Boråsregionen
Sjuhärads kommunalförbund

# Dataskyddsombudens generella råd

## Behandlingsregister enligt artikel 30 Dataskyddsförordningen

Baserad på DSO Västs råd

**Sammanfattning dataskyddsombundens råd:**

- Fastställ behandling utifrån process
- Komplettera den obligatoriska informationen i behandlingsregistret för att det ska bli ett funktionellt verktyg i verksamheten
- Ha rutiner för att hålla behandlingsregistret aktuellt

### Syfte

Personuppgiftsansvariga nämnder och bolag ansvarar för att personuppgifter behandlas lagligt, korrekt och med tillräckligt skydd. För att kunna ta det ansvaret behöver nämnden veta vilka personuppgiftsbehandlingar som sker inom verksamheten. Behandlingsregistret är därför ett av den personuppgiftsansvariges viktigaste verktyg för styrning och kontroll av dataskyddsarbetet. Registret ska ge en samlad bild av vilka personuppgifter som behandlas, varför de behandlas, vilken rättslig grund som används och vilka skyddsåtgärder som finns. Ett aktuellt och användbart behandlingsregister ger nämnden/styrelsen förutsättningar att uppfylla sin ansvarsskyldighet enligt dataskyddsförordningen. Behandlingsregistret utgör grunden för det fortsatta dataskyddsarbetet.

### Processbaserat arbetssätt för ett bättre och enklare dataskyddsarbete

Personuppgiftsbehandlingar uppstår när verksamheten utför sina uppdrag och arbetsuppgifter. Dataskyddsombuden rekommenderar därför att dataskyddsarbetet utgår från verksamhetens processer och arbetsflöden, inte från de IT-system eller tjänster som används. Samma processperspektiv bör användas vid kartläggning av personuppgiftsbehandlingar, upprättande av behandlingsregister, riskbedömningar,

konsekvensbedömningar (DPIA). Genom ett processbaserat arbetssätt skapas bättre förutsättningar att identifiera personuppgiftsbehandlingar, bedöma risker, fastställa rättslig grund, hantera registrerades rättigheter och upprätthålla ett aktuellt behandlingsregister.

**Kartlägg behandlingar**

Kartläggningen bör utgå från verksamhetens uppdrag och arbetsprocesser snarare än från de IT-system som används. Genom att beskriva hur verksamheten arbetar blir det enklare att identifiera vilka personuppgiftsbehandlingar som faktiskt sker, varför de utförs och vilka krav som gäller för behandlingen. Behandlingsregistret ska spegla verksamheten, inte systemkartan. Kartläggningen bör omfatta följande steg:

1. *Identifiera verksamhetens processer*

   Utgå från verksamhetens uppdrag och beskriv de arbetsprocesser där personuppgifter används. Exempel: Handläggning av ansökningar eller rekrytering av personal. Ta hjälp av de som vet bäst - de som arbetar ute i verksamheterna.

2. *Identifiera vilka personer som berörs*

   För varje process, beskriv vilka grupper av registrerade som omfattas. Exempel: Invånare, elever, vårdnadshavare, brukare osv

3. *Identifiera vilka personuppgifter som behandlas*

   Beskriv vilka typer av personuppgifter som används i processen. Exempel: Namn och kontaktuppgifter, Personnummer mm. Tänk på att även uppgifter som indirekt kan identifiera en person är personuppgifter.

4. *Beskriv ändamålet*

   Beskriv varför uppgifterna behandlas. Ändamålet ska vara tydligt, konkret och kopplat till verksamhetens uppdrag. Exempel: Handläggning av ansökningar om ekonomiskt bistånd.

5. *Fastställ rättslig grund enligt artikel 6 GDPR*

   Identifiera vilket stöd verksamheten har för behandlingen.

6. *Kartlägg informationsflödet*

   Beskriv varifrån uppgifterna kommer, vem som har åtkomst till dem, om de lämnas vidare till andra mottagare, om personuppgiftsbiträden används.

7. *Bedöm lagring och gallring*

   Dokumentera hur länge uppgifterna behöver sparas, vilka gallringsregler eller bevarandekrav som gäller och hur uppgifterna raderas eller arkiveras.

**Hur detaljerad ska en behandling vara?**

Behandlingsregistret ska ge en rättvisande bild av verksamhetens personuppgiftsbehandlingar utan att bli onödigt detaljerat. Behandlingen behöver vara tydligt definierad och avgränsad för att kunna användas enhetligt i dataskyddsarbetet. Samma avgränsning bör användas i bland annat behandlingsregistret, konsekvensbedömningar, riskbedömningar och ligga till grund för den information som lämnas till registrerade.

Följande frågor kan användas som stöd vid avgränsningen:

- Har behandlingen ett eget ändamål?
- Har behandlingen en annan rättslig grund eller annat lagstöd?
- Berörs andra kategorier av registrerade?
- Behandlas andra kategorier av personuppgifter?
- Finns särskilda risker eller skyddsåtgärder?

Om svaret är ja på någon av frågorna kan det vara lämpligt att dokumentera behandlingen som en separat behandling i registret.

## Dokumentera behandlingen i behandlingsregistret

Verksamhetens behandlingar ska dokumenteras i den personuppgiftsansvariges behandlingsregister. I Dataskyddsförordningen artikel 30 anges vilka uppgifter som minst ska ingå i behandlingsregistret. För att behandlingsregistret ska kunna användas som ett verktyg för styrning, uppföljning och utveckling av dataskyddsarbetet rekommenderar dataskyddsombuden att följande uppgifter finns dokumenterade:

- Ändamål med behandlingen
- Rättslig grund och tillhörande lagstöd, intresseavvägningar eller andra relevanta rättsliga bedömningar
- Kategorier av registrerade
- Kategorier av personuppgifter
- Eventuella känsliga personuppgifter och undantag enligt art. 9.2 GDPR eller uppgifter om lagöverträdelser som behandlas
- Kategorier av mottagare
- Eventuella personuppgiftsbiträden
- Eventuella överföringar till tredje land
- Gallrings- eller bevarandetid
- Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder
- Ansvarig verksamhet eller funktion
- Kontaktperson för behandlingen
- Om konsekvensbedömning (DPIA) har genomförts eller behöver genomföras
- Datum för senaste översyn eller uppdatering

## Håll behandlingsregistret aktuellt

Behandlingsregistret är ett levande dokument som behöver ses över regelbundet. Behandlingsregistret bör uppdateras när:

- nya processer eller arbetsuppgifter införs
- nya IT-system tas i bruk
- ändamålet med behandlingen förändras
- nya personuppgifter börjar behandlas

- nya mottagare eller personuppgiftsbiträden tillkommer
- gallringsregler förändras
- en riskbedömning eller konsekvensbedömning visar att ytterligare dokumentation behövs.

Ett aktuellt behandlingsregister skapar förutsättningar för att hantera registrerades rättigheter, genomföra riskbedömningar och konsekvensbedömningar samt följa upp att personuppgifter behandlas i enlighet med dataskyddsförordningen.

**Personuppgiftsbiträdesregister**

I de fall en nämnd eller styrelse agerar personuppgiftsbiträde åt en annan personuppgiftsansvarig ska den, utöver sitt eget behandlingsregister som personuppgiftsansvarig, föra ett separat register över de personuppgiftsbehandlingar som utförs i egenskap av personuppgiftsbiträde.

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