas för att behandlingen ska få utföras.

Om man inte gör en konsekvensbedömning när så krävs, eller när en sådan görs felaktigt, kan KI drabbas av sanktionsavgifter.

## 4 När ska en konsekvensbedömning göras

En konsekvensbedömning ska alltid göras i följande fall.

- Vid behandling i stor omfattning av känsliga personuppgifter, t.ex. genetiska och biometriska uppgifter, uppgifter om hälsa, sexualliv eller sexuell läggning, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, eller av personuppgifter som rör brott eller misstanke om brott.

- Systematisk övervakning av allmän plats i stor omfattning.

- Vid automatiserat individuellt beslutsfattande (även profilering), dvs. användning för att skapa särskilda profiler baserat på personliga aspekter och då dessa profiler används för att fatta automatiserade beslut, t.ex. rekrytering utan personlig kontakt och helt automatiserad antagning.

Med *stor omfattning* menas t.ex. hur många som är registrerade, hur många uppgifter som registreras om varje person, hur länge behandlingen ska pågå eller inom hur stort geografiskt område de registrerade finns.

En konsekvensbedömning ska också göras om den planerade personuppgiftsbehandlingen uppfyller *minst två* av följande kriterier och det är sannolikt att behandlingen leder till en *hög risk*.

- utvärderar eller poängsätter människor
- personuppgifter behandlas i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade

- systematiskt övervakar människor, t.ex. genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer
- behandlar känsliga personuppgifter eller uppgifter som är av mycket personlig karaktär
- behandlar personuppgifter i stor omfattning
- kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, t.ex. när man samkör register
- behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, t.ex. barn, anställda, asylsökande, äldre eller patienter
- använder ny teknik eller nya organisatoriska lösningar, t.ex. applikationer i mobiltelefoner, sakernas Internet (Internet of things) såsom användandet av smarta sensorer

Vid förändringar av personuppgiftsbehandlingen, ska man överväga om man måste genomföra en ny konsekvensbedömning.

## 5 När behöver en konsekvensbedömning inte göras

En konsekvensbedömning behöver inte göras om behandlingen

- sannolikt inte leder till en hög risk för fysiska personers fri- och rättigheter,
- är mycket lik en annan behandling där det redan finns en dokumenterad konsekvensbedömning, dvs. där behandlingen av personuppgifterna, syftet och tillvägagångssättet är mycket lik den andra behandlingen.

Denna bedömning ska dokumenteras inom det projekt eller det ärende det den tillhör.

KI:s dataskyddsombud kan bistå med råd vad gäller konsekvensbedömningen.

## 6 Genomförandet av en konsekvensbedömning

Det finns en Mall för konsekvensbedömning som stöd för bedömningen.

Dokumentationen ska sparas inom det projekt eller det ärende den tillhör. Den som ansvarar för projektet eller ärendet svarar för att konsekvensbedömningen görs.

I bedömningen kan personer som representerar olika kompetenser delta eller rådfrågas för att göra en allsidig bedömning av personuppgiftsbehandlingen, t.ex.

- projektledare
- forskargruppledare (PI) eller av denne utsedd forskare
- dataskyddsansvarig för avdelning eller institution

- it- och informationssäkerhetsansvarig för avdelning eller institution
- informationsägare
- systemägare
- arkivarie
- jurist
- dataskyddsombud

I vissa fall kan det vara lämpligt att inhämta även de registrerades synpunkter. Om det inte är lämpligt, dvs. det skulle vara oproportionerligt, opraktiskt, innebära sekretessbrott eller att syftet med behandlingen förfelas, ska det antecknas i konsekvensbedömningen.