

Bilaga 2 – Personuppgiftsbiträdesavtal

1 Allmänt

Med Dataskyddslagstiftning avses i detta personuppgiftsbiträdesavtal (PUB-avtal) all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämpliga på den personuppgiftsbehandling (Behandling) som sker enligt detta PUB-avtal, inklusive sådan nationell lagstiftning och EU-lagstiftning.

PUB-avtalets syfte är att säkerställa den vars personuppgifter behandlas (den Registrerades) fri- och rättigheter vid Behandlingen, i enlighet med vad som stadgas i artikel 28.3 i 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 (Dataskyddsförordningen).

I den mån begrepp används i PUB-avtalet som är definierade i Dataskyddsförordningen gäller den innebörd av begreppen som följer av Dataskyddsförordningen.

CSN (Biträdet) ska i enlighet med Överenskommelsen behandla personuppgifter för den Personuppgiftsansvariges räkning. PUB-avtalet består av denna handling, inklusive underbilagan Instruktioner för behandling av personuppgifter (Instruktioner). PUB-avtalet gäller Behandling som Biträdet utför för den Personuppgiftsansvariges räkning. Denna Behandling förtecknas i Instruktionerna.

2 Den personuppgiftsansvariges skyldigheter

Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att det föreligger korrekta Instruktioner så att Biträdet och eventuellt underbiträde kan fullgöra sitt eller sina uppdrag enligt PUB-avtalet.

Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Biträdet om förändringar i Behandlingen vilka påverkar Bitrådets skyldigheter enligt Dataskyddslagstiftningen.

Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

3 Bitrådets skyldigheter

3.1 Allmänt

Biträdet får inte behandla personuppgifter för annat ändamål än det som beskrivs i Instruktionerna i underbilagan. Biträdet förbinder sig att endast utföra Behandling i enlighet med detta PUB-avtal samt att följa Dataskyddslagstiftningen. Biträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

Kravet på att endast behandla personuppgifter i enlighet med detta PUB-avtal, inklusive Instruktionerna, gäller inte om en Behandling krävs enligt unionsrätten eller enligt en EU- eller EES-medlemsstats nationella rätt som Biträdet omfattas av. I sådana fall ska Biträdet informera den Personuppgiftsansvarige

om det rättsliga kravet innan uppgifterna behandlas, såvida detta inte är otillåtet enligt den aktuella rättsordningen.

Biträdet ska vidta åtgärder för att skydda personuppgifterna mot alla slag av Behandlingar som inte är förenliga med detta PUB-avtal och Dataskyddslagstiftningen.

Biträdet ska kunna ge den Personuppgiftsansvarige tillgång till all den information som krävs för att visa att skyldigheterna enligt Dataskyddslagstiftningen är uppfyllda. Biträdet ska också möjliggöra och bidra till eventuella granskningar som den Personuppgiftsansvarige eller oberoende tredje part genomför.

För det fall den Registrerade, tillsynsmyndigheten eller annan tredje part begär information om Behandlingen från Biträdet, ska Biträdet hänvisa till den Personuppgiftsansvarige.

För det fall den Registrerade vill utöva sina rättigheter enligt artiklarna 15–18 och 20–21 i dataskyddsförordningen ska Biträdet hänvisa till den Personuppgiftsansvarige.

Biträdet ska vidta de åtgärder för personuppgifternas säkerhet som krävs enligt artikel 32 (säkerhet i samband med Behandlingen) i Dataskyddsförordningen.

Biträdet ska bistå den Personuppgiftsansvarige med fullgörandet av skyldigheterna enligt artiklarna 32–36 i Dataskyddsförordningen (säkerhetsåtgärder och konsekvensbedömning), med beaktande av den information Biträdet har att tillgå.

Biträdet ska genom lämpliga tekniska och organisatoriska åtgärder i den mån det är möjligt, bistå den Personuppgiftsansvarige så att den Personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den Registrerades rättigheter i enlighet med kapitel III i Dataskyddsförordningen. Biträdet ska underrätta den Personuppgiftsansvarige om eventuella Personuppgiftsincidenter utan onödigt dröjsmål enligt artikel 33.3–4 i Dataskyddsförordningen.

Biträdet ska bistå den Personuppgiftsansvarige i utredningen och rapporteringen av Personuppgiftsincidenten till tillsynsmyndigheten.

Biträdet ska utan onödigt dröjsmål informera den Personuppgiftsansvarige skriftligen om Biträdet anser att en Instruktion strider mot Dataskyddslagstiftningen.

Biträdet ska underrätta den Personuppgiftsansvarige om Biträdet avser att ändra tjänsten, och ändringarna kommer att medföra att Behandlingen kan komma att förändras.

3.2 Särskilda säkerhetsinstruktioner

När datorutrustning och löstagbara datamedier hos Biträdet 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.

Personuppgifter som överförs via datorkommunikation utanför lokaler som Biträdet kontrollerar ska skyddas med kryptering.

För det fall Biträdet använder bärbara datorer vid Behandlingarna ska personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.

Biträdet ska regelbundet överföra personuppgifterna till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas efter en störning. Det ska finnas en rutin för test av återläsning.

Biträdet ska se till att endast personal som för sitt arbete behöver tillgång till lokaler med IT-utrustning där personuppgifterna lagras, får tillträde till lokalerna.

Biträdet ska hålla personuppgifterna åtskilda från andra Användares personuppgifter.

Biträdet ska ha ett tekniskt system för behörighetskontroll som styr åtkomsten till personuppgifterna. Behörigheten ska begränsas till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord eller annan teknikkontroll ska vara personlig och får inte överlåtas på någon annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter.

Biträdet ska kunna följa upp åtkomst till och åtgärder avseende personuppgifter i efterhand genom enlogg eller liknande underlag. Underlaget ska innehålla uppgifter om vem vid CSN och hos aktör som CSN anlitar som har fått tillgång till vad och när. Underlaget ska även innehålla uppgifter om vilken användaridentitet hos den Personuppgiftsansvarige som har fått tillgång till vad och när samt vilka åtgärder som vidtagits av denna användaridentitet och när. Underlaget ska kunna kontrolleras och återrapporteras till den Personuppgiftsansvarige. Det ankommer på den Personuppgiftsansvarige att systematiskt och regelbundet följa upp Behandling som utförs av dess användare.

Biträdet ska skydda anslutning för datakommunikation med sådan teknisk funktion som säkerställer att uppkopplingen är behörig.

4 Sekretess

Biträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt.

Tillgång till personuppgifterna ska begränsas till den personal hos Biträdet som behöver tillgång till dem för att fullgöra Överenskommelsen. Biträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av författning.

Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje part utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande författning att information ska lämnas. Biträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller författningskrav.

Bestämmelser om sekretess i detta PUB-avtal ska fortsätta gälla även om PUB-avtalet i övrigt upphör att gälla.

5 Granskning, tillsyn och revision

Biträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3 h i Dataskyddsförordningen.

Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Biträdet), följa upp att Biträdet uppfyller PUB-avtalets och Dataskyddslagstiftningens krav. Biträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med den dokumentation som behövs för att kunna granska Bitrådets efterlevnad av PUB-avtalet och Dataskyddslagstiftningen. Den

Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt författning eller avtal.

Biträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

6 Rättelse, radering m.m.

För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Bitrådets felaktiga Behandling ska Biträdet vidta lämplig åtgärd utan onödigt dröjsmål från det att Biträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Biträdet endast utföra Behandling av den aktuella personuppgiften som ett led i processen för rättelse eller radering.

Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Biträdet, vilka kan väntas påverka Behandlingen, ska Biträdet skriftligt informera den Personuppgiftsansvarige om detta.

7 Underbiträden

Biträdet får ett allmänt skriftligt förhandstillstånd att anlita underbiträde. Biträdet redovisar anlitade underbiträden i Instruktionerna.

Biträdet ska skriftligen informera den Personuppgiftsansvarige om eventuella planer på att anlita nytt underbiträde eller ersätta underbiträde.

Den Personuppgiftsansvarige har möjlighet att inom 30 dagar göra invändningar mot anlitande av nytt underbiträde.

Biträdet ska genom skriftligt avtal ålägga underbiträdet samma skyldigheter som följer av detta PUB-avtal.

Om underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska Biträdet vara fullt ansvarigt gentemot den Personuppgiftsansvarige för utförandet av underbitrådets skyldigheter.

För att den Personuppgiftsansvarige ska kunna uppfylla sina lagstadgade skyldigheter som personuppgiftsansvarig, ska samtliga underbiträden vara kända av och redovisade för den Personuppgiftsansvarige. Den Personuppgiftsansvarige måste även ha kännedom om underbitrådets säte, i vilket land Behandlingen äger rum samt vilken typ av Behandling som underbiträdet utför.

8 Personuppgiftsincidenter

Biträdet ska ha förmåga att återställa tillgängligheten och tillgången till personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1 c i Dataskyddsförordningen.

Biträdet åtar sig att med beaktande av Behandlingens art, och den information som Biträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Biträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörig Behandling och/eller åtkomst till personuppgifterna.

Vid Personuppgiftsincident, ska Biträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Biträdet ska, med beaktande av typen av Behandling och den

information som Biträdet har att tillgå, tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

9 Överföring av personuppgifter till tredjeland

Biträdet äger inte rätt att överföra personuppgifter till tredjeland eller en internationell organisation utan att den Personuppgiftsansvarige har lämnat sitt skriftliga samtycke i förväg till en sådan överföring.

En överföring till tredjeland förutsätter under alla förhållanden, d.v.s. även för det fall den Personuppgiftsansvarige lämnat sitt skriftliga samtycke, att överföringen sker i enlighet med bestämmelserna angående tredjelandsoverföring i Dataskyddsförordningen.

10 Ansvar för skada i samband med behandling

Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.

Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

Om någon av parterna får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

11 Skyldigheter efter behandlingens upphörande

Vid uppsägning av Överenskommelsen ska den Personuppgiftsansvarige överföra samtliga personuppgifter från lagringsytan till den Personuppgiftsansvariges egen it-miljö eller begära att Biträdet raderar dem. Den Personuppgiftsansvarige ska utan onödigt dröjsmål begära att Biträdet överlämnar annan tillhörande information såsom loggar, instruktioner, beskrivningar och andra handlingar som Biträdet erhållit genom informationsutbyte med den Personuppgiftsansvarige eller begära att Biträdet raderar informationen. Om annat inte meddelas av den Personuppgiftsansvarige ska personuppgifterna och tillhörande information raderas hos Biträdet.

Biträdet ska även radera befintliga kopior av personuppgifter och tillhörande information, förutsatt att hinder mot detta inte följer av unionsrätten eller tillämplig nationell författning.

Om personuppgifter eller tillhörande information överförs ska det ske i ett allmänt använt och standardiserat format, om parterna inte har kommit överens om något annat format.

Till dess att uppgifterna raderas eller överförs ska Biträdet säkerställa efterlevnaden av PUB-avtalet.

Överföring eller radering av personuppgifter ska vara utförd senast 30 dagar räknat från den tidpunkt Överenskommelsen upphör att gälla.

Underbilaga – Instruktioner för behandling av personuppgifter

Ändamålet med behandlingen

Ändamålet med Behandlingen av personuppgifter är att den Personuppgiftsansvarige ska kunna lagra uppgifter om studerande på en lagringsyta och därifrån lämna ut uppgifter för att fullgöra sin uppgiftsskyldighet i förhållande till CSN.

Kategorier av registrerade

De kategorier av personer vars personuppgifter kommer att behandlas av Biträdet för den Personuppgiftsansvariges räkning är studerande.

Vilken typ av personuppgifter behandlas

De personuppgifter som behandlas är följande¹:

- Namn
- Person- eller samordningsnummer
- Utbildning
- Kurskod
- Kursdel
- Nivå på utbildning eller kurs
- Utbildningsgrupp
- Poäng eller annat mått på omfattning på kurs eller utbildning
- Studietid för kurs eller utbildning
- Uppgift om färdighetsträning
- Registrering
- Uppdragsutbildning
- Studieavbrott
- Uppnådda studieresultat

Känsliga personuppgifter

Inga känsliga personuppgifter behandlas

¹ Vilka uppgifter som behandlas för en enskild studerande beror på vilken utbildning han eller hon genomgår.



Behandling

Behandling av personuppgifter sker i Tjänsten endast för teknisk bearbetning och teknisk lagring för den Personuppgiftsansvariges räkning.

Särskilda instruktioner rörande behandlingen

Personuppgifter som Biträdet behandlar för den Personuppgiftsansvariges räkning ska raderas ett år efter att de fördes till lagringsytan.

Personuppgifter i loggar över åtkomst till och åtgärder avseende personuppgifter ska raderas efter ett år.

Personuppgifter som behandlas för backup-ändamål ska raderas senast efter ett år.

Godkända underbiträden

Organisation	Säte	Plats för behandling (land)	Typ av behandling
GDM Konsult AB	Sundsvall	Sverige	IT-drift