

# Datainspektionen informerar

Nr 3/2016

## Allmänna råd

Datainspektionen har utarbetat en allmän vägledning gällande skriftligt avtal om registerbitrådets behandling av personuppgifter för den personuppgiftsansvarigas räkning (registerbitrådesavtal).

Vägledningen innehåller en mall till skriftligt avtal.

Datainspektionen

den 6 oktober 2016



1	Vägledning om databehandlingsavtal.....	4
2	Förutsättningar och definitioner.....	4
3	Minimikrav .....	5
3.1	Ange ändamålen med behandlingen.....	5
3.2	Beskrivning av vilka personuppgifter som ska behandlas .....	5
3.2.1	Konkreta rutiner för användning av personuppgifterna.....	5
3.2.2	Regler för att lämna ut personuppgifterna .....	5
3.3	Eventuella underleverantörer ska framgå av avtalet.....	6
3.4	Ta tillvara den registrerades rättigheter.....	6
3.5	Enligt avtalet ska registerbiträdet hålla en god säkerhet vid behandling.....	6
3.6	Avtalets giltighetstid .....	7
4	Överföring till utlandet.....	7

## 1 Vägledning om databehandlingsavtal

Denna vägledning innehåller en mall på hur personuppgifter behandlas av registerbiträdet i ett databehandlingsavtal. Vägledningen ska läsas parallellt med avtalsmallen.

Det har inte varit ändamålsenligt att göra en uttömmande mall eller lista över vad som erfordras av ett databehandlingsavtal. Det är Datainspektionens förhoppning att mallen kan ge en indikation om vilka huvudfrågorna enligt personuppgiftslagen<sup>1</sup> bör vara.

## 2 Förutsättningar och definitioner

Verksamheter som väljer att utlokalisera hela eller delar av behandlingen av personuppgifter till andra verksamheter anlitar registerbiträden. Det ska finnas ett skriftligt avtal om registerbitrådets behandling av personuppgifter för den registeransvariges räkning enligt 19 § 2 mom. personuppgiftslagen.

Den registeransvariga ska försäkra sig om att registerbiträdet håller tillräckligt hög säkerhetsnivå enligt 18 § personuppgiftslagen.

### *Registeransvarig*

- Den myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
- Har ansvar för att uppgifter behandlas i enlighet med personuppgiftslagens bestämmelser

Behandling av personuppgifter definieras som varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring et cetera.

### *Registerbiträde*

- Den som behandlar personuppgifter för den registeransvariges räkning
- Ska bara behandla personuppgifter i enlighet med vad som avtalats med de registeransvarige

Registerbiträdet är ansvarigt för personuppgifter som behandlas inom den egna verksamheten såsom till exempel personuppgifter om egen personal.

---

<sup>1</sup> Härmed avses landskapslag (2007:88) om behandling av personuppgifter inom landskaps- och kommunalförvaltningen

Behandling av känsliga personuppgifter kräver i regel ett mera detaljerat avtal än vad som till exempel krävs för ett enklare faktureringsuppdrag. Graden av specificering varierar från helt grundläggande krav till mera detaljerade såsom nivån på informationssäkerheten.

### 3 Minimikrav

Nedanstående punkter är minimikrav för vad som bör finnas med i ett skriftligt avtal om registerbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning (registerbiträdesavtal). Den registeransvariga kan ställa högre krav än vad som följer av personuppgiftslagen, men får inte avtala om villkor som är i strid med de krav som personuppgiftslagen ställer.

#### 3.1 Ange ändamålen med behandlingen

Det ska framgå av avtalet vilket ändamålet är med behandlingen av personuppgifterna. Registerbitrådet ska kunna behandla personuppgifterna i förhållande till hur ändamålet är definierat.

Exempel på behandling är makulering av pappersdokument, IT-drift, fakturering, kameraövervakning, behandling av personaluppgifter såsom utbetalning av löner eller liknande.

#### 3.2 Beskrivning av vilka personuppgifter som ska behandlas

Det ska tydligt framgå av avtalet vad registerbitrådet ska göra med personuppgifterna.

Ska de lagras för framtida bruk (arkivering), eller ska de bearbetas? Avtalet ska också klart reglera om det ska ske annan behandling, till exempel koppling med andra personuppgifter/register eller motsvarande.

##### 3.2.1 Konkreta rutiner för användning av personuppgifterna

Registerbitrådet har inte rätt att förfoga över personuppgifterna och får därför inte behandla dem för egna ändamål.

##### 3.2.2 Regler för att lämna ut personuppgifterna

Registerbitrådet ska följa avtalet. Om personuppgifterna ska lämnas ut till externa parter ska det framgå klart och tydligt i avtalet. Avtalet kan innehålla bestämmelser om vem som ska kunna få tillgång till personuppgifterna och på vilka villkor det kan ske.

### 3.3 Eventuella underleverantörer ska framgå av avtalet

Om registerbiträdet använder sig av tjänsteunderleverantörer ska det klart framgå av avtalet mellan den registeransvariga och registerbiträdet. 5 kapitlet personuppgiftslagen ställer krav på säkerheten vid behandling av personuppgifter. Samtliga som på registerbitrådets uppdrag utför arbete där de aktuella personuppgifterna ingår ska känna till de avtalsmässiga och lagbaserade villkoren. Därför bör även ett avtal upprättas mellan registerbiträdet och underleverantörerna som ett tillägg till registerbitrådesavtalet.

### 3.4 Ta tillvara den registrerades rättigheter

Avtalet kan innehålla en arbetsfördelning mellan registeransvarig och registerbiträde, till exempel vem som ska hantera och behandla förfrågningar från registrerade. Den registeransvariga kan få en förfrågan som denna vidareförmedlar till registerbiträdet som behandlar förfrågan. Det kan gälla förfrågningar om

- Information till den registrerade
- Rättelse av personuppgifter

### 3.5 Enligt avtalet ska registerbiträdet hålla en god säkerhet vid behandling

Enligt 18 § 1 och 2 mom. personuppgiftslagen ska lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas. I avtalet ska klargöras vilken säkerhetsnivå beträffande sekretess, integritet och tillgänglighet ska vara.

Avtalet bör innehålla bestämmelser om

- Avvikelsehantering
- Behörighetskontroll, till exempel loggföring
- Andra krav enligt 5 kapitlet personuppgiftslagen:
  - Tystnadsplikt
  - Säkerhetsrevisioner
  - Fysiska säkerhetsåtgärder
  - Vilka rutiner med mera som ska dokumenteras
  - Personal hos parterna som ska ha tillgång till personuppgifterna

Båda parter har ett självständigt ansvar enligt personuppgiftslagen och avtalet kan reglera arbetsfördelningen mellan parterna.

### 3.6 Avtalets giltighetstid

Avtalet ska innehålla följande uppgifter

- Hur länge avtalet är ikraft
- Vad som ska ske med uppgifterna efter att avtalet har upphört – om uppgifterna ska lämnas tillbaka eller utplånas, och om sparade säkerhetskopior ska lämnas tillbaka eller utplånas
- Hur ofta säkerhetsrevision ska göras

## 4 Överföring till utlandet

Om det är aktuellt att överföra personuppgifter till utlandet ska det regleras i avtalet. Se 6 och 7 §§ personuppgiftslagen.

**BILAGA: Avtalsskiss – avtal om behandling av personuppgifter****Avtal om behandling av personuppgifter  
(registerbiträdesavtal)**

mellan

.....  
Registeransvarig

och

.....  
Registerbiträde

- 1. Avsikten med avtalet**
- 2. Ändamål**
- 3. Registerbitrådets skyldigheter**
- 4. Anlitandet av underleverantörer**
- 5. Säkerhet**
- 6. Säkerhetsrevisioner**
- 7. Avtalets giltighetstid**
- 8. Avtalets upphörande**
- 9. Information**
- 10. Lagval**



Avtalet är upprättat i två exemplar, vardera ett för registeransvarig och registerbiträde.

Ort och tid

Registeransvarig

Registerbiträde

.....  
(underskrift)

.....  
(underskrift)