# Datainspektionen informerar

# Nr 7/2018

# Allmänna råd

Datainspektionen ger ut allmänna råd i syfte:

1) att öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt EU:s dataskyddsförordning samt

2) att öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling av personuppgifter.

De allmänna råden är inte bindande, utan innehåller rekommendationer om hur de bindande kraven i dataskyddsförordningens kan uppnås. Detta dokument är en **allmän vägledning gällande personuppgiftsbiträdens behandling av personuppgifter för personuppgiftsansvariga myndigheters räkning.** Vägledningen innehåller en mall till ett skriftligt avtal mellan personuppgiftsansvarig myndighet och ett personuppgiftsbiträde.

Datainspektionen

Den 14 maj 2018

di.ax datainspektionen

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

# 1. Inledning

Om en myndighet så önskar kan den utlokalisera hela eller delar av behandlingen av personuppgifter genom att anlita personuppgiftsbiträden. Denna vägledning handlar om kraven som ställs i EU:s dataskyddsförordning[1] för att personuppgifter ska kunna behandlas av ett personuppgiftsbiträde. Dataskyddsförordningen tillämpas från och med den 25 maj 2018.

Den personuppgiftsansvariga myndigheten ska försäkra sig om att personuppgiftsbiträdet håller tillräckligt hög säkerhetsnivå enligt dataskyddsförordningen.

Det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning, enligt artikel 28.3 och artikel 28.9 i dataskyddsförordningen. Avtalet, kallat *personuppgiftsbiträdesavtal*, måste innehålla bestämmelser om flera olika saker såsom

- vilka personuppgifter som ska behandlas
- syftet med behandlingen av personuppgifter
- tystnadsplikt
- säkerhetsnivån
- säkerhetsrevision och
- åtgärder när behandlingen av personuppgifterna ska avslutas.

# 2. Definitioner

*Behandling av personuppgifter*

- en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

*Personuppgiftsansvarig*

- Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

- Har ansvar för att uppgifter behandlas i enlighet med dataskyddsförordningens bestämmelser.

[1] Härmed avses 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.

*Personuppgiftsbiträde*

- Den som behandlar personuppgifter för den personuppgiftsansvarigas räkning.

- Ska bara behandla personuppgifter i enlighet med vad som avtalats med den personuppgiftsansvarige.

Personuppgiftsbiträdet är personuppgiftsansvarig för personuppgifter som behandlas inom den egna verksamheten, såsom personuppgifter om egen personal.

# 3. Innehållet i ett personuppgiftsbiträdesavtal

Nedanstående punkter är minimikrav för vad som enligt artikel 28.3 i dataskyddsförordningen bör finnas med i ett personuppgiftsbiträdesavtal. Den personuppgiftsansvariga kan ställa högre krav än vad som följer av dataskyddsförordningen, men får inte avtala om villkor som är i strid med de krav som dataskyddsförordningen ställer.

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.

I avtalet ska det enligt artikel 28.3 föreskrivas om:

- föremålet för behandlingen,
- behandlingens varaktighet, art och ändamål,
- typen av personuppgifter och kategorier av registrerade samt
- den personuppgiftsansvariges skyldigheter och rättigheter.

## 3.1 Behandlingens art

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

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

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

Om personuppgifterna får lämnas ut till externa parter ska det framgå i avtalet eller i dokumenterade instruktioner. Avtalet kan innehålla bestämmelser om vem som ska kunna få tillgång till personuppgifterna och på vilka villkor det kan ske. För att personuppgiftsbiträdet ska kunna överföra personuppgifter till något land utanför EU, krävs att det finns dokumenterade instruktioner från den personuppgiftsansvariga myndigheten eller att överföringen grundar sig på en rättsregel som personuppgiftsbiträdet i så fall måste underrätta den personuppgiftsansvariga om detta innan personuppgifterna överförs (artikel 28.3 a).

### 3.2 Behandlingens ändamål

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

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

### 3.3 Personuppgiftsbiträdets skyldigheter

I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet

a) endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige,
b) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,
c) ska vidta alla åtgärder som krävs enligt artikel 32 i dataskyddsförordningen,
d) ska respektera de villkor som anges i dataskyddsförordningen för anlitandet av ett annat personuppgiftsbiträde,
e) med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvariga kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,
f) ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32-36 i dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå,
g) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida det inte finns något särskilt lagkrav beträffande lagring av personuppgifterna och
h) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige (säkerhetsrevisorn)

Enligt artikel 32 i dataskyddsförordningen ska lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas. I avtalet behöver det klarläggas vilken säkerhetsnivån beträffande sekretess, integritet och tillgänglighet ska vara. Det behöver finnas bestämmelser om behörighetskontroll, till exempel loggföring, samt om fysiska säkerhetsåtgärder

### 3.4 Tillvaratagande av enskildas rättigheter

Arbetsfördelningen mellan personuppgiftsansvarig och personuppgiftsbiträdet bör framgå av avtalet, till exempel vem som ska hantera och behandla förfrågningar från registrerade. Den personuppgiftsansvariga myndigheten kan få en förfrågan som denna vidareförmedlar till personuppgiftsbiträdet som behandlar förfrågan. Det kan gälla förfrågningar om t.ex.

- Information till den registrerade.
- Rättelse av personuppgifter.
- Radering av personuppgifter.

### 3.5 Avtalets giltighetstid

Avtalet ska innehålla följande uppgifter

- Hur länge avtalet är i kraft
- 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

## 4. Krav på register över behandling av personuppgifter

Enligt artikel 30.2 i dataskyddsförordningen är varje personuppgiftsbiträde skyldigt att föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvarigas räkning. Registret ska på begäran göras tillgängligt för Datainspektionen. Registret ska innehålla:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar, och, i tillämpliga fall, för den personuppgiftsansvariges eller personuppgiftsbiträdes företrädare samt dataskyddsombudet.
b) De kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning.
c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
d) En allmän beskrivning (om möjligt) av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 i dataskyddsförordningen.

I artikel 30.5 finns ett undantag från skyldigheten att upprätta registerbeskrivningar för företag eller organisationer som sysselsätter färre än 250 personer. Dock gäller detta undantag inte all behandling av personuppgifter. Även om antalet anställda är mindre än 250 personer **måste** register över behandling ändå föras ifall något av följande gäller:

- Behandlingen kommer sannolikt att medföra en risk för registrerades rättigheter och friheter. Exempel: lokalisering av anställda genom GPS.
- Behandlingen är **inte** tillfällig. Exempel: behandling av anställdas personuppgifter för att kunna betala ut löner.
- Behandlingen omfattar särskilda kategorier av personuppgifter enligt artikel 9 eller personuppgifter som rör fällande domar i brottmål samt överträdelser enligt artikel 10. Exempel: behandling av uppgifter om anställdas hälsa.

## 5. Personuppgiftsbiträdets anlitande av ett annat personuppgiftsbiträde

Om personuppgiftsbiträdet använder sig av tjänsteunderleverantörer ska det klart framgå av personuppgiftsbiträdesavtalet eller av ett skriftligt förhandstillstånd i annan form (artikel 28.2). Dataskyddsförordningen ställer krav på säkerheten vid behandling av personuppgifter. Samtliga som på personuppgiftsbiträdets uppdrag utför arbete där de aktuella personuppgifterna ingår ska känna till de avtalsmässiga och lagbaserade villkoren. I enlighet med dataskyddsförordningen måste ett avtal upprättas mellan personuppgiftsbiträdet och underleverantörerna.

Detta dokument ersätter Datainspektionen informerar Nr 3/2016, gällande skriftligt avtal om registerbiträdets behandling av personuppgifter för den personuppgiftsansvarigas räkning (registerbiträdesavtal).

# BILAGA: Avtalsskiss – avtal om behandling av personuppgifter

**Avtal om behandling av personuppgifter**
**i enlighet med artikel 28.3 i EU:s dataskyddsförordning**

mellan

.....
Personuppgiftsansvarig

och

.....
Personuppgiftsbiträde

1. **Avsikten med avtalet**

2. **Ändamålet med behandlingen av personuppgifter**

3. **Typen av personuppgifter som ska behandlas**

4. **Kategorier av personer vilkas personuppgifter ska behandlas**

5. **Den personuppgiftsansvariges skyldigheter och rättigheter gentemot personuppgiftsbiträdet**

6. **Personuppgiftsbiträdets skyldigheter**

*Personuppgiftsbiträdet får endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige.*

*Personuppgiftsbiträdet ska säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lagstadgad tystnadsplikt.*

*Personuppgiftsbiträdet ska vidta alla åtgärder som krävs enligt artikel 32 i dataskyddsförordningen.*

*Personuppgiftsbiträdet ska respektera villkoren i dataskyddsförordningen för anlitande av ett annat personuppgiftsbiträde.*

*Personuppgiftsbiträdet ska med tanke på behandlingens art, hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter.*

*Personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 i dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.*

*Personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i artikel 28 i dataskyddsförordningen har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som har bemyndigats av den personuppgiftsansvarige.*

*Övriga skyldigheter för personuppgiftsbiträdet.*

## 7. Avtalets giltighetstid

## 8. Personuppgiftsbiträdets åtgärder vid avtalets upphörande

*Personuppgiftsbiträdet ska, beroende på vad den personuppgiftsansvarige väljer, radera eller återlämna alla personuppgifter till den personuppgifts-ansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida det inte finns något särskild lagkrav beträffande lagring av personuppgifterna.*

Avtalet är upprättat i två exemplar, vardera ett för personuppgiftsansvarig och personuppgiftsbiträde.

Ort och tid

| Personuppgiftsansvarig | Personuppgiftsbiträde |
|---|---|
| ..... | ..... |
| (underskrift) | (underskrift) |