Bilaga
Utkast till
Personuppgifts-
biträdesavtal
AV och videokonferens

23.3-7192-16

KAMMARKOLLEGIET

Innehåll

1 Personuppgiftsbiträdes-avtalets syfte

Personuppgiftsbiträdets fullgörande av Kontrakt innebär att personuppgiftsbiträdet behandlar personuppgiftsansvarigs personuppgifter i enlighet med vad som stadgas i personuppgiftslagen (1998:204).

Detta Personuppgiftsbiträdesavtal syftar till att uppfylla stadgandet i 30 § personuppgiftslagen, som föreskriver att det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I Personuppgiftsbiträdesavtalet finns föreskrifter om att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

- de tekniska möjligheter som finns,
- vad det skulle kosta att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna, och
- hur känsliga de behandlade personuppgifterna är.

Kompletterande föreskrifter beträffande behandling av personuppgifter ges i personuppgiftsförordningen (1998:1191).

2 Parter

Namn på den personuppgiftsansvariges organisation:

Adress:
Telefonnummer:
Fax:
E-postadress:
Organisationsnummer:

och

Namn på personuppgiftsbiträdets organisation:

Adress:
Telefonnummer:
Fax:
E-postadress:
Organisationsnummer:

Har tecknat följande Personuppgiftsbiträdesavtal för att säkerställa ett adekvat skydd för privatliv och grundläggande rättigheter och friheter för enskilda i samband med överföring från personuppgiftsansvarig till personuppgiftsbiträdet av sådana personuppgifter som anges i Personuppgiftsbiträdesavtalets avsnitt 10 (Behandlingar omfattade av Personuppgiftsbiträdesavtalet).

3 Definitioner

Samtliga definitioner och termer som används i detta Personuppgiftsbiträdesavtal är definierade i bilaga Allmänna villkor.

4 Allmänt om Personuppgiftsbiträdes-avtalet

4.1 Detta Personuppgiftsbiträdesavtal utgör en del av Ramavtalet AV och videokonferens, diarienummer 23.3-7192-16.

4.2 Information om behandlingen, och i förekommande fall om känsliga eller integritetskänsliga personuppgifter avses att behandlas, anges i avsnitt 10 (Behandlingar omfattade av Personuppgiftsbiträdesavtalet).

4.3 Alla behandlingar av personuppgifter som regleras i Personuppgiftsbiträdesavtalet omfattas av personuppgiftslagens (1998:204) bestämmelser, eller annan författning som reglerar behandling av personuppgifter.

4.4 Genom signeringen ges den personuppgiftsansvarige rätt att följa upp att personuppgiftsbiträdet lever upp till den personuppgiftsansvariges krav på behandlingen och verkligen vidtar lämpliga tekniska och organisatoriska säkerhetsåtgärder.

4.5 Personuppgiftsbiträdet intygar att dennes verksamhet bedrivs på sätt som säkerställer att personuppgiftslagens bestämmelser och krav avseende adekvat skydd för personuppgiftsbehandlingar efterlevs.

5 Personuppgiftsbiträdets skyldigheter

5.1 För att skydda behandlingen av personuppgifter mot obehörig åtkomst, förstörelse eller ändring ska personuppgiftsbiträdet vidta sådana tekniska och organisatoriska säkerhetsåtgärder som anges i avsnitt 11 (Tekniska och organisatoriska säkerhetsåtgärder), i syfte att upprätthålla en lämplig säkerhetsnivå. Personuppgiftsbiträdet åtar sig att i sin verksamhet vid var tid tillse att berörd personal följer Personuppgiftsbiträdesavtalet, de instruktioner som ges av den

personuppgiftsansvarige samt att de hålls informerade om innehållet i personuppgiftslagen. Det är ytterst den personuppgiftsansvarige som bedömer vilka säkerhetsåtgärder som minst måste vidtas.

5.2 Personuppgiftsbiträdet ska omgående underrätta den personuppgiftsansvarige vid upptäckt av fullbordade fall av eller försök till obehörig åtkomst, förstörelse eller ändring av personuppgifter.

5.3 Personuppgiftsbiträdet får inte behandla personuppgifter på något annat sätt, för andra ändamål eller enligt andra instruktioner än de som anges i avsnitt 10 (Behandlingar omfattade av Personuppgiftsbiträdesavtalet) med iakttagande av de tekniska och organisatoriska säkerhetsåtgärder som anges i avsnitt 11 (Tekniska och organisatoriska säkerhetsåtgärder). För det fall att personuppgiftsbiträdet bedömer att det saknas instruktioner som är nödvändiga för att genomföra uppdraget enligt vad som sägs i detta Personuppgiftsbiträdesavtal ska personuppgiftsbiträdet 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.

5.4 Personuppgiftsbiträdet och eventuella underbiträden ska efter personuppgiftsansvarigs beslut om radering av personuppgifter antingen radera dessa helt från det medium där de lagras eller att de avidentifieras på ett sådant sätt att de inte är möjliga att koppla till en enskild individ eller går att återskapa. Radering ska vara utförd senast 180 dagar efter beslut omradering.

5.5 För det fall den registrerade, tillsynsmyndigheten eller annan tredje man begär information från personuppgiftsbiträdet som rör behandling 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, eller om utlämnandet är en följd av en laglig skyldighet.

5.6 Personuppgiftsbiträdet ska utan dröjsmål informera den personuppgiftsansvarige om eventuella kontakter med tillsynsmyndigheten som rör, eller kan vara av betydelse för, personuppgiftsbiträdets behandling av personuppgifter. Åtagandet är dock begränsat till sådan behandling av personuppgifter som berör, eller kan komma att beröra, den personuppgiftsansvarige. Personuppgiftsbiträdet har inte rätt att företräda den personuppgiftsansvarige eller agera för dennes räkning gentemot tillsynsmyndigheten.

5.7 Den personuppgiftsansvarige har rätt att själv eller genom en oberoende tredje man kontrollera att personuppgiftsbiträdet följer vad som anges i Personuppgiftsbiträdesavtalet och av de instruktioner som utfärdats av den personuppgiftsansvarige. Personuppgiftsbiträdet ska lämna den personuppgiftsansvarige den assistans och tillhandahålla den dokumentation som erfordras för detta.

5.8 Uppgifter i loggar 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 loggar.

5.9 Den registrerade har laglig rätt att begära registerutdrag eller kräva rättelse, blockering eller utplåning av de personuppgifter som omfattas av Personuppgiftsbiträdesavtalet. Personuppgiftsbiträdet är skyldigt att bistå den personuppgiftsansvarige i sådan omfattning att denna rätt kan säkerställas.

5.10 All behandling av personuppgifter sker med iakttagande av sekretess, innebärande att personuppgiftsbiträdet, någon av dennes anställda eller underbiträden inte får lämna ut några uppgifter till tredje man utan att först ha inhämtat den personuppgiftsansvariges samtycke.

5.11 Fullt skadeståndsansvar rörande registrerads personuppgifter ärantingen:

(a) Personuppgiftsbiträdet ansvarar endast för personuppgiftsansvarigs skadeståndskrav från registrerad om skadan orsakats av uppsåt eller grov vårdslöshet.
(b) Personuppgiftsbiträdet ansvarar för personuppgiftsansvarigs skadeståndskrav från registrerad om skadan orsakats av uppsåt, grov vårdslöshet. vårdslöshet eller försumlighet.
(c) Personuppgiftsbiträdet ansvarar för personuppgiftsansvarigs skadeståndskrav från registrerad oavsett orsak till skadansuppkomst.

6 Utläggning av behandlingar till underbiträden

6.1 Om personuppgiftsbiträdet, med den personuppgiftsansvariges godkännande, lägger över sina skyldigheter enligt detta Personuppgiftsbiträdesavtal på ett underbiträde, får detta endast ske genom ingående av ett skriftligt avtal med underbiträdet, varigenom denne åläggs samma skyldigheter som enligt Personuppgiftsbiträdesavtalet åliggerpersonuppgiftsbiträdet.

6.2 För det fall att behandlingar av personuppgifter kommer att utföras av underbiträde i tredje land, kan personuppgiftsansvarige och personuppgiftsbiträdet välja mellan följande:

(a) Personuppgiftsansvarig ger personuppgiftsbiträdet mandat att teckna Personuppgiftsbiträdesavtal för personuppgiftsansvarigs räkning med underbiträden i tredje land, i enlighet med Kommissionens beslut (2010/87/EU) om standardavtalsklausuler för överföring av personuppgifter till tredje land.
(b) Ett Personuppgiftsbiträdesavtal tecknas mellan personuppgiftsansvarig och personuppgiftsbiträdets underbiträde i tredje land, i enlighet med Kommissionens

beslut (2010/87/EU) om standardavtalsklausuler för överföring av personuppgifter till tredje land.

6.3 Om personuppgiftsbiträdet har verksamhet i flera länder och överför personuppgifter till annat bolag i tredje land innebär det att personuppgiftsbiträdet anlitar ett underbiträde i tredje land. I detta fall kan Kommissionens beslut (2010/87/EU) om standardavtalsklausuler för överföring av personuppgifter till tredje land inte användas då detta förutsätter att överföringen av personuppgifter görs till ett underbiträde som är etablerat i tredjeland.

6.4 Om underbiträdet inte uppfyller sina skyldigheter i fråga om behandling enligt ett underbiträdesavtal ska personuppgiftsbiträdet förbli fullt ansvarig gentemot den personuppgiftsansvarige för underbiträdets uppfyllande av sina skyldigheter enligt Personuppgiftsbiträdesavtalet.

6.5 För att den personuppgiftsansvarige ska kunna uppfylla sina lagstadgade skyldigheter som personuppgiftsansvarig, måste alla underbiträden vara kända av och redovisade för den personuppgiftsansvarige. Den personuppgiftsansvarige måste vidare ha kännedom om i vilket land behandlingen äger rum samt underbiträdets åtagande. Den personuppgiftsansvarige har rätt att avsluta Kontrakt enligt Allmänna villkor avsnitt 22 (Rätt att avsluta kontrakt), om denne inte godtar ett visst underbiträde eller en viss typ avbehandling.

7 Skyldigheter efter Personuppgifts-biträdesavtalets upphörande

7.1 Personuppgiftsansvarige och personuppgiftsbiträdet är överens om att personuppgiftsbiträdet och eventuella underbiträden efter behandlingens upphörande och beroende på vad personuppgiftsansvarig beslutar antingen att personuppgifterna raderas helt från det medium där de lagras eller att de avidentifieras på ett sådant sätt att de inte är möjliga att koppla till en enskild individ eller går att återskapa. Radering ska vara utförd senast 180 dagar efter beslut om radering. Innan radering av personuppgifter sker ska, om personuppgiftsansvarig så kräver, personuppgiftsbiträdet återlämna alla överförda personuppgifter till personuppgiftsansvarig. 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.

7.2 Personuppgiftsbiträdet och eventuella underbiträden garanterar att de på personuppgiftsansvarigs eller tillsynsmyndighets begäran kommer att ställa relevanta delar av medium till förfogande för en granskning av de åtgärder som anges i punkt 7.1.

8 Ändringar i personuppgiftsbiträdes-avtalet

8.1 Den personuppgiftsansvarige får ändra innehållet i Personuppgiftsbiträdesavtalet endast i den mån så erfordras för att tillgodose krav som följer av tillämplig uppgiftsskyddslagstiftning eller för att möjliggöra sådana behandlingar som avses i punkt 8.3. Ändring träder i kraft 30 dagar efter att meddelandet om ändring kommit personuppgiftsbiträdet tillhanda. Sådan ändring ska hanteras i enlighet med Allmänna villkor avsnitt 24 (Ändringar av Kontrakt eller Kontraktsföremål).

8.2 Personuppgiftsbiträdet har ingen självständig rätt att påkalla ändringar av detta Personuppgiftsbiträdesavtal.

8.3 För det fall att Leverans innehåll ändras på så sätt att nya funktioner tillkommer, vilka kan föranleda att nya typer av behandlingar av personuppgifter kan komma att utföras, ska den personuppgiftsansvarige underrättas om förändringarna.

9 Giltighetstid

9.1 Detta Personuppgiftsbiträdesavtal gäller från undertecknandet av Kontrakt och så länge som personuppgiftsbiträdet behandlar den personuppgiftsansvariges personuppgifter. Regler om uppsägning av Kontrakt finns i bilaga Allmänna villkor.

10 Behandlingar omfattade av Personuppgiftsbiträdes-avtalet

10.1 Detta avsnitt ska fyllas i av den personuppgiftsansvarige och personuppgiftsbiträdet.

Registrerade
De personuppgifter som ska överföras rör följande kategorier av registrerade:

Typ av personuppgifter som överförs
De personuppgifter som överförs är av följande slag:

Känsliga personuppgifter (i förekommande fall)
Överföringen rör följande känsliga personuppgifter:

Behandling
De personuppgifter som överförs kommer att behandlas på följande sätt:

Ändamålet med behandlingarna
Behandlingen av personuppgifter sker i syfte att:

Särskilda instruktioner angående behandlingarna
Vid behandlingen av personuppgifter ska personuppgiftsbiträdet särskilt beakta:

Behandling av underbiträden i tredje land
Behandling av underbiträden i tredje land regleras enligt alternativ (a) – (b) i punkt 6.2 i detta Personuppgiftsbiträdesavtal. Om inget alternativ anges i vare sig Kontrakt eller Personuppgiftsbiträdesavtal gäller alternativ (a). Ange alternativ:

Skadeståndsansvar
Skadeståndsansvar regleras enligt alternativ (a) – (c) i punkt 5.11 i detta Personuppgiftsbiträdesavtal. Om inget alternativ anges i vare sig Kontrakt eller Personuppgiftsbiträdesavtal gäller alternativ (b). Ange alternativ:

11 Tekniska och organisatoriska säkerhetsåtgärder

11.1 Detta avsnitt 11 (Tekniska och organisatoriska säkerhetsåtgärder) utgör instruktioner till personuppgiftsbiträdet. Villkoren i detta avsnitt kan förändras utifrån vad som framkom i den personuppgiftsansvariges laglighetsprövning och den risk- och sårbarhetsanalys som den personuppgiftsansvarige gjorde i samband med Avrop. I detta avsnitt redogörs för de tekniska och organisatoriska säkerhetsåtgärder som personuppgiftsbiträdet vidtagit i enlighet med punkt 5.1. Den personuppgiftsansvarige har rätt att kontrollera att åtgärderna verkligen vidtas under Kontraktsfullgörande.

11.2 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. I annat fall ska personuppgifterna krypteras.

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

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

11.5 Ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna för personuppgiftsbiträdet. Behörigheten ska begränsas till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord ska vara personliga och får inte överlåtas på någon annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter.

11.6 Åtkomst till personuppgifter ska kunna följas upp i efterhand genom en logg eller liknande underlag. Underlaget ska kunna kontrolleras av personuppgiftsbiträdet och återrapporteras till den personuppgiftsansvarige.

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

11.8 För åtkomst till känsliga och integritetskänsliga personuppgifter krävs tvåfaktorsautentisering.

11.9 Personuppgifter som överförs via datorkommunikation utanför lokaler som kontrolleras av personuppgiftsbiträdet ska skyddas medkryptering.

11.10 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.

11.11 När reparation och service av datorutrustning, vilken används för att lagra personuppgiftsansvariges personuppgifter, utförs av annan än personuppgiftsbiträdet, ska avtal som reglerar säkerhet och sekretess träffas med serviceföretaget.

11.12 Vid servicebesök ska service ske under personuppgiftsbiträdets överinseende. Är detta inte möjligt ska lagringsmedier som innehåller personuppgifter avlägsnas.

11.13 Service via fjärrstyrd datorkommunikation får endast ske via säker anslutning och efter säker elektronisk identifiering av den som utför service. Servicepersonal ska ges åtkomst i systemet endast vid servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.

11.14 Den personuppgiftsansvarige har rätt att utföra kontroller av att avtalade säkerhetsåtgärder faktiskt vidtas.

11.15 Den personuppgiftsansvarige har rätt att utreda obehörig åtkomst hos personuppgiftsbiträdet.

På personuppgiftsansvarigs vägnar:

Namn (fullständigt):

Befattning:

Ort och datum:

….

Namnteckning

På personuppgiftsbiträdets vägnar:

Namn (fullständigt):

Befattning:

Ort och datum:

….

Namnteckning