

Dnr 76/2020

Bilaga 6

Utkast till Personuppgiftsbiträdes- avtal

Statens inköpscentral vid Kammarkollegiets anvisningar:

Detta dokument är ett utkast till Personuppgiftsbiträdesavtal.

Personuppgiftsansvarig modifierar och anpassar utkastet utifrån de specifika förutsättningar som varje avrop innebär. Tänk på att Ramavtalet ska läsas tillsammans med Personuppgiftsbiträdesavtalet.

Punkt 4.1 fokuserar på säkerhet och kan anpassas utifrån den tänkta behandlingen.

De gula fälten måste hanteras inför avrop. Vissa delar framgår av leverantörens avropssvar och fylls i senast vid kontraktstecknande.



Innehåll

1	Personuppgiftsbiträdesavtalets syfte.....	3
2	Parter	3
3	Allmänt om Personuppgiftsbiträdesavtalet.....	4
4	Personuppgiftsbiträdets skyldigheter.....	4
5	Behandling med hjälp av underbiträden.....	7
6	Skyldigheter efter Kontrakts upphörande.....	8
7	Ändringar i personuppgiftsbiträdesavtal	8
8	Giltighetstid	9
9	Skadestånd	9
	Instruktion till Personuppgiftsbiträdesavtal	10
	Avsnitt 1 Behandling som omfattas av Personuppgiftsbiträdesavtal	10
	Avsnitt 2 Underbiträden	12
	Avsnitt 3 Tekniska och organisatoriska säkerhetsåtgärder.....	13



1 Personuppgiftsbiträdesavtalets syfte

Detta Personuppgiftsbiträdesavtal reglerar Personuppgiftsbitrådets behandling av personuppgifter för den Personuppgiftsansvariges räkning. Avtalet är utformat med beaktande av kraven i EU:s dataskyddsförordning (EU) 2016/679, men kan – med eventuellt nödvändiga justeringar – användas för personuppgiftsbehandling som regleras av andra dataskyddsbestämmelser.

Notera att den andra delen av detta Personuppgiftsbiträdesavtal ”Instruktion till Personuppgiftsbiträdesavtal” måste fyllas i av parterna för att dataskyddslagstiftningens krav ska kunna uppfyllas.

2 Parter

Personuppgiftsansvarig:

Adress:

Telefonnummer:

E-postadress:

Organisationsnummer:

och

Personuppgiftsbiträde:

Adress:

Telefonnummer:

E-postadress:

Organisationsnummer:



3 Allmänt om Personuppgiftsbiträdesavtalet

- 3.1 Detta Personuppgiftsbiträdesavtal utgör en del av avrop från Ramavtal programvaror och tjänster, Systemutveckling dnr 23.3-5559-17.
- 3.2 Vissa begrepp som används i detta Personuppgiftsbiträdesavtal definieras i Ramavtalet. Dataskyddsrättsliga begrepp används med samma innebörd som i EU:s dataskyddsförordning.
- 3.3 Om Personuppgiftsbiträde inte är Ramavtalsleverantör ska Ramavtalsleverantör godkänna Personuppgiftsbiträdesavtal.
- 3.4 Personuppgiftsbiträdesavtal gäller behandlingar av personuppgifter som Personuppgiftsbiträde utför för den Personuppgiftsansvariges räkning. Dessa behandlingar förtecknas i avsnitt 1 i Instruktion till Personuppgiftsbiträdesavtal.
- 3.5 Alla behandlingar av personuppgifter som regleras i Personuppgiftsbiträdesavtal omfattas av EU:s dataskyddsförordning eller annan författning som reglerar behandling av personuppgifter.
- 3.6 Personuppgiftsbiträde garanterar att dennes verksamhet bedrivs på sätt som säkerställer dataskyddslagstiftningens krav på lämpliga tekniska och organisatoriska åtgärder och på att den registrerades rättigheter skyddas. Personuppgiftsbiträde garanterar att det har tillräcklig kunskap och förfogar över tillräckliga resurser för att dataskyddslagstiftningens krav ska kunna tillgodoses.
- 3.7 Om Personuppgiftsbiträde kommer att behandla personuppgifter i tredje land ska det framgå av instruktionen. Parterna måste i denna situation komma överens om en lämplig rättslig lösning för att överföringen till tredje land ska vara tillåten (jfr kapitel V i EU:s dataskyddsförordning eller motsvarande dataskyddsreglering).

4 Personuppgiftsbiträdets skyldigheter

- 4.1 För att skydda behandlingen av personuppgifter mot bl.a. obehörig åtkomst, förstörelse eller ändring ska Personuppgiftsbiträde vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med dataskyddslagstiftningens krav.

Personuppgiftsbiträde ska under alla förutsättningar vidta de säkerhetsåtgärder som framgår nedan.

När datorutrustning och löstagbara datamedier hos Personuppgiftsbiträde inte står under uppsikt ska utrustningen och medierna låsas in för att skyddas mot obehörig användning, påverkan och stöld.



För det fall eventuella bärbara datorer eller dylik utrustning används vid behandlingar ska personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.

Personuppgifterna ska regelbundet överföras till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas. Personuppgiftsbiträde ska ha en rutin för regelbunden test av återläsning.

Ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna för Personuppgiftsbiträde. Användaridentitet ska vara personlig och får inte överlåtas på någon annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter.

Åtkomst till personuppgifter ska kunna följas upp genom en logg eller liknande underlag. Underlaget ska kunna kontrolleras av Personuppgiftsbiträde och återrapporteras till den Personuppgiftsansvarige.

Anslutning för extern datorkommunikation ska skyddas med sådan teknisk funktion som säkerställer att uppkopplingen är behörig.

För åtkomst till känsliga personuppgifter krävs stark autentisering.

Personuppgifter som överförs via datorkommunikation utanför lokaler som kontrolleras av Personuppgiftsbiträde ska skyddas med kryptering.

När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre ska användas för sitt ändamål ska personuppgifterna raderas på sådant sätt att de inte kan återskapas.

Ytterligare preciseringar av tekniska och organisatoriska säkerhetsåtgärder kan framgå av avsnitt 3 i Instruktion till Personuppgiftsbiträdesavtal samt av övriga avtalshandlingar.

- 4.2 Personuppgiftsbiträde får inte behandla den Personuppgiftsansvariges personuppgifter på något annat sätt, för andra ändamål eller enligt andra instruktioner än de som framgår av detta Personuppgiftsbiträdesavtal, inklusive avsnitt 1 i Instruktion till Personuppgiftsbiträdesavtal, med iakttagande av de tekniska och organisatoriska säkerhetsåtgärderna enligt detta Personuppgiftsbiträdesavtal och avsnitt 3 i Instruktion till Personuppgiftsbiträdesavtal.

Första stycket gäller inte om en behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som Personuppgiftsbiträde omfattas av. I sådana fall ska Personuppgiftsbiträde informera den Personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida detta inte är otillåtet enligt den aktuella rättsordningen.

- 4.3 Om Personuppgiftsbiträde bedömer att det saknas instruktioner för hur den Personuppgiftsansvariges personuppgifter ska behandlas ska Personuppgiftsbiträde utan dröjsmål informera den Personuppgiftsansvarige om sin inställning, ange om fullgörandet av Kontrakt kan påverkas av behovet av instruktioner samt invänta vidare instruktioner från den Personuppgiftsansvarige.



Om Personuppgiftsbiträde bedömer att instruktioner om hur personuppgifter ska behandlas strider mot tillämpliga dataskyddsbestämmelser ska Personuppgiftsbiträde omedelbart informera den Personuppgiftsansvarige om detta.

- 4.4 Personuppgiftsbiträde åtar sig att i sin verksamhet vid var tid tillse att berörd personal följer detta Personuppgiftsbiträdesavtal och att de hålls informerade om innehållet i dataskyddslagstiftningen.

Personer som utför arbete under Personuppgiftsbiträdes överinseende, t.ex. som anställda, och som får tillgång till personuppgifter, får endast behandla uppgifterna enligt den Personuppgiftsansvariges instruktioner, såvida inte en skyldighet att göra något annat framgår i unionsrätten eller medlemsstaternas nationella rätt. Endast personer som har ett strikt behov av att få tillgång till personuppgifterna ska ges sådan tillgång.

Personuppgiftsbiträde garanterar att personer som får tillgång till personuppgifter har åtagit sig att iaktta konfidentialitet eller omfattas av lämplig lagstadgad tystnadsplikt.

- 4.5 Personuppgiftsbiträde ska efter den Personuppgiftsansvariges beslut om radering av personuppgifter avlägsna dessa permanent från alla lagringsmedier som biträdet förfogar över. Detta ska ske snarast, dock senast 180 dagar efter beslut om radering. Som beslut om radering räknas t.ex. att uppgifter har raderats via användargränssnittet i den tjänst som omfattas av Kontrakt.
- 4.6 Personuppgiftsbiträde ska efter att biträdet fått vetskap om en personuppgiftsincident som omfattar den Personuppgiftsansvariges personuppgifter utan onödigt dröjsmål underrätta den Personuppgiftsansvarige om incidenten. Underrättelsen ska innehålla den information som krävs för att den Personuppgiftsansvarige ska kunna fullgöra sina skyldigheter enligt dataskyddslagstiftningen.

Personuppgiftsbiträde ska på begäran från den Personuppgiftsansvarige lämna nödvändig information och i övrigt bistå den Personuppgiftsansvarige så att denne kan uppfylla sina skyldigheter beträffande säkerheten i behandlingen och konsekvensbedömningen avseende dataskydd.

- 4.7 För det fall den registrerade, tillsynsmyndigheten eller annan tredje man begär information från Personuppgiftsbiträde som rör behandling av personuppgifter, ska Personuppgiftsbiträde hänvisa till den Personuppgiftsansvarige. Personuppgiftsbiträde får inte lämna ut personuppgifter eller annan information om behandlingen av personuppgifter utan uttrycklig instruktion från den Personuppgiftsansvarige, såvida utlämnandeskyldigheten inte framgår i unionsrätten eller tillämplig nationell lag i en medlemsstat.
- 4.8 Personuppgiftsbiträde ska utan dröjsmål informera den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndigheten som rör, eller kan vara av betydelse för, Personuppgiftsbiträdes behandling av personuppgifter. Åtagandet gäller inte om Personuppgiftsbiträde är förbjudet att lämna den aktuella informationen enligt tvingande lagstiftning.

Personuppgiftsbiträde har inte rätt att företräda den Personuppgiftsansvarige eller agera för dennes räkning gentemot tillsynsmyndigheten.



- 4.9 Den Personuppgiftsansvarige har rätt att kontrollera att Personuppgiftsbiträde följer Personuppgiftsbiträdesavtal och instruktioner som utfärdats av den Personuppgiftsansvarige. Personuppgiftsbiträde ska för detta ändamål ge den Personuppgiftsansvarige tillgång till all nödvändig information samt möjliggöra och bidra till granskningar inbegripet inspektioner som genomförs av den Personuppgiftsansvarige eller av en granskare som bemyndigats av den Personuppgiftsansvarige. Den som granskar bitrådets verksamhet ska iaktta regler om sekretess för bitrådets affärs- och driftsförhållanden.
- 4.10 Uppgifter i loggar som avser behandlingen av den Personuppgiftsansvariges personuppgifter får endast användas av Personuppgiftsbiträde för vad som krävs för upprätthållande av funktionalitet och kvalitet. Den Personuppgiftsansvarige har rätt att ta del av de uppgifter som registreras i sådana loggar.
- 4.11 Personuppgiftsbiträde ska, med beaktande av behandlingens art, genom lämpliga tekniska och organisatoriska åtgärder hjälpa den Personuppgiftsansvarige att fullgöra sina skyldigheter att tillgodose den registrerades rättigheter, t.ex. rätten till information, rätten till rättelse, rätten till radering eller begränsning av behandlingen och rätten till dataportabilitet.

5 Behandling med hjälp av underbiträden

- 5.1 Personuppgiftsbiträde äger endast rätt att anlita ett annat Personuppgiftsbiträde (underbiträde) för behandling av personuppgifter om detta anges i instruktionen.

Den Personuppgiftsansvarige har i instruktionen till detta Personuppgiftsbiträdesavtal angivit vilka underbiträden som är godkända vid Personuppgiftsbiträdesavtals ikraftträdande.

Personuppgiftsbiträde ska tillse att underbiträde inte anlitar ett annat underbiträde utan den Personuppgiftsansvariges skriftliga förhandstillstånd.

- 5.2 Om personuppgiftsbiträde med stöd i detta Personuppgiftsbiträdesavtal anlitar ett underbiträde för hela eller en del av behandlingen ska underbiträdet genom avtal åläggas samma skyldigheter avseende dataskydd som de som fastställs i detta Personuppgiftsbiträdesavtal och vid varje tidpunkt gällande instruktioner rörande behandlingen.
- 5.3 Vid en begäran om att få anlita ett nytt underbiträde ska Personuppgiftsbiträde lämna den Personuppgiftsansvarige all relevant information om det föreslagna underbiträdet som krävs för en dataskyddsrettslig bedömning. Information ska därvid särskilt lämnas om i vilket land som underbiträdet kommer att behandla personuppgifterna och vilka typer av behandlingar som underbiträdet är tänkt att utföra.
- 5.4 Personuppgiftsbiträde ska hålla en förteckning över de underbiträden som vid den aktuella tidpunkten anlitas, samt göra denna förteckning tillgänglig för den Personuppgiftsansvarige. Av förteckningen ska särskilt framgå i vilka länder underbiträdet behandlar personuppgifterna och vilka typer av behandlingar som underbiträdet utför. På



begäran ska Personuppgiftsbiträde lämna den Personuppgiftsansvarige information om ett underbiträdes rättsliga åtaganden samt övrig information som krävs för att den Personuppgiftsansvarige ska kunna fullgöra sina skyldigheter enligt dataskyddslagstiftningen.

- 5.5 Om ett underbiträde inte fullgör sina skyldigheter avseende dataskydd är Personuppgiftsbiträde fullt ansvarigt i förhållande till den Personuppgiftsansvarige.
- 5.6 Har den Personuppgiftsansvarige enligt reglerna i detta avsnitt godtagit behandling av personuppgifter i tredje land ansvarar Personuppgiftsbiträde för att överföringen till ett sådant tredje land sker enligt tillämpliga dataskyddsregler (t.ex. kapitel V i EU:s dataskyddsförordning).

6 Skyldigheter efter Kontrakts upphörande

- 6.1 Personuppgiftsbiträde ska i samband med Kontrakts upphörande permanent avlägsna uppgifterna från använda lagringsmedier på ett sådant sätt att uppgifterna inte längre kan återskapas. Denna åtgärd ska vara fullt genomförd senast 180 dagar efter Kontrakts upphörande.

Om den Personuppgiftsansvarige kräver det ska Personuppgiftsbiträde innan sådan radering sker återlämna alla överförda personuppgifter till den Personuppgiftsansvarige. Såvida inte annat avtalats eller uppenbart följer av omständigheterna, ska personuppgifterna överlämnas i ett format som är läsbart och möjligt att använda i andra sammanhang. Detta innebär att inte enbart personuppgifterna ska tillhandahållas utan även all annan logisk information som behövs för att kunna nyttja personuppgifterna. Vidare ska också loggfiler, revisionsdata, accessdata och liknande metadata tillhandahållas. Även sådan data ska lämnas i ett sådant format att den är användbar för Personuppgiftsansvarig.

- 6.2 Personuppgiftsbiträde ska på den Personuppgiftsansvariges eller en behörig tillsynsmyndighets begäran ställa relevanta delar av använda lagringsmedium till förfogande för en granskning av de åtgärder som anges i punkt 6.1.

7 Ändringar i personuppgiftsbiträdesavtal

- 7.1 Den Personuppgiftsansvarige har rätt att påkalla ändring av Personuppgiftsbiträdesavtal om en sådan ändring är nödvändig för att tillämplig dataskyddslagstiftning ska kunna efterlevas.

Ändring ska hanteras i enlighet med Ramavtalet. Personuppgiftsbiträde får inte motsätta sig ändringen om inte Personuppgiftsbiträde kan visa sakliga skäl för en sådan vägran. Om Personuppgiftsbiträde inte är Ramavtalsleverantör får inte heller Ramavtalsleverantör motsätta sig en sådan ändring utan att kunna visa sakliga skäl.



Om Personuppgiftsbiträde inte är Ramavtalsleverantör ska även Ramavtalsleverantör godkänna ändringen.

8 Giltighetstid

- 8.1 Detta Personuppgiftsbiträdesavtal gäller från undertecknandet och så länge som Personuppgiftsbiträde behandlar den Personuppgiftsansvariges personuppgifter. Regler om uppsägning av Kontrakt finns i Ramavtalet.

9 Skadestånd

- 9.1 Ansvar för skada regleras i enlighet med Artikel 82 i dataskyddsförordning (EU) 2016/679. Kund har regressrätt mot Ramavtalsleverantör oaktat vem som är Personuppgiftsbiträde.



Instruktion till Personuppgiftsbiträdesavtal

Avsnitt 1 Behandling som omfattas av Personuppgiftsbiträdesavtal

Denna del utgör den Personuppgiftsansvariges instruktioner till Personuppgiftsbiträde.

Registrerade

Personuppgifter som rör följande kategorier av registrerade ska behandlas av Personuppgiftsbiträde:

Besökare på webbplatsen som anmäler till Konkurrensverket att de till exempel ett delta i ett seminarium, beställa publikationer eller prenumerera på nyheter eller nyhetsbrev.

Typ av personuppgifter som överförs

De personuppgifter som överförs är av följande slag:

Namn, organisation, adress, e-postadress, telefonnummer, särskilda önskemål kring kost eller andra önskemål.

Känsliga personuppgifter (i förekommande fall)

Överföringen rör följande känsliga personuppgifter:



Personliga önskemål så som allergi eller särskild kost.

Behandling

De personuppgifter som överförs kommer att behandlas på följande sätt:

Fylls i vid avtalstecknandet

Art och ändamål med behandlingarna

Behandlingen av personuppgifter sker i syfte att:

Fylls i vid avtalstecknandet

Särskilda instruktioner angående behandlingarna

Vid behandlingen av personuppgifter ska Personuppgiftsbiträde särskilt beakta:

Fylls i vid avtalstecknandet

Behandling med hjälp av underbiträden

- Personuppgiftsbiträde äger inte rätt att anlita ett annat Personuppgiftsbiträde (underbiträde) enligt denna instruktion.
- Personuppgiftsbiträde får endast anlita ett annat Personuppgiftsbiträde om ett skriftligt förhandstillstånd har inhämtats från den Personuppgiftsansvarige.
- Personuppgiftsbiträde har en allmän rätt att anlita ett nytt Personuppgiftsbiträde (underbiträde), som uppfyller dataskyddslagstiftningen och Personuppgiftsbiträdesavtals krav. Ett nytt underbiträde får emellertid endast anlitas efter det att den Personuppgiftsansvarige har underrättats om planerna och givits möjlighet att inom skälig tid göra invändningar mot valet.



Behandling av personuppgifter inom Sverige, EU/EES samt tredje land

Alternativ 1: Personuppgifter får endast behandlas inom Sverige.

Alternativ 2: Personuppgifter får behandlas inom EU/EES.

Alternativ 3: Personuppgifter får överföras till ett tredje land. Ange rättslig lösning för att sådan överföring ska vara tillåten:

Molntjänst/molndrift driftas inom EU/EES. Om leverantören är ansluten till Privacy Shield accepterar Konkurrensverket även en sådan lösning.

Vid alternativ 2 eller 3 ovan, ange land där Personuppgiftsbiträde kommer att hantera personuppgifter:

Fylls i.

Avsnitt 2 Underbiträden

I detta avsnitt förtecknas underbiträden som har godkänts av den Personuppgiftsansvarige. Enligt punkt 5.4 är Personuppgiftsbiträde skyldigt att hålla en aktuell förteckning över underbiträden som anlitas.

Underbiträde (namn)	Organisationsnummer	Bistår Personuppgiftsbiträde med följande	Behandling sker i (land)
Fylls i vid behov.	Fylls i vid behov.	Fylls i vid behov.	Fylls i vid behov.



Avsnitt 3 Tekniska och organisatoriska säkerhetsåtgärder

Detta avsnitt utgör kompletterande instruktioner till Personuppgiftsbiträde avseende tekniska och organisatoriska säkerhetsåtgärder.

Ange kompletterande instruktioner:

Fylls i vid behov.

På Personuppgiftsansvarigs vägnar:

Namn (fullständigt):

Befattning:

Ort och datum:

.....
Namnteckning

På Personuppgiftsbiträdes vägnar:

Namn (fullständigt):

Befattning:

Ort och datum:

.....
Namnteckning

På Ramavtalsleverantörs vägnar (om denne inte är Personuppgiftsbiträde):

Namn (fullständigt):

Befattning:

Ort och datum:

.....
Namnteckning