

Dataskyddsombudens generella råd

Personuppgiftsbiträdesavtal

Inledning

Innan en personuppgiftsansvarig anlitar ett personuppgiftsbiträde behöver den personuppgiftsansvarige försäkra sig om att biträdet kan uppfylla dataskyddsförordningens krav. Personuppgiftsbiträdet ska kunna visa att lämpliga tekniska och organisatoriska åtgärder finns på plats för att skydda personuppgifterna och säkerställa den registrerades rättigheter.

Hantering ska regleras genom avtal eller annan rättsakt.

Att tänka på

Vanligen upprättas ett personuppgiftsbiträdesavtal (PUB-avtal) mellan parterna.

Dataskyddsombuden rekommenderar de personuppgiftsansvariga att använda SKR:s mall vid upprättande av PUB-avtal och vill särskilt betona vikten av tydliga och aktuella instruktioner till personuppgiftsbiträdet. Instruktionerna bör vara anpassade till den aktuella behandlingen och dess särskilda krav. Vid ändringar i tjänsten, behandlingen eller avtalsvillkoren bör instruktionerna och övriga avtalsdokument ses över för att säkerställa att de fortsatt motsvarar den faktiska personuppgiftsbehandlingen.

Personuppgiftsansvariga behöver också vara uppmärksamma på eventuella ändringar eller tillägg i villkoren i PUB-avtalen som kan innebära att ansvarsfördelningen förändras eller att personuppgiftsbiträdets åtaganden begränsas på ett sätt som inte är förenligt med den personuppgiftsansvariges skyldigheter enligt dataskyddsförordningen.

Avtalsförändringar bör alltid bedömas innan de accepteras.

I de fall en nämnd inom samma kommun är personuppgiftsbiträde kan hantering regleras genom PUB-avtal eller reglemente, riktlinje eller liknande styrdokument. Om styrdokument används bör den personuppgiftsansvarige säkerställa att det finns tydliga instruktioner som beskriver den aktuella personuppgiftsbehandlingen och vilka hanteringskrav som personuppgiftsbiträdet har att följa.

Övrigt dataskyddsarbete

Att ett PUB-avtal upprättas innebär inte i sig att en personuppgiftsbehandling är laglig. Innan ett personuppgiftsbiträde anlitas och PUB-avtal tecknas bör den personuppgiftsansvarige säkerställa att de grundläggande förutsättningarna för behandlingen är uppfyllda. Detta omfattar bland annat att den rättsliga grunden har fastställts, att behandlingen dokumenterats i behandlingsregistret samt att nödvändiga bedömningar och analyser har genomförts. PUB-avtalet bör därför ses som en del av det övergripande dataskyddsarbetet, inte som en fristående åtgärd.

Nedan checklista kan användas för att säkerställa att viktiga aspekter beaktats innan PUB-avtal tecknas.

Checklista inför tecknande av PUB-avtal

1. Fastställ rollerna

- ☐ Är det verkligen ett personuppgiftsbiträde?
- ☐ Bestämmer leverantören inga egna ändamål med behandlingen?
- ☐ Finns risk att relationen istället är gemensamt personuppgiftsansvar?
- ☐ Är personuppgiftsansvarig korrekt identifierad?

2. Behövs PUB-avtal?

- ☐ Behandlar leverantören personuppgifter för vår räkning?
- ☐ Har leverantören tillgång till personuppgifter eller möjlighet att få tillgång till dem?
- ☐ Om nej, behövs kanske inte något PUB-avtal.

3. Säkerställ att instruktionerna är tydliga

Instruktionerna ska minst beskriva:

- ☐ Ändamål med behandlingen
- ☐ Föremålet för behandlingen
- ☐ Behandlingens art
- ☐ Behandlingens varaktighet
- ☐ Kategorier av registrerade
- ☐ Typer av personuppgifter
- ☐ Eventuella särskilda instruktioner eller begränsningar

4. Kartlägg personuppgifterna

- ☐ Vilka personuppgifter behandlas?
- ☐ Förekommer personnummer?
- ☐ Förekommer känsliga personuppgifter?
- ☐ Förekommer uppgifter om lagöverträdelser?
- ☐ Förekommer fritextfält?
- ☐ Förekommer bilder, video eller ljudinspelningar? – vad kommer att framkomma där?

5. Underbiträden

- ☐ Används underbiträden?
- ☐ Finns aktuell underbiträdeslista?
- ☐ Är det tydligt var underbiträdena finns?
- ☐ Finns rutin för information vid förändringar?
- ☐ Säkerställs samma dataskyddskrav hos underbiträdena?

6. Tredjelandsoverföringar

- ☐ Behandlas uppgifter utanför EU/EES?

- ☐ Har supportpersonal åtkomst från tredje land?
- ☐ Används amerikanska eller andra utländska molntjänster?
- ☐ Är laglig grund för eventuell överföring dokumenterad?

7. Informationssäkerhet

- ☐ Finns behörighetsstyrning?
- ☐ Finns multifaktorautentisering (MFA)?
- ☐ Loggas åtkomst och händelser?
- ☐ Finns kryptering?
- ☐ Finns rutin för incidenthantering?
- ☐ Finns regelbunden säkerhetsuppföljning?

8. Uppföljning och revision

- ☐ Hur ska biträdet följas upp?
- ☐ Finns rätt till revision?
- ☐ Kan leverantören visa säkerhetsarbete genom rapporter eller certifieringar?
- ☐ Har verksamheten en plan för löpande kontroll?

9. Avtalets upphörande

- ☐ Ska uppgifter raderas eller återlämnas?
- ☐ När ska detta ske?
- ☐ Hur verifieras att radering genomförts?
- ☐ Vad händer med säkerhetskopior och loggar?

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