

IMY:s mall för

Bedömning av behovet av konsekvensbedömning enligt dataskyddsförordningen

Motsvarar Steg 1 i *En praktisk guide*

Om mallen

Mallen motsvarar Steg 1 i En praktisk guide. Mallen är tänkt att underlätta för er som personuppgiftsansvariga att på ett strukturerat sätt dokumentera bedömningen av behovet av att genomföra en konsekvensbedömning avseende dataskydd i enlighet med artikel 35 i dataskyddsförordningen¹.

Vid bedömningen av om en konsekvensbedömning är obligatorisk ska den personuppgiftsansvarige utgå från:

- de faktorer som anges i artikel 35.1 i dataskyddsförordningen
- exemplen i artikel 35.3 i dataskyddsförordningen
- IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen (som bygger på kriterierna i EDPB:s riktlinjer om konsekvensbedömning).

Läs mer om bedömningen av behovet av konsekvensbedömning

En praktisk guide: Steg 1

Bilagan Rättsligt tolkningsstöd: avsnitt 4

Allt material finns på imy.se/konsekvensbedomning

Vår webbplats www.imy.se erbjuder översiktlig information om konsekvensbedömningar.

Dokumentation

I mallen är utrymmet för anteckningar begränsat. Om ni har behov av mer utrymme för er dokumentation går det bra att hänvisa till en bilaga.

Kom ihåg!

Det är *typen av behandling* som är relevant när behovet av konsekvensbedömning ska bedömas. Åtgärder som ska reducera eller eliminera risker vid den enskilda planerade behandlingen kan därför inte beaktas vid denna bedömning.

¹ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Övergripande information

Roller	
Ange den personuppgiftsansvarige för den planerade personuppgiftsbehandlingen och vilka roller som deltagit i bedömningen av behovet av att genomföra en konsekvensbedömning.	
Personuppgiftsansvarig	
Personuppgiftsbiträde(n)	
De roller som deltagit i bedömningen	
Ansvarig för bedömningen av behovet av att genomföra en konsekvensbedömning	

Planerad personuppgiftsbehandling
Beskriv övergripande vilken behandling som planeras, exempelvis tjänsten, processen eller systemet som ska implementeras.

Steg 1. Bedöm behovet av att genomföra en konsekvensbedömning

De faktorer som anges i artikel 35.1 i dataskyddsförordningen

Utgå från faktorerna i artikel 35.1 i dataskyddsförordningen när ni avgör om det är en sådan typ av behandling som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, och som innebär att en konsekvensbedömning ska göras.

- Användning av ny teknik
- Behandlingens art
- Behandlingens omfattning
- Behandlingens sammanhang
- Behandlingens ändamål

Läs mer om faktorernas innebörd i bilagan Rättsligt tolkningsstöd – avsnitt 4.1.

Fråga: Finns det redan med hänsyn till dessa faktorer något som talar för att en konsekvensbedömning behöver genomföras?

Exemplen i artikel 35.3 i dataskyddsförordningen

- a. En 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.
- b. Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott, som avses i artikel 10.
- c. Systematisk övervakning av en allmän plats i stor omfattning.

Läs mer om tolkning av artikel 35.3 a–c i dataskyddsförordningen i bilagan
Rättsligt tolkningsstöd – avsnitt 4.2.

Fråga: Motsvarar eller liknar den planerade behandlingen något av exemplen i artikel 35.3 i dataskyddsförordningen (se ovan)?

☐ Ja

☐ Nej

IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen

Huvudregeln är att om en planerad behandling uppfyller minst två av kriterierna i IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen måste en konsekvensbedömning genomföras. Förteckningen är inte uttömmande. En konsekvensbedömning kan behöva genomföras i ett enskilt fall även om bara ett av kriterierna i förteckningen är uppfyllt.

Om den personuppgiftsansvarige gör bedömningen att typen av behandling i ett enskilt fall sannolikt inte leder till en hög risk, trots att två eller flera av kriterierna är uppfyllda, ska en noggrann motivering för detta dokumenteras.

Fråga: Vilka av kriterierna i förteckningen är uppfyllda?		
Kriterium	Exempel	Svar
1. Innebär behandlingen utvärdering eller poängsättning av människor?	Ett företag som erbjuder genetiska tester till konsumenter för att bedöma och förutse risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare.	☐ Ja ☐ Nej
2. Behandlas personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade?		☐ Ja ☐ Nej
3. Innebär behandlingen systematisk övervakning av människor?	Genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer	☐ Ja ☐ Nej
4. Behandlas känsliga personuppgifter enligt artikel 9 eller uppgifter som är av mycket personlig karaktär?	Ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringuppgifter eller en bank som hanterar finansiella uppgifter	☐ Ja ☐ Nej
5. Behandlas personuppgifter i stor omfattning?		☐ Ja ☐ Nej
6. Kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig?	Samkörning av register	☐ Ja ☐ Nej
7. Behandlas personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara?	Barn, anställda, asylsökande, äldre och patienter	☐ Ja ☐ Nej
8. Används ny teknik eller nya organisatoriska lösningar?	Sakernas internet-applikation (Internet of things, IoT)	☐ Ja ☐ Nej

Fråga: Vilka av kriterierna i förteckningen är uppfyllda?

Kriterium	Exempel	Svar
9. Behandlas personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal?	När en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.	☐ Ja ☐ Nej

Läs mer om IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen i bilagan Rättsligt tolkningsstöd – avsnitt 4.3.

Fråga: Är två eller fler av kriterierna i förteckningen uppfyllda?

- ☐ Ja (huvudregeln som innebär att en konsekvensbedömning ska genomföras är därmed uppfylld)
- ☐ Nej

Fråga: Om svaret är ja, är bedömningen att *typen av behandling* ändå inte medför att en konsekvensbedömning ska genomföras?

- ☐ Ja (ange en utförlig motivering för svaret nedan)
- ☐ Nej

Fråga: Om svaret är nej, är bedömningen att *typen av behandling* innebär att en konsekvensbedömning ska genomföras ändå?

- ☐ Ja (ange motivering nedan)
- ☐ Nej

Ingen skyldighet att genomföra en konsekvensbedömning

Fråga: Är behandlingen mycket lik en behandling för vilken det redan genomförts en konsekvensbedömning?

☐ Ja (utveckla detta nedan)

☐ Nej

Fråga: Omfattas behandlingen av en allmän konsekvensbedömning enligt artikel 35.10 i dataskyddsförordningen?

☐ Ja (utveckla detta nedan)

☐ Nej

Rådfråga dataskyddsombudet

Om två eller fler av kriterierna är uppfyllda och den personuppgiftsansvarige trots detta överväger att inte genomföra en konsekvensbedömning, bör dataskyddsombudet (om ett sådant utsetts) rådfrågas. Dataskyddsombudet kan ange sina bedömningar nedan och därefter returnera dokumentet till den som är ansvarig.

Fråga: Delar dataskyddsombudet bedömningen att en konsekvensbedömning inte ska genomföras? (I de fall minst två kriterier i förteckningen är uppfyllda bör svaret utvecklas noggrant.)

- ☐ Ja (ange motivering nedan)
 - ☐ Nej (ange motivering nedan)
 - ☐ Inte aktuellt
-

Fråga: Har dataskyddsombudet några rekommendationer?☐ Ja (ange dessa i tabellen nedan)☐ Nej

Nr	Dataskyddsombudets rekommendation	Datum	Den personuppgiftsansvariges svar på rekommendationen
001			☐ Accepterar ☐ Accepterar och vidtar åtgärd ☐ Avfärdar Om dataskyddsombudets rekommendationer avfärdats, ange en noggrann motivering nedan.
002			☐ Accepterar ☐ Accepterar och vidtar åtgärd ☐ Avfärdar Om dataskyddsombudets rekommendationer avfärdats, ange en noggrann motivering nedan.
003			☐ Accepterar ☐ Accepterar och vidtar åtgärd ☐ Avfärdar Om dataskyddsombudets rekommendationer avfärdats, ange en noggrann motivering nedan.

Slutsats

Fråga: Bedömer den personuppgiftsansvarige att det finns ett behov av att genomföra en konsekvensbedömning före den planerade behandlingen?

☐ Ja

☐ Nej
