

IMY:s mall för

Konsekvensbedömning enligt dataskyddsförordningen

Motsvarar Steg 3–10 i *En praktisk guide*

Innehåll

Övergripande information	3
Ansvariga för konsekvensbedömningen	3
Steg 3. Systematisk beskrivning av personuppgiftsbehandlingen	4
Steg 4. Rättslig analys	13
Steg 5. Riskhantering	25
Steg 6. Bedömning av skyldigheten att begära förhandssamråd	26
Steg 7. Synpunkter som hämtats in från berörda	27
Steg 8. Sammantagen bedömning	29
Steg 9. Förankring av bedömningen i organisationen	30
Steg 10. Kontinuerlig översyn	31

Om mallen

Mallen motsvarar Steg 3–10 i En praktisk guide. I guiden finns mer information om respektive steg. Excelbladet Riskhantering vid konsekvensbedömning kan användas i Steg 5.

Den praktiska guiden och mallarna finns på imy.se/konsekvensbedomning

Mallen är tänkt att underlätta för personuppgiftsansvariga att på ett strukturerat sätt dokumentera en konsekvensbedömning avseende dataskydd enligt artikel 35 i dataskyddsförordningen¹.

Observera att vissa av momenten kan behöva utföras i en annan ordning. I vissa fall kan det exempelvis vara lämpligt att hämta in synpunkter från de registrerade i ett tidigare skede. Om den personuppgiftsansvarige har utsett ett dataskyddsombud bör detta rådfrågas löpande.

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.

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

Personuppgiftsansvarig för behandlingen

Organisation (inkl.
organisationsnummer)

Adress

Telefon

E-post

Kontaktuppgifter till dataskyddsombud

Organisationens
dataskyddsombud

Adress

Telefon

E-post

Ansvariga för konsekvensbedömningen

Ansvarig för att genomföra
konsekvensbedömningen

Ansvarig för innehållet i
konsekvensbedömningen
och de bedömningar
som görs

Roller som deltagit i arbetet
med att genomföra
konsekvensbedömningen

Ansvarig för att hantera
eventuella kvarvarande
risker efter att
konsekvensbedömningen
avslutats

Ansvarig för att följa upp
konsekvensbedömningen

Steg 3. Systematisk beskrivning av personuppgiftsbehandlingen

3.1 Behandlingens art

Allmän beskrivning och bakgrund

Anvisningar

Avgränsa och beskriv objektet för konsekvensbedömningen. Ge en bakgrund och beskriv vad som föranlett den planerade behandlingen.

Kategorier av personuppgifter

Anvisningar

Lista de kategorier av personuppgifter som kommer att behandlas. Använd en rad för varje kategori och lägg till så många rader i tabellen som behövs. Om tabellen blir omfattande kan det vara lämpligt att istället lägga den som en bilaga till konsekvensbedömningen.

Ange i höger kolumn om någon av följande kategorier gäller:

- sådana kategorier av personuppgifter som anges i artikel 9 och artikel 10 i dataskyddsförordningen
- personuppgifter som är integritetskänsliga av andra skäl (t.ex. för att de rör enskildas ekonomiska eller personliga förhållanden)
- personnummer eller samordningsnummer.

Nr	Kategori av personuppgifter	Särskild kategori av personuppgifter
01		
02		
03		
04		
05		
06		

Kategorier av registrerade

Anvisningar

Lista de kategorier av registrerade vars personuppgifter kommer att behandlas. Använd en rad för varje kategori och lägg till så många rader i tabellen som behövs. Om tabellen blir omfattande kan det vara lämpligt att istället lägga den som en bilaga till konsekvensbedömningen.

Ange i höger kolumn om någon av följande kategorier gäller:

- personer som befinner sig i beroendeställning (exempelvis anställda, patienter eller elever)
- barn eller andra sårbara personer (exempelvis äldre, eller personer med funktionsvariationer)

Nr	Kategori av personuppgifter	Särskild kategori av personuppgifter
01		
02		
03		
04		
05		
06		

3.2 Behandlingens omfattning

Behandlingens volym

Anvisningar

Gör en uppskattning av antalet individer som berörs av behandlingen och den totala mängd personuppgifter som kommer att behandlas. Beskriv även antalet kategorier av personuppgifter (variationen).

Beakta hur ofta personuppgifter kommer att samlas in.

Behandlingens geografiska omfattning

Anvisningar

Beskriv i vilka länder uppgifterna kommer att behandlas. Ange om det kommer bli fråga om länder utanför EU/EES, s.k. tredjelandsöverföringar.

3.3 Behandlingens sammanhang

Anvisningar

Beskriv behandlingen i ett större perspektiv, dvs. de interna och externa faktorer som har relevans för det sammanhang där behandlingen ska ske.

3.4 Behandlingens ändamål

Anvisningar

Beskriv anledningen till att den personuppgiftsansvarige vill genomföra behandlingen och fördelarna med den (t.ex. för verksamheten, allmänheten och tredje parter). Beskriv även det avsedda utfallet för enskilda. Ändamålet ska anges så noggrant, utförligt och tydligt som möjligt.

3.5 Nödvändiga resurser

Anvisningar

Beskriv de resurser och informationstillgångar som behövs för att genomföra personuppgiftsbehandlingen (t.ex. programvara, servrar, hårdvara, nätverk, molntjänster, m.m.).

3.6 Funktionell beskrivning av behandlingen

Anvisningar

Beskriv hur behandlingen ska gå till mer i detalj och varifrån personuppgifterna kommer. Om det är fråga om en komplex behandling kan det vara lämpligt att hänvisa till en bilaga som innehåller ett flödesschema, en tabell eller liknande.

3.7 Roller och ansvarsfördelning

Personuppgiftsansvar

Anvisningar

Specificera den eller de personuppgiftsansvariga, dvs. de aktörer som ensamt eller tillsammans bestämmer ändamålen och tillvägagångssätten för behandlingen av personuppgifterna. Ange om behandlingen innebär ett separat eller gemensamt personuppgiftsansvar för de personuppgiftsansvariga.

Lista vilka avtalsdokument som anger ansvarsfördelningen mellan de personuppgiftsansvariga.

Mottagare inklusive personuppgiftsbiträden

Anvisningar

Ange om personuppgifter kommer att överföras till externa mottagare och i så fall vilka. Ange även om personuppgiftsbiträden kommer att vara involverade i behandlingen och vilka tjänster dessa ska tillhandahålla.

Lista eventuella personuppgiftsbiträdesavtal.

Nr	Personuppgiftsbiträde	Kategorier av personuppgifter som behandlas av biträdet	Ändamål med bitrådets behandling
01			
02			
03			
04			
05			

Steg 4. Rättslig analys

4.1 Gällande regelverk

Anvisningar

Gör en sammanställning över de regelverk som gäller för den aktuella behandlingen. Beakta även antagna uppförandekoder, genomförda certifieringar och branschpraxis.

4.2 Dataskyddsprinciperna och den rättsliga grunden för behandlingen

Principen om laglighet, korrekthet och öppenhet

Anvisningar

Beskriv hur ni garanterar att principen följs.

Rättslig grund för behandlingen

Anvisningar

Ange den rättsliga grunden för behandling av personuppgifter. Var noga med att ange om det finns flera rättsliga grunder, dvs. om olika kategorier av personuppgifter eller olika led i behandlingen har stöd i olika rättsliga grunder.

- Om den rättsliga grunden är samtycke bör det framgå av beskrivningen hur samtycket dokumenteras och administreras samt hur den registrerade kan återkalla sitt samtycke.
- Om den rättsliga grunden är intresseavvägning bör den bedömning som gjorts vid avvägningen mellan den personuppgiftsansvariges intresse och de registrerades intresse noga dokumenteras.

Nr	Beskrivning av behandlingen (ev. delmoment)	Personuppgifter som behandlas	Rättslig grund	Kommentar
01				
02				
03				
04				
05				
06				

4 Genomför en rättslig analys

Nr	Beskrivning av behandlingen (ev. delmoment)	Personuppgifter som behandlas	Rättslig grund	Kommentar
07				
08				
09				
10				
11				
12				
13				
14				

Rättsligt stöd för behandling av vissa kategorier av personuppgifter

Anvisningar

Om särskilda kategorier eller särskilt skyddsvärda personuppgifter ska behandlas, ange vilket undantag som är tillämpligt på behandlingen (förutom den rättsliga grunden ovan).

- För särskilda kategorier av personuppgifter: se undantagen i artikel 9.2 i dataskyddsförordningen.
- För personuppgifter som rör fällande domar i brottmål samt lagöverträdelse som innefattar brott: se artikel 10 i dataskyddsförordningen
- För personnummer och samordningsnummer: se 10 § i dataskyddslagen²

Nr	Personuppgifter	Tillämpligt undantag	Kommentar
01			
02			
03			
04			
05			
06			

² Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

4 Genomför en rättslig analys

Nr	Personuppgifter	Tillämpligt undantag	Kommentar
07			
08			
09			
10			
11			
12			
13			
14			

Principen om ändamålsbegränsning

Anvisningar

Beskriv hur ni garanterar att principen följs.

Principen om uppgiftsminimering

Anvisningar

Beskriv hur ni garanterar att principen följs.

Personuppgift

Behandlingen är nödvändig för att

Vid behov, utveckla svaret nedan

Principen om riktighet

Anvisningar

Beskriv hur ni garanterar att principen följs.

Principen om lagringsminimering

Anvisningar

Beskriv hur ni garanterar att principen följs.

Principen om integritet och konfidentialitet

Anvisningar

Beskriv hur ni garanterar att principen följs.

4.3 Registrerades rättigheter

Anvisningar

Beskriv vilka rutiner organisationen har för att kunna tillgodose de registrerades rättigheter enligt dataskyddsförordningen, dvs.

- Rätten till information
- Rätten till tillgång
- Rätten till rättelse
- Rätten till radering
- Rätten till begränsning av behandling
- Rätten till dataportabilitet
- Rätten att göra invändningar
- Rätten att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering

I de fall det finns rutindokument som bedöms ge en tillräckligt utförlig beskrivning kan hänvisning göras till dessa.

4.4 Skyddsåtgärder för internationella överföringar

Anvisningar

Om personuppgifter kommer att överföras till ett land utanför EU/EES i samband med behandlingen, ange de skyddsåtgärder som vidtagits nedan.

4.5 Sammantagen bedömning

Anvisningar

Ange den samlade bedömningen av om de rättsliga förutsättningarna för att genomföra behandlingen är uppfyllda (inkluderat bedömningen av behovet av och proportionaliteten hos behandlingen i förhållande till syftena med den).

Steg 5. Riskhantering

Anvisningar

Använd gärna Excelbladet Riskhantering vid konsekvensbedömning för att

1. identifiera risker
2. analysera riskernas sannolikhet och allvarighet
 - Sannolikheten för att risken ska realiseras kan anges som låg, medel, hög och mycket hög.
 - Allvarlighetsgraden av konsekvenserna kan bedömas som begränsade, relativt allvarliga, allvarliga och mycket allvarliga.
3. beskriva de riskreducerande åtgärderna och
4. följa upp riskerna genom en ny riskbedömning.

Summera bedömningen nedan.

Steg 6. Bedömning av skyldigheten att begära förhandssamråd

Anvisningar

Dokumentera bedömningen av om riskerna är fortsatt höga efter att de riskreducerande åtgärderna har beaktats.

Resultatet av eventuellt förhandssamråd

Anvisningar

Dokumentera resultatet av ett eventuellt förhandssamråd eller bifoga IMY:s yttrande.

Steg 7. Synpunkter som hämtats in från berörda

7.1 Dataskyddsombudets rekommendationer

Anvisningar			
<p>Dokumentera synpunkter och/eller rekommendationer som dataskyddsombudet har lämnat under arbetets gång. Dokumentera även eventuella slutliga utlåtanden från dataskyddsombudet.</p> <p>Dokumentera och motivera eventuella beslut att inte följa formella rekommendationer från dataskyddsombudet.</p>			
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.

Om dataskyddsombudets rekommendationer avfärdats, ange en noggrann motivering nedan.

7.2 Synpunkter från de registrerade

Anvisningar

Ange nedan om ni har hämtat in synpunkter från de registrerade. Ange även om synpunkter inte har hämtats in och i så fall varför.

Dokumentera eventuella synpunkter från de registrerade. Motivera och dokumentera även eventuella beslut som går emot de registrerades synpunkter.

Notera att de registrerade kan behöva tillfrågas redan innan, eller i samband med, riskbedömningen. De personuppgiftsansvariga kan behöva omvärdera riskerna enligt synpunkterna.

7.3 Synpunkter från övriga intressenter

Anvisningar

Ange om ni har hämtat in synpunkter från någon övrig intressent, exempelvis en informationssäkerhetsansvarig eller någon med särskild teknisk kompetens. Dokumentera eventuella synpunkter från dessa, om lämpligt.

Steg 8. Sammantagen bedömning

Anvisningar

Ange den sammantagna bedömningen av om den planerade behandlingen kan genomföras eller inte.

Steg 9. Förankring av bedömningen i organisationen

Anvisningar

Dokumentera hur och när de beskrivningar och bedömningar som ni gjort har förankrats i organisationens ledningsgrupp, exempelvis genom en internremiss eller föredragning på ledningsgruppsmöte eller dylikt.

Tydliggör vem som bär ansvaret för att vidta de riskreducerande åtgärderna och vem som ansvarar för eventuell kvarstående risk med behandlingen.

Steg 10. Kontinuerlig översyn

10.1 Plan för att genomföra översyn

Anvisningar

Ange när och hur ofta konsekvensbedömningen ska följas upp samt vilka roller eller funktioner i organisationen som ansvarar för uppföljningen. Beskriv även hur det ska säkerställas att eventuella förändringar av risken fångas upp inom organisationen.

10.2 Versionshistorik

Anvisningar

Fyll i tabellen för att tydliggöra när förändringar i konsekvensbedömningen har gjorts.

Version	Datum	Deltagare	Fastställd av	Ändringar
01				
02				
03				
04				
05				
06				

Version	Datum	Deltagare	Fastställd av	Ändringar
07				
08				
09				
10				
11				
12				