# Bilaga

# Utkast till Person-uppgiftsbiträdesavtal

# Datacenter 2019

23.3-5432-19

***Kammarkollegiets anvisningar:***
*Detta dokument är ett utkast till personuppgiftsbiträdesavtal.*

*Personuppgiftsansvarig modifierar och anpassar utkastet utifrån de specifika förutsättningarna i avropet. Ramavtalet ska läsas tillsammans med personuppgiftsbiträdesavtalet.*

*Avsnitt 5 behandlar i första hand säkerhet och kan i Instruktion till personuppgiftsbiträdesavtalet anpassas utifrån den tänkta behandlingen.*

*Textrutor och radioknappar måste hanteras inför avrop. Vissa delar framgår av leverantörens avropssvar och fylls i senast vid kontraktstecknande.*

KAMMARKOLLEGIET

# Innehåll

# 1 Personuppgiftsbiträdes-avtalets syfte

1.1 Detta personuppgiftsbiträdesavtal har till syfte att reglera personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. Avtalet är utformat med beaktande av kraven i EU:s dataskyddsförordning (EU) 2016/679 (hädanefter dataskyddsförordningen), men kan – med eventuellt nödvändiga justeringar – även användas för personuppgiftsbehandling som regleras av andra dataskyddsbestämmelser.

1.2 Instruktion till personuppgiftsbiträdesavtalet (hädanefter instruktionen) fylls i av parterna för att kraven i dataskyddsförordningen och annan tillämplig författning som reglerar behandling av personuppgifter ska kunna uppfyllas.

# 2 Parter

**Personuppgiftsansvarig:**

Adress:

Telefonnummer:

E-postadress:

Organisationsnummer:

och

**Personuppgiftsbiträde:**

Adress:

Telefonnummer:

E-postadress:

Organisationsnummer:

# 3 Allmänt om Personuppgifts-biträdesavtalet

3.1 Detta personuppgiftsbiträdesavtal utgör en bilaga till avropet från ramavtalet Datacenter 2019, dnr: 23.3-5432-19.

3.2 Vissa begrepp som används i detta personuppgiftsbiträdesavtal definieras i ramavtalet. Dataskyddsrättsliga begrepp används med samma innebörd som i dataskyddsförordningen.

3.3 Om ramavtalsleverantör inte är personuppgiftsbiträde ska ramavtalsleverantör, genom sin underskrift, godkänna personuppgiftsbiträdesavtalet.

3.4 Personuppgiftsbiträdesavtalet gäller behandlingar av personuppgifter som personuppgiftsbiträdet utför för den personuppgiftsansvariges räkning. Dessa behandlingar förtecknas i avsnitt 1 i instruktionen. Alla behandlingar av personuppgifter enligt personuppgiftsbiträdesavtalet omfattas av dataskyddsregleringen.

# 4 Personuppgiftsansvariges generella åtaganden

4.1 Den personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för behandlingen och för att utforma korrekta instruktioner så att personuppgiftsbiträdet kan fullgöra sitt uppdrag enligt detta personuppgiftsbiträdesavtal.

4.2 Den personuppgiftsansvarige ansvarar för att informera registrerade om behandlingen, tillvarata den registrerades rättigheter samt att vidta varje annan åtgärd som åligger den personuppgiftsansvarige enligt dataskyddslagsregleringen.

# 5 Personuppgiftsbiträdets generella åtaganden

5.1 Personuppgiftsbiträdet garanterar att dennes verksamhet bedrivs på ett sätt som säkerställer dataskyddsregleringens krav på lämpliga tekniska och organisatoriska åtgärder och att den registrerades rättigheter skyddas. Personuppgiftsbiträdet garanterar att det har tillräcklig kunskap och förfogar över tillräckliga resurser för att dataskyddsregleringens krav ska kunna tillgodoses.

5.2 Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till risken för oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörig åtkomst till den personuppgiftsansvariges personuppgifter.

5.3 Personuppgiftsbiträdet ska under alla förutsättningar vidta de säkerhetsåtgärder som framgår av punkterna 5.4 – 5.9.

5.4 När datorutrustning och löstagbara datamedier hos personuppgiftsbiträdet 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 behandlingen ska personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.

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

5.6 Ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna för personuppgiftsbiträdet. 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 personuppgiftsbiträdet och återrapporteras till den personuppgiftsansvarige.

5.7 Uppgifter i loggar som avser behandlingen av den personuppgiftsansvariges personuppgifter får endast användas av personuppgiftsbiträdet 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.

5.8 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 personuppgiftsbiträdet ska skyddas med kryptering.

5.9 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.

5.10 Ytterligare preciseringar av tekniska och organisatoriska säkerhetsåtgärder kan framgå av avsnitt 3 i instruktionen samt av övriga avtalshandlingar.

# 6 Behandling av personuppgifter

6.1 Personuppgiftsbiträdet 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 instruktionen. Behandlingen av personuppgifter ska ske med iakttagande av de tekniska och organisatoriska säkerhetsåtgärder som följer av detta personuppgiftsbiträdesavtal och avsnitt 3 instruktionen.

Första stycket gäller inte om en behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I sådana fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt. Innan personuppgiftsbiträdet står inför att behandla personuppgifter enligt andra stycket ska personuppgiftsbiträdet ha gjort en kvalificerad rättslig prövning av om behandlingen får ske. I tveksamma fall, eller om prövningen visar att behandlingen inte får ske, ska personuppgiftsbiträdet motsätta sig det rättsliga kravet på behandling för att erhålla ett lagakraftvunnet avgörande i syfte att säkerställa den registrerades rättigheter.

6.2 För det fall att personuppgiftsbiträdet finner att instruktioner är otydliga, i strid med dataskyddslagsregleringen eller saknas och personuppgiftsbiträdet bedömer att nya eller kompletterande instruktioner är nödvändiga för att genomföra sina åtaganden ska personuppgiftsbiträdet utan dröjsmål informera den personuppgiftsansvarige, tillfälligt upphöra med behandlingen och invänta nya instruktioner.

6.3 Personuppgiftsbiträdet åtar sig, att i sin verksamhet, vid var tid tillse att berörd personal följer detta personuppgiftsbiträdesavtal och att de hålls informerade om innehållet i dataskyddsregleringen.

6.4 Personer som utför arbete under personuppgiftsbiträdets 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 krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt. Endast personer som behöver uppgifterna för att kunna utföra sina arbetsuppgifter ska ges sådan tillgång.

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

6.6 Personuppgiftsbiträdet 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 beslutet om radering. Som beslut om radering räknas t.ex. att uppgifter har raderats via användargränssnittet i den tjänst som omfattas av kontraktet.

# 7 Den registrerades rättigheter

7.1 Personuppgiftsbiträdet ska på begäran från den personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt art. 32 - 36 dataskyddsförordningen fullgörs och svara på begäran om utövande av den registrerades rättigheter i enlighet med kap. III dataskyddsförordningen. Detta ska göras med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

# 8 Personuppgiftsincidenter

8.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt art. 32.1 c dataskyddsförordningen.

8.2 Personuppgiftsbiträdet åtar sig att, med beaktande av behandlingens art och den information som personuppgiftsbiträdet har att tillgå, bistå den personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en personuppgiftsincident beträffande behandlingen. Personuppgiftsbiträdet ska på den personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörig behandling och/eller åtkomst till personuppgifterna.

8.3 Vid personuppgiftsincidenter, vilka personuppgiftsbiträdet fått vetskap om, ska personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå tillhandahålla den personuppgiftsansvarige en skriftlig beskrivning av personuppgiftsincidenten.

Beskrivningen ska minst redogöra för:
1. personuppgiftsincidentens art och, om möjligt, de kategorier och antalet registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
2. de sannolika konsekvenserna av personuppgiftsincidenten, och
3. åtgärder som har vidtagits till följd av personuppgiftsincidenten, förslag för att ytterligare åtgärda personuppgiftsincidenten samt förslag på åtgärder för att mildra personuppgiftsincidentens potentiella negativa effekter.

# 9 Tillsyn och revision

9.1 För det fall registrerade, tillsynsmyndigheten eller annan tredje man begär information från personuppgiftsbiträdet som rör behandlingen av personuppgifter, ska personuppgiftsbiträdet hänvisa till den personuppgiftsansvarige. Personuppgiftsbiträdet får inte lämna ut personuppgifter eller annan information om behandlingen av personuppgifter utan uttrycklig instruktion från den personuppgiftsansvarige, såvida inte en sådan utlämnandeskyldighet krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt.

9.2 Personuppgiftsbiträdet 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 personuppgiftsbiträdet är förhindrat att lämna den aktuella informationen enligt tvingande lagstiftning.

9.3 Personuppgiftsbiträdet har inte rätt att företräda den personuppgiftsansvarige eller agera för dennes räkning gentemot tillsynsmyndigheten.

9.4 Den personuppgiftsansvarige äger rätt att själv eller genom en utsedd oberoende tredje part följa upp att personuppgiftsbiträdet uppfyller personuppgiftsbiträdesavtalets, instruktionernas och dataskyddsregleringens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den personuppgiftsansvarige, eller den som utför granskningen i den personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska personuppgiftsbiträdets efterlevnad av personuppgiftsbiträdesavtalet, instruktioner och dataskyddslagsregleringen. Den personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastad konfidentialitet enligt lag eller avtal.

# 10 Behandling med hjälp av underbiträden

10.1 Personuppgiftsbiträdet äger endast rätt att anlita ett annat personuppgiftsbiträde (underbiträde) för behandlingen av personuppgifter om detta anges i instruktionen.

10.2 Den personuppgiftsansvarige har i och med personuppgiftsbiträdesavtalets ikraftträdande godkänt de underbiträden som angivits i instruktionen.

10.3 Om personuppgiftsbiträdet 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.

10.4 Vid en begäran om att få anlita ett nytt underbiträde ska personuppgiftsbiträdet lämna den personuppgiftsansvarige all relevant information om det föreslagna underbiträdet som krävs för en dataskyddsrättslig 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.

10.5 Personuppgiftsbiträdet ska tillse att underbiträde inte anlitar ett annat underbiträde utan den personuppgiftsansvariges skriftliga förhandstillstånd.

10.6 Personuppgiftsbiträdet ska hålla en förteckning över de underbiträden som vid varje aktuell tidpunkt 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 personuppgiftsbiträdet lämna den personuppgiftsansvarige information om ett underbiträdes rättsliga åtaganden samt övrig information som krävs för att den personuppgiftsansvarige ska kunna fullgöra sina skyldigheter enligt dataskyddsregleringen.

10.7 Om ett underbiträde inte fullgör sina skyldigheter avseende dataskydd är personuppgiftsbiträdet fullt ansvarigt i förhållande till den personuppgiftsansvarige.

10.8 Om personuppgiftsbiträdet får 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 kap. V dataskyddsförordningen eller motsvarande dataskyddsreglering).

# 11 Skyldigheter efter kontraktets upphörande

11.1 I samband med kontraktets upphörande ska personuppgifterna återlämnas till den personuppgiftsansvarige såvida inte denne uttryckligen önskar att uppgifterna ska raderas. Efter att personuppgifter har återlämnats eller raderats ska eventuella kopior raderas från använda lagringsmedier på ett sådant sätt att uppgifterna inte längre kan återskapas. Denna åtgärd ska vara fullt genomförd senast 180 dagar efter kontraktets upphörande.

11.2 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, utöver personuppgifterna, även all annan logisk information som behövs för att kunna nyttja personuppgifterna ska tillhandahållas. Vidare ska också loggfiler, revisionsdata, accessdata och liknande metadata tillhandahållas. Även sådan data ska lämnas i ett sådant format att den är användbar för den personuppgiftsansvarige.

11.3 Personuppgiftsbiträdet 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 punkterna 11.1 - 11.2.

# 12 Ändringar i personuppgifts-biträdesavtalet

12.1 Den personuppgiftsansvarige har rätt att påkalla ändring av personuppgiftsbiträdesavtalet om en sådan ändring är nödvändig för att dataskyddslagregleringen ska kunna efterlevas.

12.2 Ändring ska hanteras i enlighet med ramavtalet. Personuppgiftsbiträdet får inte motsätta sig ändringen om inte personuppgiftsbiträdet kan visa sakliga skäl för en sådan vägran. Om ramavtalsleverantör inte är personuppgiftsbiträde får inte heller ramavtalsleverantör motsätta sig en sådan ändring utan att kunna visa sakliga skäl.

12.3 Om ramavtalsleverantör inte är personuppgiftsbiträde ska ramavtalsleverantör skriftligen godkänna ändringen.

# 13 Giltighetstid

13.1 Detta personuppgiftsbiträdesavtal gäller från undertecknandet och så länge som personuppgiftsbiträdet behandlar den personuppgiftsansvariges personuppgifter.

13.2 Bestämmelser avseende uppsägning av kontraktet följer av ramavtalet.

# 14 Ansvar för skada i samband med behandling

14.1 Vid ersättning för skada i samband med behandling som, genom fastställd dom eller beslut, utgått till den registrerade på grund av överträdelse av bestämmelse i

personuppgiftsbiträdesavtalet, instruktioner och/eller bestämmelse i dataskyddslagsregleringen ska art. 82 dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter ska enligt art. 83 dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till dataskyddsförordningen bäras av den av personuppgiftsbiträdesavtalets parter som påförts en sådan avgift.

14.3 Part som får kännedom om omständighet som kan leda till skada för motparten ska omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Den personuppgiftsansvarige har regressrätt avseende ansvar enligt 14.1 mot ramavtalsleverantören oaktat vem som är personuppgiftsbiträde. Den personuppgiftsansvarige har regressrätt gentemot ramavtalsleverantören, även för det fall annan leverantör är personuppgiftsbiträde, med anledning av att ramavtalsleverantören är bunden av ramavtalet och har godkänt personuppgiftsbiträdesavtalet.

# 15 Tvistelösning

15.1 Bestämmelser om tvist samt tillämplig lag med anledning av detta personuppgiftsbiträdesavtal regleras i ramavtalet.

# Instruktion till Personuppgiftsbiträdesavtalet

## Avsnitt 1 Behandling som omfattas av Personuppgiftsbiträdesavtalet

Denna del utgör den personuppgiftsansvariges instruktioner till personuppgiftsbiträdet.

**Registrerade**

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

| |
|---|
| |

**Typ av personuppgifter som behandlas**

De personuppgifter som behandlas är av följande slag:

| |
|---|
| |

**Känsliga personuppgifter (i förekommande fall)**

Behandlingen rör följande känsliga personuppgifter:

| |
|---|
| |

**Behandling**

Personuppgifter kommer att behandlas på följande sätt:

| |
|---|
| |

**Art och ändamål med behandlingen**

Behandlingen av personuppgifter sker i syfte att:

| |
|---|
| |

**Särskilda instruktioner angående behandlingen**

Vid behandlingen av personuppgifter ska personuppgiftsbiträde särskilt beakta:

| |
|---|
| |

**Behandling med hjälp av underbiträden**

○ Personuppgiftsbiträdet äger inte rätt att anlita ett annat personuppgiftsbiträde (underbiträde) enligt denna instruktion.

○ Personuppgiftsbiträdet får endast anlita ett annat personuppgiftsbiträde om ett skriftligt förhandstillstånd har inhämtats från den personuppgiftsansvarige.

○ Personuppgiftsbiträdet har en allmän rätt att anlita ett nytt personuppgiftsbiträde (underbiträde) som uppfyller dataskyddslagsregleringen och personuppgiftsbiträdesavtalets 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 endast behandlas inom EU/EES.

○ Alternativ 3: Personuppgifter får endast behandlas inom EU/EES och i angivet tredje land.

Vid alternativ 3 ovan, ange rättslig lösning enligt kap. V dataskyddsförordningen för att sådan behandling ska vara tillåten:

| |
|---|
| |

Vid alternativ 2 eller 3 ovan, ange land där personuppgiftsbehandling får förekomma:

| |
|---|
| |

# Avsnitt 2 Underbiträden

I detta avsnitt förtecknas underbiträden som har godkänts av den personuppgiftsansvarige. Enligt punkt 10.6 är personuppgiftsbiträdet skyldigt att hålla en vid varje tidpunkt aktuell förteckning över underbiträden som anlitas.

| **Underbiträde (namn)** | **Organisations -nummer** | **Bistår personuppgifts-biträdet med följande** | **Behandling sker i (land)** |
|---|---|---|---|

# Avsnitt 3 Tekniska och organisatoriska säkerhetsåtgärder

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

Ange kompletterande instruktioner:

På personuppgiftsansvarigs vägnar:

Namn (fullständigt):

Befattning:

Ort och datum:

…….

Namnteckning

På personuppgiftsbiträdets vägnar:

Namn (fullständigt):

Befattning:

Ort och datum:

…….

Namnteckning

På ramavtalsleverantörens vägnar (om denne inte är personuppgiftsbiträde):

Namn (fullständigt):

Befattning:

Ort och datum:

…….

Namnteckning