

Dnr

Datum

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3, Allmänna dataskyddsförordningen EU 2016/679¹

Detta Personuppgiftsbiträdesavtal har dagen för undertecknandet ingåtts mellan:

1. _____ (nedan kallad "Personuppgiftsansvarig"),
organisationsnummer _____
med adress _____
och _____
2. _____ (nedan kallad "Personuppgiftsbiträde"),
organisationsnummer _____
med adress _____

1. BAKGRUND OCH SYFTE

- 1.1 Detta Personuppgiftsbiträdesavtal är en del av ett huvudavtal om tillhandahållandet av tjänster som ingåtts mellan _____ och _____ ska läsas och förstås mot bakgrund av detta.

Personuppgiftsbiträdesavtalet reglerar Personuppgiftsbitrådets behandling av Personuppgifter för Personuppgiftsansvarigs räkning (nedan kallad behandling/en).

- 1.2 Detta Personuppgiftsbiträdesavtal syftar till att säkerställa de registrerades fri- och rättigheter när anlitar ett Personuppgiftsbiträde vid behandling av personuppgifter och till att uppfylla artikel 28.3 Allmänna Dataskyddsförordningen EU 2016/679, i det följande kallad Dataskyddsförordningen.
- 1.3 Detta Personuppgiftsbiträdesavtal reglerar inte Personuppgiftsbitrådets rätt till ersättning för tjänsterna utan denna rätt regleras genom huvudavtalet.

¹ Allmänna Dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbitrådets behandling av personuppgifter för den Personuppgiftsansvariges räkning.

2. DEFINITIONER²

Behandling av personuppgifter	Åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser sådan integritets- och personuppgiftslagstiftning samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter) som är tillämplig på den personuppgiftsbehandling som sker under detta Avtal, inklusive nationell sådan lagstiftning och EU Lagstiftning, såsom denna kan komma att förändras över tid.
Loggning	
Personuppgiftsansvarig	Ett kontinuerligt insamlande av uppgifter om den befattning med personuppgifterna som utförs enligt avtalet och som kan knytas till en enskild fysisk person.
	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgifter	Varje upplysning som avser en identifierad eller identifierbar fysisk person (registrerad), varvid en identifierbar fysisk person är en person

² Jfr. artikel 4 Allmänna dataskyddsförordningen EU 2016/679

Personuppgiftsincident	som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Register	
Registrerad	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.
	En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.
	Den som personuppgiften avser.
Tredje land	En stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet.

3. BEHANDLING AV PERSONUPPGIFTER, ÄNDAMÅL OCH TYP AV PERSONUPPGIFTER

- 3.1 Personuppgiftsbiträdet får endast behandla den Personuppgiftsansvariges personuppgifter i enlighet med detta avtal och tillhörande skriftliga instruktioner för att fullgöra sitt uppdrag åt den Personuppgiftsansvarige.

4. PERSONUPPGIFTSANSVARIGES ANSVAR

- 4.1 Den Personuppgiftsansvarige åtar sig att säkerställa att det finns en laglig grund för aktuella behandlingar enligt punkt 3 och att utforma skriftliga instruktioner för att Personuppgiftsbiträdet och eventuella underbiträden ska kunna fullgöra sitt uppdrag enligt detta personuppgiftsbiträdesavtal (bilaga 1).
- 4.2 Den Personuppgiftsansvarige åtar sig att utan dröjsmål informera Personuppgiftsbiträdet om förändringar i behandlingen vilka

påverkar Personuppgiftsbitrådets skyldigheter enligt Dataskyddslagstiftningen eller annan relevant lagstiftning.

- 4.3 Den Personuppgiftsansvarige ansvarar för att informera registrerade om behandlingarna enligt avtalet och för att, i de fall det krävs, inhämta samtycke från den registrerade samt tillvarata de registrerades rätt till insyn och radering m.m.

5. PERSONUPPGIFTSBITRÅDETS ÅTAGANDEN

- 5.1 Personuppgiftsbitrådet förbinder sig att endast behandla personuppgifterna för de syften i enlighet med Personuppgiftsansvarigs instruktioner som anges i bilaga 1 och att följa Dataskyddslagstiftningen eller annan relevant lagstiftning med avseende på behandling av personuppgifter samt att hålla sig informerad om gällande rätt på området.
- 5.2 Personuppgiftsbitrådet ska vidta åtgärder för att skydda personuppgifterna mot alla slag av otillåtna behandlingar.
- 5.3 Personuppgiftsbitrådet åtar sig att säkerställa att samtliga personer som arbetar under dennes ledning följer vad som framgår av detta Personuppgiftsbitrådesavtal och vid var tid gällande instruktion från Personuppgiftsansvarig, samt att de informeras om relevant lagstiftning.
- 5.4 Personuppgiftsbitrådet ska på begäran från Personuppgiftsansvarig bistå denne vid konsekvensbedömningar och förhandssamråd samt att ta fram information inom ramen för gällande Huvudavtal.
- 5.5 För det fall att Personuppgiftsbitrådet finner att Personuppgiftsansvarigas instruktioner, enligt bilaga 1, är otydliga, olagliga eller saknas, och som Personuppgiftsbitrådet bedömer är nödvändiga för att genomföra sina åtaganden ska denne, utan dröjsmål, informera Personuppgiftsansvarig om detta och invänta nya instruktioner.

6. SÄKERHETSÅTGÄRDER

- 6.1 Personuppgiftsbitrådet åtar sig att vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med Dataskyddslagstiftningen eller annan relevant lagstiftning samt vidta eventuella åtgärder som framgår av instruktionerna³ för att skydda personuppgifterna.

³ Om huvudavtalet innebär att sekretessreglerade uppgifter ska göras tekniskt tillgängliga för en aktör som inte behöver ta del av uppgifterna i fråga, bör avtalet utformas så att det är osannolikt att tjänsteleverantören eller någon annan obehörig faktiskt kommer att ta del av uppgifterna. I en sådan situation bör uppgifterna inte betraktas som röjda i offentlighets- och sekretesslagens mening.

- 6.2 I de fall Personuppgiftsbiträdet behandlar känsliga personuppgifter vilka omfattas av sekretess, kan Personuppgiftsansvarig ställa ytterligare krav på säkerhetsåtgärder.
- 6.3 Personuppgiftsbiträdet ska ha rutiner och verktyg som förhindrar obehörig behandling av, eller obehörig åtkomst till, personuppgifter. Personuppgiftsbiträdet ska kunna spåra behandlingen av personuppgifter genom loggning. Dessa loggar ska omfattas av erforderliga skyddsåtgärder.
- 6.4 Personuppgiftsbiträdet ska genom behörighetskontrollsystem aktivt kunna begränsa åtkomsten till personuppgifterna till sådana personer som arbetar under dennes ledning och som behöver personuppgifterna för att utföra sina arbetsuppgifter för fullgörande av avtalen mellan Personuppgiftsbiträdet och Personuppgiftsansvarig.
- 6.5 Personuppgiftsbiträdet åtar sig att kontinuerligt logga åtkomst till personuppgifter enligt detta avtal i den utsträckning det krävs enligt instruktionen (bilaga 1). Loggar får gallras först fem (5) år efter loggningstillfället om inte annat anges i instruktionerna.

7. SEKRETESS

- 7.1 Personuppgiftsbiträdet och den personal som arbetar under detta personuppgiftsbiträdesavtal ska vid behandling av personuppgifter iaktta såväl handlingssekretess som tystnadsplikt.

Personuppgifter som hanteras inom ramen för detta avtal får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, om inte personuppgiftsansvarig skriftligen medgivit detta.

- 7.2 Personuppgiftsbiträdet ska tillse att samtliga anställda, konsulter och övriga som personuppgiftsbiträdet svarar för och som behandlar personuppgifterna, är bundna av en sekretessförbindelse. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag.

Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med eventuella underbiträden samt sekretessförbindelser mellan underbiträdet och dess personal.

- 7.3 Personuppgiftsbiträdet ska skyndsamt underrätta personuppgiftsansvarig om eventuella kontakter med tillsynsmyndighet avseende behandling av personuppgifterna.

Personuppgiftsbiträdet har inte rätt att företräda personuppgiftsansvarig eller agera för personuppgiftsansvarigs räkning gentemot tillsynsmyndigheter i frågor avseende sådan behandling.

- 7.4 Om den registrerade, tillsynsmyndighet eller tredje man begär information från personuppgiftsbiträdet som rör behandling av personuppgifter, ska personuppgiftsbiträdet informera personuppgiftsansvarig.

Information om behandlingen av personuppgifter får inte lämnas ut till tredje man utan skriftligt medgivande från personuppgiftsansvarig, såvida det inte framgår av tvingande lag att information ska lämnas.

Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

8. GRANSKNING, TILLSYN OCH REVISION

- 8.1 Personuppgiftsbiträdet ska utan dröjsmål, på Personuppgiftsansvariges begäran, tillhandahålla all information, t.ex. tekniska och organisatoriska säkerhetsåtgärder som den Personuppgiftsansvarige behöver för att kunna granska och utöva sin insyn i Personuppgiftsbitrådets behandling av personuppgifter som följer av detta Personuppgiftsbiträdesavtal.
- 8.2 Personuppgiftsbiträdet åtar sig att minst en gång om året revidera säkerheten i personuppgiftsbehandlingen genom en intern revision för att kontrollera att Personuppgiftsbitrådets behandling av personuppgifter följer detta Personuppgiftsbiträdesavtal. Resultatet ska på begäran delges Personuppgiftsansvarig.
- 8.3 Personuppgiftsansvarig äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet) följa upp att Personuppgiftsbiträdet lever upp till den Personuppgiftsansvariges krav på Behandlingen. Personuppgiftsbiträdet ska vid sådan uppföljning bistå Personuppgiftsansvarig eller den som utför granskningen med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna följa upp Personuppgiftsbitrådets efterlevnad av detta Personuppgiftsbiträdesavtal.
- 8.4 Personuppgiftsbiträdet äger dock rätt att erbjuda alternativa tillvägagångssätt för uppföljning, exempelvis granskning genomförd av oberoende tredje part. Personuppgiftsansvarig ska i sådant fall äga rätt, men inte skyldighet att tillämpa detta alternativa tillvägagångssätt för uppföljning. Vid sådan revision eller kontroll ska Personuppgiftsbiträdet ge Personuppgiftsansvarig eller en tredje part den assistans som behövs för genomförandet.
- 8.5 Personuppgiftsbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som det rör eller kan vara av betydelse för Behandling av Personuppgifter, möjlighet att göra tillsyn på plats

- 8.6 Personuppgiftsbiträdet ska även tillförsäkra Personuppgiftsansvarig motsvarande rättigheter i förhållande till anlitade Underbiträden.

9. RÄTTELSE OCH RADERING AV PERSONUPPGIFTER, samt Drift och underhåll

- 9.1 Personuppgiftsbiträdet åtar sig att utan dröjsmål vidta rättelse av felaktiga eller ofullständiga personuppgifter efter instruktioner från personuppgiftsansvarig. Efter det att personuppgiftsansvarig begärt rättelse som innebär borttagande av personuppgift får personuppgiftsbiträdet endast behandla personuppgiften som ett led i rättelseprocessen och åtar sig att vidta åtgärden utan dröjsmål, dock senast inom 30 dagar.
- 9.2 Om Personuppgiftsbiträdet avser att göra förändringar i sina system (uppgraderingar, felsökningar etc.) på sätt som kan förväntas påverka informationshanteringen ska Personuppgiftsbiträdet samråda med den Personuppgiftsansvarige om detta. Sådan information ska lämnas i god tid före förändringen.

10. Personuppgiftsincidenter

- 10.1 Personuppgiftsbiträdet åtar sig att bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en personuppgiftsincident. Personuppgiftsbiträdet ska tillhandahålla stöd för att utreda misstankar om att någon obehörigen behandlat eller haft obehörig åtkomst till personuppgifterna.
- 10.2 Vid personuppgiftsincidenter, samt risker för sådana, ska personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta personuppgiftsansvarig om händelsen. Personuppgiftsbiträdet ska tillhandahålla Personuppgiftsansvarig en skriftlig beskrivning av personuppgiftsincidenten. En sådan ska redogöra för:
1. personuppgiftsincidentens art och, om möjligt, de kategorier och antalet registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
 2. sannolika konsekvenserna av personuppgiftsincidenten, och
 3. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra personuppgiftsincidentens potentiella negativa effekter.

11. UNDERBITRÄDEN

- 11.1 Personuppgiftsbiträdet är skyldig att informera personuppgiftsansvarig då nya underbiträden anlitas. Personuppgiftsbiträdet åtar sig att teckna avtal och säkerställa att alla underbiträden omfattas av samma villkor som gäller personuppgiftsbiträdet. Personuppgiftsbiträdet ansvarar fullt ut för de underbiträden som anlitas gentemot personuppgiftsansvarige.

- 11.2 Om Personuppgiftsbiträdet avser att anlita Underbiträden ska denne tillhandahålla information om vilken typ av uppgifter och kategorier av registrerade ett visst Underbiträde ska befatta sig med samt dess kapacitet och förmåga att leva upp till sina skyldigheter enligt Dataskyddslagstiftningen och annan relevant lagstiftning med avseende på behandling av personuppgifter.
- 11.3 Personuppgiftsbiträdet ska på Personuppgiftsansvariges begäran översända en kopia på personuppgiftsbiträdesavtalet med underbiträdet.
- 11.4 Personuppgiftsbiträdet åtar sig även att informera Personuppgiftsansvarig om eventuella planer på att upphöra att använda sig av ett godkänt underbiträde.

12. ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND OCH LOKALISERING

- 12.1 Personuppgiftsbiträdet ska tillse att personuppgifterna (hanteras och) lagras inom EU/EES, om inte parterna kommer överens om något annat.
- 12.2 Personuppgiftsbiträdet äger endast rätt att överföra personuppgifter till tredje land, för exempelvis service, support, underhåll, utveckling, drift eller liknande hantering, om den personuppgiftsansvarige godkänt sådan överföring och utfärdat särskilda instruktioner (bilaga 1).
- 12.3 Överföring till tredje land får endast ske om Dataskyddslagstiftningen och annan relevant lagstiftning samt detta avtal med tillhörande instruktioner är uppfyllda.

13. ANSVAR FÖR SKADA

- 13.1 Vid ersättning för skada som, genom fastställd dom eller annat beslut, utgått till registrerad på grund av överträdelse av någon bestämmelse i detta avtal, instruktion från Personuppgiftsansvarig eller tillämplig dataskyddsbestämmelse ska artikel 82 Dataskyddförordningen tillämpas.
- 13.2 Sanktionsavgifter enligt artikel 83 i Dataskyddförordningen eller 6 kap. 2 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddförordning ska bäras av den Part som påförts en sådan avgift.
- 13.3 Om Personuppgiftsansvarig får kännedom om omständighet som kan leda till skadestånd eller betalningsansvar för Personuppgiftsbiträde ska Personuppgiftsansvarig omedelbart informera Personuppgiftsbiträdet om förhållande och aktivt arbeta tillsammans med Personuppgiftsbiträdet för att förhindra och minimera sådant skadestånd eller betalningsansvar.

- 13.4 Oaktat vad som anges i Huvudavtalet och dess Bilagor gäller 13.1 och 13.2 före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser behandling av personuppgifter.

14. LAGVAL OCH TVISTLÖSNING

- 12.1 För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol.

15. TILLÄGG, ÄNDRING ELLER UPPSÄGNING AV AVTAL

- 15.1 Tillägg och ändringar av detta Personuppgiftsbiträdesavtal ska, för att vara giltiga, vara skriftliga och undertecknas av båda Parter.
- 15.2 Parterna har rätt att påkalla omförhandling av detta avtal och andra bilagor, för det fall att
1. motpartens ägarförhållanden ändras väsentligt, eller
 2. tillämplig lagstiftning eller tolkningen av den, ändras på ett sätt som påverkar behandlingen av personuppgifter som omfattas av detta avtal, eller
 3. Personuppgiftsansvarig har invändningar mot anlitan av underbiträde (se 15.5 nedan).
- 15.3 En begäran om ändring av endera parten innebär inte att Personuppgiftsbiträdesavtalet bryts utan endast att en omförhandling påbörjas.
- 15.4 Vardera Part har rätt att skriftligen säga upp tjänsten om motparten gör sig skyldig till väsentligt brott mot bestämmelse i detta avtal, och underlåter att vidta rättelse inom trettio (30) dagar från mottagande av skriftlig begäran därom från den andra Parten.
- 15.5 Om den Personuppgiftsansvarige invänder mot ett ev. utbyte av underbiträde har denne rätt att säga upp tjänsten och erhålla återbetalning av erlagda avgifter för kvarvarande period.
- 15.6 Vid uppsägning av avtalet gäller en uppsägningstid om tre (3) månader.

16. AVTALSTID OCH UPPHÖRANDE AV BEHANDLING,

- 16.1 Detta Personuppgiftsbiträdesavtal gäller tillsvidare och upphör först när Personuppgiftsbiträdet slutat behandla Personuppgifter för Personuppgiftsansvarigs räkning. När Personuppgiftsbiträdes-avtal upphör, oavsett orsak, ska samtliga Personuppgifter på begäran av Personuppgiftsansvarig överlämnas till Personuppgiftsansvarig i ett överenskommet standardiserat eller öppet format eller raderas.

- 16.2 Radering av personuppgifter ska ske omgående om inte annat överenskommits, dock senast inom 30 dagar. Vid överlämning av personuppgifter gäller samma tidsfrist efter det att överlämning skett. Detta gäller även annan tillhörande information såsom, instruktioner, systemlösningar, beskrivningar eller andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt detta Personuppgiftsbiträdesavtal
- 16.3 Personuppgiftsbiträdet ska även lämna ut loggarna till den Personuppgiftsansvarige i överenskomet standardiserat eller öppet format om detta avtal upphör att gälla.
- 16.4 Bestämmelser om sekretess i punkten 7 ska fortsätta att gälla även efter detta Personuppgifts-biträdesavtal i övrigt upphört av gälla.

17. ÖVRIGT

- 17.1 Parterna ska utse var sin kontaktperson med ansvar för Parternas samarbete. Ändring av kontaktperson eller kontaktuppgifter ska skriftligen meddelas den andra parten.
- 17.2 Reglering av ersättning med anledning av detta Personuppgiftsbiträdesavtal och de eventuella merkostnader Personuppgiftsbiträdet har för att fullgöra sina skyldigheter enligt detta avtal regleras av huvudavtalet.

Biträdesavtal har upprättats i två (2) exemplar, varav Parterna har tagit var sitt.

Behörig firmatecknare för
Personuppgiftsansvarig

Behörig firmatecknare för
Personuppgiftsbiträdet

Ort och datum

Ort och datum

Underskrift

Underskrift

Namnförtydligande

Namnförtydligande

Bilaga 1 – Instruktion för hantering av Personuppgifter

Utöver vad som redan framgår av detta avtal ska personuppgiftsbiträdet även följa nedanstående instruktioner:

<p>Ändamål</p> <p>Beskriv kortfattat syftet med de personuppgifter som biträdet kommer behandla.</p> <p>Beskriv var informationen kommer lagras.</p>	
<p>Behandlingen omfattar följande typer av personuppgifter</p> <p>Ange vilka personuppgifter biträdet kommer ha åtkomst till.</p>	
<p>Behandlingen omfattar kategorier av registrerade personer</p> <p>Ange vilka kategorier av registrerade vars uppgifter personuppgiftsbiträdet har åtkomst till eller kommer behandla.</p>	
<p>Ange särskilda hanteringskrav vad gäller personuppgiftsbehandlingen som utförs av personuppgiftsbiträdet.</p> <p>Lägg till förtydligande beskrivningar i förekommande fall till exempel avseende gallring</p>	
<p>Ange särskilda tekniska skyddsåtgärder vad gäller personuppgiftsbehandlingen som utförs av personuppgiftsbiträdet.</p> <p>Lägg till förtydligande beskrivningar i förekommande fall.</p>	
<p>Ange särskilda loggningskrav vad gäller personuppgiftsbehandlingen samt vilka som ska tillgång till dem.</p>	

Överföring av personuppgifter till tredje land	
Övriga instruktioner angående personuppgiftshanteringen som utförs av personuppgiftsbiträdet	

Bilaga B2 Lista över underbiträden

Inom parentes anges de länder där respektive bolag är etablerat och från vilka personal kan komma att behandla personuppgifter.

Behandla supportärenden, samtal och andra supportförfrågningar från den personuppgiftsansvarige:

Upprätta fjärråtkomst till den personuppgiftsansvariges system för att undersöka och åtgärda tekniska problem.