#  Personuppgiftsbiträdesavtal inom ramen för DiVA-samarbetet

Detta avtal reglerar förutsättningarna för behandling av personuppgifter i publikationsdatabasen DiVA för PuAs räkning, enligt EU:s dataskyddsförordning som trädde i kraft 25 maj 2018.

## Parter

**Personuppgiftsansvarig: [**DiVA-medlem]**,** (nedan kallad **PuA**), [202100-4920, Box 50500, 205 06 Malmö]

**Personuppgiftsbiträde:** Uppsala universitet, Uppsala universitetsbibliotek, (nedan kallad **Biträdet/PuB)**, organisationsnummer 202100-2932, Box 256, 751 05 Uppsala har denna dag ingått följande personuppgiftsbiträdesavtal (”**Biträdesavtal**”).

## Avtalets bakgrund och syfte

Detta Biträdesavtal ska säkerställa att de Personuppgifter som omfattas av Biträdets Behandling hanteras i enlighet med de krav som följer av Dataskyddsförordningen, annan gällande lagstiftning och etablerad standard samt att Personuppgifterna inte blir tillgängliga för obehöriga.

Parterna har ingått en överenskommelse rörande publikationsdatabasen DiVA**.** Detta Biträdesavtal har ingått för att reglera rätten för DiVAs systemutvecklare, support och förvaltning att behandla PaAs personuppgifter.

Detta Biträdesavtal syftar till att uppfylla Dataskyddsförordningens krav, som föreskriver att det ska finnas ett skriftligt Biträdesavtal om Biträdets behandling av Personuppgifter för den PuA:s räkning.

## Definitioner

Detta Biträdesavtal har motsvarande definitioner som återfinns i artikel 4 i Dataskyddsförordningen, vilket bland annat innebär följande.

Med **Behandling** (eller **Behandla**) avses en åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättning av Personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Med **Dataskyddsförordningen** 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 (allmän dataskyddsförordning) (EUT 119, 4.5.2016, s 1).

Med **Personuppgifter** avses varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med **Personuppgiftsansvarig** avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandling av Personuppgifter; om ändamålen och medlen för behandling bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den Personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Med **Personuppgiftsbiträde** avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.

Med **Personuppgiftsincident** avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.

Med **Personuppgiftslagen** avses Personuppgiftslagen (1998:204).

Med **Pseudonymisering** avses Behandling av Personuppgifter på ett sätt som innebär att Personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att Personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Med **Registrerad** avses den person som Personuppgiften avser.

## Biträdesavtalets avtalshandlingar

Biträdesavtalet består av detta dokument och instruktionerna i bilaga 1 och 2.

## Behandlingen som omfattas av biträdesavtalet

5.1 Preciserade instruktioner till Biträdet avseende dess Behandling av Personuppgifter inom ramen för detta Biträdesavtal framgår av **bilaga 1**.

5.2 Åtgärderna för inbyggt dataskydd och dataskydd som standard ska genomföras av parterna i enlighet med instruktionerna i **bilaga 2**.

5.3 Parterna är överens om att PuA kan ändra eller utfärda ytterligare skriftliga instruktioner som det åligger Biträdet att följa. Parterna ska säkerställa att vid var tid gällande instruktioner framgår av **bilaga 1 och 2**.

## Behandling av Personuppgifter

6.1 Biträdet åtar sig att Behandla Personuppgifter i enlighet med Dataskyddsförordningen, detta Biträdesavtal samt i enlighet med vid var tid gällande skriftliga instruktioner från PuA hänförliga till detta Biträdesavtal.

6.2 PuA bestämmer ensam ändamålet med och medlen för den Behandling av Personuppgifter som Biträdet utför för PuAs räkning.

6.3. Biträdet får inte Behandla Personuppgifter för något annat ändamål eller på något annat sätt än vad som vid varje Behandlingstillfälle är absolut nödvändigt för att uppfylla sina åtaganden enligt detta Biträdesavtal eller annan åtgärd som PuA särskilt skriftligen medger.

## Personuppgiftsbiträdets grundläggande skyldigheter

7.1 Biträdet garanterar att denne besitter nödvändig kapacitet och förmåga att fullgöra sina skyldigheter enligt detta Biträdesavtal och gällande dataskyddslagstiftning, samt att denne löpande vidtar sådana lämpliga tekniska och organisatoriska åtgärder som krävs för att säkerställa att den Registrerades rättigheter skyddas.

7.2 För det fall att Biträdet saknar instruktioner som Biträdet bedömer är nödvändiga för att genomföra uppdraget ska Biträdet utan dröjsmål, informera PuA om sin inställning och invänta instruktioner från PuA.

7.3 Biträdet ska utan dröjsmål informera PuA om eventuella kontakter från Tillsynsmyndigheten som rör eller kan vara av betydelse för Behandling av Personuppgifterna. Biträdet har inte rätt att företräda PuA eller agera för PuA:s räkning gentemot Tillsynsmyndigheten eller annan tredje man.

7.4 För det fall att Registrerad, Tillsynsmyndigheten eller annan tredje man begär information från Biträdet som rör Behandlade Personuppgifter ska Biträdet hänvisa till PuA. PuA och Biträdet ska därefter komma överens om lämpligt tillvägagångsätt för utgivande av efterfrågad information.

7.5 Biträdet ska vid behov bistå den PuA att tillmötesgå en begäran om rättelse, blockering eller utplåning av Personuppgifter som framställts av den Registrerade.

7.6 Biträdet ska omgående och senast inom 48 timmar underrätta PuA vid upptäckt av fullbordade fall av eller försök till obehörig åtkomst, förstörelse eller ändring av Personuppgifter.

7.7 PuA har rätt att själv eller genom tredje man kontrollera att Biträdet följer vad som anges i detta Biträdesavtal och av de instruktioner som utfärdats av PuA. Biträdet ska då kostnadsfritt lämna PuA den hjälp och tillhandahålla den dokumentation som erfordras för detta.

7.8 Uppgifter i tjänstens logg får endast användas av Biträdet för vad som krävs för upprätthållande av tjänstens funktionalitet och kvalitet. PuA har rätt att ta del av de uppgifter som Registreras i loggen.

## Sekretess och tystnadsplikt

8.1 All Behandling av Personuppgifter ska ske med hänsyn till sekretess och tillämpliga bestämmelser i offentlighet- och sekretesslagen (2009:400) ska följas.

8.2 Biträdet ansvarar för att berörd personal och anlitad underleverantör informeras om och iakttar gällande sekretess. Om PuA så önskar ska särskild sekretessförbindelse undertecknas av berörd personal och anlitad underleverantör

8.3 Om annat inte följer av tvingande lag får Biträdet, dennes anställda eller underbiträden inte lämna ut några uppgifter till tredje man utan att först ha inhämtat PuAs samtycke.

1. Underbiträde

9.1 Biträdet får inte anlita ett annat underbiträde utan att ett särskilt skriftligt medgivande i förväg har erhållits av PuA. Detta får dock endast ske genom ingående av ett skriftligt avtal med underbiträdet. Enligt detta underbiträdesavtal ska underbiträdet åläggas samma skyldigheter som enligt detta biträdesavtal åligger Biträdet och framförallt ska underbiträdet ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddsförordningen.

9.2 Om underbiträdet inte uppfyller sina skyldigheter i fråga om Behandling enligt ett underbiträdesavtal är Biträdet fullt ansvarig gentemot PuA.

9.3 För att PuA ska kunna uppfylla sina lagstadgade skyldigheter som PuA, ska samtliga underbiträden vara kända av och redovisade för PuA. PuA måste även ha kännedom om i vilket land Behandlingen äger rum.

1. Säkerhetsåtgärder

10.1 Biträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att Behandlingen utförs i enlighet med Dataskyddsförordningen samt säkerställa att den Registrerades rättigheter skyddas mot bland annat obehörig åtkomst, förstörelse och ändring. Biträdet ska även iaktta Tillsynsmyndigheten instruktioner i dess allmänna råd "Säkerhet för personuppgifter" eller andra föreskrifter som Tillsynsmyndigheten ger ut.

10.2 Parterna ansvarar var för sig och i samråd med beaktande av senaste utvecklingen, genomförandekostnader och Behandlingens art, omfattning, sammanhang och ändamål samt risker, för att vidta lämpliga tekniska och organisatoriska åtgärder utformade för ett inbyggt dataskydd och dataskydd som standard i enlighet med gällande dataskyddslagstiftning, (bilaga 2).

1. Underrättelse i händelse av Personuppgiftsincident

Biträdet ska efter att ha fått vetskap om en personuppgiftsincident lämna underrättelse till PuA inom den tid som anges i punkt 7.6.

En sådan underrättelse ska åtminstone innehålla följande information.

1. En beskrivning av Personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs, samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
2. Förmedla namnet och kontaktuppgifterna för Biträdets dataskyddsombud eller andra kontaktuppgifter där mer information kan erhållas,
3. En beskrivning av de sannolika konsekvenserna av Personuppgiftsincidenten och
4. En beskrivning av de åtgärder som Biträdet har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om PuA eller tillsynsmyndigheten så begär ska Biträdet informera den Registrerade om Personuppgiftsincidenten på så sätt som följer av Dataskyddsförordningen.

1. Konsekvensbedömning och förhandssamråd

12.1 Om en typ av Behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål sannolikt leder till en högre risk för fysiska personers rättigheter och friheter ska Biträdet före det att Behandlingen utförs, på egen bekostnad, vid behov och på begäran av PuA, bistå PuA vid en bedömning av den planerade Behandlingens konsekvenser för skyddet av Personuppgifter. En enda bedömning kan omfatta en serie liknande Behandlingar som medför liknande höga risker.

12.2 För det fall bedömningen av den planerade Behandlingen visar att Behandlingen skulle leda till hög risk om PuA inte vidtar åtgärder för att minska risken ska Biträdet före Behandlingen utförs vara PuA behjälplig vid samråd med tillsynsmyndigheten.

1. Överföring av personuppgifter till tredje land

13.1 Biträdet äger inte rätt att överföra Personuppgifter till tredjeland eller en internationell organisation utan att PuA först har lämnat sitt skriftliga samtycke i förväg till en sådan överföring.

13.2 En överföring till tredjeland förutsätter under alla förhållanden, dvs. även för det fall PuA lämnat sitt skriftliga samtycke, att Biträdet uppfyller de krav och åtgärder som följer av Dataskyddsförordningen vad avser tredjelandsöverföring.

1. Skada och ansvar

14.1 Biträdet är medveten om att varje person som har lidit skada till följd av Biträdets överträdelser av Dataskyddsförordningen, detta Biträdesavtal eller instruktionen ska ha rätt till ersättning från Biträdet för den uppkomna skadan.

14.2 Biträdet ska hålla PuA skadelös för skada eller administrativa sanktionsavgifter som denna drabbats av om Biträdet, eller av denne anlitat underbiträde, vidtagit otillåten eller försumlig Behandling av Personuppgifter i strid med Dataskyddsförordningen, detta Biträdesavtal eller instruktionen.

1. Ändring och tillägg

15.1 Ändringar och tillägg till detta Biträdesavtal ska göras skriftligen och undertecknas av behöriga företrädare för båda parter för att vara giltiga. Ändringen eller tillägget träder i kraft 30 dagar efter att meddelandet om ändring eller tillägg kommit Biträdet tillhanda. PuA äger dock ändra i den vid var tid gällande instruktionen som framgår av **bilaga 1 och 2**.

15.2 Om tjänstens innehåll ändras till exempel genom att nya funktioner tillkommer, och att nya sätt att behandla Personuppgifter på kan uppstå ska PuA omgående skriftligen underrättas om förändringarna.

1. Avslut

16.1 Vid Biträdesavtalets upphörande ska Personuppgifterna antingen återföras till PuA eller raderas. Om annat inte meddelas av PuA ska Personuppgifterna återföras till PuA och därefter raderas hos Biträdet inom 180 dagar eller den längre tid som framgår av instruktionen i bilaga 1. På begäran ska Biträdet lämna ett skriftligt besked om vilka åtgärder som vidtagits med Personuppgifterna i samband med att Behandlingen slutförts.

16.2 För det fall att Biträdet på grund av lag, förordning, myndighetsföreskrifter eller beslut är skyldiga att behålla Personuppgifter även efter det att detta Biträdesavtal har upphört att gälla får dessa Personuppgifter endast användas för det ändamål som framgår av den lag, förordning, myndighets föreskrifter eller beslut som föranleder att Personuppgifterna behålls. PuA ska informeras om detta och grunderna härför.

1. Överlåtelse av avtal

Biträdet äger inte rätt att helt eller delvis överlåta sina åtaganden enligt detta Biträdesavtal, till annan utan skriftligt medgivande från PuA.

1. Avtalstid

Detta Biträdesavtal gäller så länge som Biträdet Behandlar Personuppgifter för PuA:s räkning.

1. Tillämplig lag och tvist

19.1 Parternas rättigheter och skyldigheter enligt detta Biträdesavtal omfattas i sin helhet av svensk rätt.

19.2 Tvist angående tolkning eller tillämpning av detta Biträdesavtal ska avgöras enligt svensk lag och föras vid allmän svensk domstol. För det fall Biträdet är en svensk myndighet ska tvist istället slutligt avgöras av närmast överordnad myndighet eller eljest av den tillämpliga tvistelösningsmekanism inom svenska staten som står till buds.

Detta biträdesavtal har upprättats i två (2) likalydande exemplar av vilka parterna tagit var sitt.

Malmö universitet Uppsala universitetsbibliotek

*Underskrift behörig firmatecknare Underskrift behörig firmatecknare*

*Namnförtydligande, befattning Namnförtydligande, befattning*

*Ort och datum Ort och datum*

Bilaga 1 – PuA:s instruktioner

Parterna har nedan konkretiserat vad som ingår i Behandlingen enligt Biträdesavtalet.

1. **Ändamålet med Behandlingen**

*Personuppgiftsbehandlingen i DiVA består i att säkerställa att rätt person kopplas till rätt publikation och projekt.*

1. **Kategorier av Registrerade**

*Upphovspersoner till publikationer och projekt registreras och lagras i databasen.*

1. **Vilken typ av Personuppgifter Behandlas**

*De uppgifter som lagras är namn, alternativa namn, organisationstillhörighet, Orcid-id, DiVA-id och lokalt-id (organisationsspecifikt), födelseår, dödsår.*

1. **Känsliga/ integritetskänsliga Personuppgifter (i förekommande fall)**

*Inga känsliga eller integritetskänsliga uppgifter hanteras i anslutning till DiVAs hantering av upphovspersoner och deras personuppgifter.*

1. **Behandling**

Personuppgifterna kommer att Behandlas på följande sätt:

 I DiVA används personposten som en auktoritetspost, för att säkerställa upphovspersonen till publikationen och/eller projektet. DiVA-medlemmen (PuA) kan själv skapa personposten med hjälp av ett lokalt-id och/eller orcid-id. När personposten är skapad kan övriga medlemmar göra tillägg med sina lokala id:n och andra generella identifikatorer. Medlemmen äger rätten att själv hantera sina lokala id:n. Biträdet har rätt att på uppdrag från PuA redigera, ta bort och skapa personposter med lokala-id:n.

Personuppgifter som DiVA-medlemmen registrerat kan exporteras i olika format och är tillgänglig för alla.



De ljusgröna fälten markerar de uppgifter som PuA och Biträdet tillsammans kan hantera i DiVA-samarbetet. Det mörkgröna fältet anger den unika information som PuA lägger till personposten. Hur Biträdet ska behandla den informationen specificeras i punkt VI.

De rödmarkerade fälten anger information som antingen systemet genererar (DiVA-id) eller information som läggs till personposten från andra organisationer i samarbetet (lokalt-id).

1. **Särskilda instruktioner rörande Behandlingen:**

DiVA-medlemmen (PuA) ansvarar själv för de lokala id:n som härrör från den egna organisationen. Vid ändringar av PuAs lokala id:n så ska Biträdet agera på direkta förfrågningar från PuA.

1. **Avslutsrutiner**

Se punkt 16 i Biträdesavtalet.

Om PuA önskar radera alla lokala id:n i de personposter där den egna organisationen finns representerad kan PuA uppdra åt Biträdet att göra det.

Bilaga 2 – Inbyggt dataskydd

PuA och Biträdet har vidtagit följande tekniska och organisatoriska åtgärder för inbyggt dataskydd.

* Användaren har möjlighet att ta ut informationen om sig själv från DiVA
* Användaren har själv eller genom DiVAs lokala helpdesk möjlighet att korrigera eventuella felaktigheter
* All hantering av personuppgifter kräver inloggning
* Ingen hantering av personnummer förekommer i DiVA