Boråsregionen
Sjuhärads kommunalförbund

Dataskyddsombudens generella råd

Konsekvensbedömning (DPIA)

Sammanfattning dataskyddsombudens råd

- Genomför och dokumentera tröskelanalyser för samtliga registrerade behandlingar
- Kontakta DSO inför att konsekvensbedömning ska genomföras
- Använd IMY:s vägledning och mallar som stöd
- Kontakta DSO för stöd och råd under arbetets gång
- Begär skriftligt yttrande när konsekvensbedömningen bedöms vara färdigställd

Syfte

En konsekvensbedömning avseende dataskydd (Data Protection Impact Assessment, DPIA) är ett verktyg för att identifiera, bedöma och hantera risker för fysiska personers fri- och rättigheter innan en personuppgiftsbehandling påbörjas eller förändras.

Dataskyddsförordningen artikel 35 kräver att en konsekvensbedömning genomförs när en planerad behandling sannolikt leder till en *hög risk* för de registrerade. Detta för att säkerställa att risker identifieras i ett tidigt skede och att nödvändiga skyddsåtgärder kan vidtas innan behandlingen genomförs.

Konsekvensbedömningar är en del av den personuppgiftsansvariges ansvarsskyldighet och bidrar till att personuppgifter behandlas på ett lagligt, säkert och transparent sätt.

Dataskyddsombudens generella råd är baserat på Integritetsskyddsmyndighetens (IMY) vägledning och mall för konsekvensbedömningar.

Processbaserat arbetssätt för ett bättre och enklare DPIA-arbete

Personuppgiftsbehandlingar uppstår när verksamheten utför sina uppdrag.

Dataskyddsombuden rekommenderar att personuppgiftsansvarigas behandlingsregister enligt art 30 utgår ifrån dessa processer (se Dataskyddsombudens

generella råd om Behandlingsregister) och att även konsekvensbedömningar utgår från dessa processer. Genom att utgå från processerna blir det enklare att förstå varför personuppgifterna behandlas, vilka registrerade som berörs, vilka risker som kan uppstå och vilka skyddsåtgärder som behövs.

Arbetssätten stärker varandra och skapar bättre förutsättningar för ett sammanhållet och effektivt dataskyddsarbete.

När ska en konsekvensbedömning genomföras?

En konsekvensbedömning ska genomföras när en personuppgiftsbehandling sannolikt leder till hög risk för de registrerades rättigheter och friheter. Konsekvensbedömningen ska i de fallen genomföras innan behandlingen påbörjas eller innan väsentliga förändringar genomförs. Syftet är att identifiera och hantera risker innan behandlingen sker. Som stöd i bedömningen om en konsekvensbedömning ska genomföras bör IMY:s kriterier för hög risk användas. Om två eller fler kriterier uppfylls finns det ofta anledning att genomföra en konsekvensbedömning. Även en behandling som endast uppfyller ett kriterium kan i vissa fall kräva en konsekvensbedömning beroende på behandlingens art, omfattning, sammanhang och ändamål. Vid osäkerhet om en konsekvensbedömning krävs bör frågan dokumenteras och dataskyddsombuden kontaktas för rådgivning.

Dataskyddsombuden rekommenderar att dokumentera så kallad tröskelanalys för samtliga behandlingar som finns registrerade i behandlingsregistret, för att visa att den personuppgiftsansvarige bedömt om behandlingen är en högriskbehandling eller inte.

Genomför konsekvensbedömningen

Dataskyddsombuden rekommenderar att konsekvensbedömningar genomförs med stöd av IMY:s vägledning och mall för konsekvensbedömningar. Om verksamheten använder en egen mall bör den omfatta samma moment och bedömningar som framgår av IMY:s vägledning.

Konsekvensbedömningen bör utgå från den verksamhetsprocess där behandlingen sker eller en sammanhängande behandling och inte ett enskilt IT-system. Ett IT-system kan användas i flera olika processer med olika ändamål, registrerade, risker och skyddsåtgärder.

Verksamheten bör särskilt analysera och dokumentera:

- den planerade behandlingen och dess ändamål
- bedömning av nödvändighet och proportionalitet
- risker för de registrerades rättigheter och friheter
- planerade skyddsåtgärder
- bedömning av kvarstående risk

Detta är områden som dataskyddsombuden särskilt går igenom vid rådgivning och granskning. Om konsekvensbedömningen visar att en hög risk kvarstår trots planerade skyddsåtgärder ska den personuppgiftsansvarige samråda med IMY innan behandlingen påbörjas.

Om konsekvensbedömningen omfattar flera personuppgiftsansvariga eller gemensamt personuppgiftsansvar ska ansvarsfördelning och respektive parts skyldigheter beskrivas i konsekvensbedömningen.

Dokumentera och följ upp

Konsekvensbedömningar ska dokumenteras och hållas aktuella. Konsekvensbedömningar är en del av verksamhetens löpande dataskyddsarbete och bör följas upp regelbundet och även ses över när behandlingar förändras, nya personuppgifter börjar behandlas, nya system eller leverantörer används eller när riskbilden förändras.

Dataskyddsombudens stöd och råd

Enligt Dataskyddsförordningen artikel 35.2 ska den personuppgiftsansvarige rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd. Enligt Dataskyddsförordningen artikel. 39.1 c ska dataskyddsombudet på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av konsekvensbedömningen.

Dataskyddsombuden bör uppmärksammas tidigt på planerade konsekvensbedömningar (DPIA), för att kunna planera att tid finns för rådgivning och yttrande. Beroende på behandlingens art, omfattning och personuppgiftsansvarigas behov kan dataskyddsombuden involveras i arbetet med konsekvensbedömningar och bistå med råd och synpunkter under arbetets gång. Stöd vid framtagande av konsekvensbedömning prioriteras utefter risk. Stöd kan ges genom:

- Genomgång av metod
- Rådgivning kring avgränsning inför konsekvensbedömning
- Rådgivning kring specifik frågeställning, t.ex. rättslig grund eller riskbedömning
- Marginalkommentarer på skriftliga underlag under arbetets gång

Dataskyddsombuden ska alltid ges möjlighet att lämna yttrande över genomförd konsekvensbedömning innan den fastställs. När ansvarig för konsekvensbedömning bedömer att konsekvensbedömningen är färdigställd skickas en begäran om samråd till DSO. Skriftligt yttrande lämnas som huvudregel inom 14 dagar. DSO skriver ett skriftligt yttrande och lämnar formella rekommendationer. Yttrandet ska dokumenteras i konsekvensbedömningen (biläggas och diarieföras). Om dataskyddsombudens rekommendationer inte följs ska det dokumenteras särskilt.

Det är den personuppgiftsansvarige som ansvarar för bedömningen av behandlingens laglighet. Dataskyddsombuden kan rekommendera att en behandling inte genomförs om kraven i dataskyddslagstiftningen inte bedöms vara uppfyllda. Att någon sådan rekommendation inte lämnas innebär inte att dataskyddsombuden tagit ställning till behandlingens laglighet.

Relaterade dokument

- IMY:s Vägledning vid konsekvensbedömning
- Dataskyddsombudens generella råd om Behandlingsregister enligt artikel 30 Dataskyddsförordningen

Dataskyddsombuden ger råd och stöd i dataskyddsfrågor. Ansvaret för personuppgiftsbehandlingen ligger alltid hos den personuppgiftsansvariga verksamheten.