Denna avtalsmall lämpar sig för användning inom Sverige och bygger på kraven i EU 2016/679 (”GDPR”). Där andra lagrum är styrande för personuppgiftshanteringen (t.ex. utanför EU/EES) bör denna avtalsmall ej användas.

# Avtal mellan personuppgiftsansvarig och personuppgiftsbiträde

Detta avtal är upprättat mellan nedanstående personuppgiftsansvarig samt nedanstående personuppgiftsbiträde som behandlar personuppgifter (i avtalet nedan sammataget kallat Parterna) för personuppgiftsansvarigs räkning.

|  |  |  |
| --- | --- | --- |
|  | **Personuppgiftsansvarig** | **Personuppgiftsbiträdet** |
| **Namn:** |  |  |
| **Organisationsnummer:** |  |  |
| **Adress:** |  |  |
| **Kontaktperson:** |  |  |
| **E-postadress kontaktperson:** |  |  |
| **Dataskyddsombud:** |  |  |
| **E-postadress dataskyddsombud:** |  |  |

Detta avtal utgör komplement till avtal XXX, i detta avtal kallat Tjänsteavtalet, mellan personuppgiftsansvarig och personuppgiftsibträde i rollerna som kund respektive leverantör.

## Instruktioner

Personuppgiftsbiträdet behandlar personuppgifter för Personuppgiftsansvarig i enlighet med nedanstående tabell/tabeller.

Nedanstående tabell anpassas till ändamålet. Det kan t.ex. betyda att vissa rader uteblir. När det gäller lagringstid/gallringsfrist så gäller detta ibland inte är relevant (om inte biträdet ansvarar för gallring).

Tabell 1 Beskrivning av personuppgiftsbehandling

|  |
| --- |
| **Beskrivning av behandlingen** |
| **Tjänst och ändamål med behandlingen:** |  |
| **Behandlingsaktiviteter:** |  |
| **Kategorier av registrerade:** |  |
| **Kategorier av personuppgifter:** |  |
| **Plats för behandling:** |  |
| **Lagringstid/gallringsfrist:** |  |
| **Säkerhetsåtgärder** |
| **Fysisk åtkomst:** |  |
| **Åtkomst till system:** |  |
| **Åtkomst till personuppgifter:** |  |
| **Överföring av personuppgifter:** |  |
| **Behörighetsstyrning:** |  |
| **Kryptering av lagrat data:** |  |
| **Säker autentisering:** |  |
| **Hantering av lagringsmedia:** |  |
| **Kapacitets- och kontinuitetsplanering:** |  |
| **Separation av data (logisk/fysisk):** |  |
| **Loggning:** |  |
| **Hantering av tekniska sårbarheter:** |  |
| **Redundans:** |  |
| **Dokumenterade driftrutiner:** |  |
| **Oberoende granskning:** |  |

# Innehåll och syfte

Detta avtal har upprättats för att uppfylla kraven på avtal mellan personuppgiftsansvarig och personuppgiftsbiträde i enlighet med artikel 28 i Dataskyddsförordningen (EU 2016/679).

Nedanstående stycke tas med om det är relevant (dvs. att man agerar personuppgiftsbiträde och avtalet riktar sig mot underbiträde)

Personuppgiftsbiträdet är informerad om att Personuppgiftsansvarig i vissa situationer agerar som Personuppgiftsbiträde för kunders räkning. Vid hantering av personuppgifter kan Personuppgiftsbiträdet i förekommande fall därmed komma att agera som underbiträde. I rollen som underbiträde har Personuppgiftsbiträdet identiska skyldigheter vid hantering av personuppgifter enligt detta avtal och villkoren i detta personuppgiftsbiträdesavtal är gällande även för det fall att Personuppgiftsbiträdet agerar som underbiträde.

# Ansvar och instruktion

Den Personuppgiftsansvarige har ansvar för all behandling av personuppgifter som sker med anledning av Tjänsteavtalet.

Personuppgiftsbiträdet åtar sig att enbart behandla avtalade personuppgifter i enlighet med detta avtal, Tjänsteavtalet och den Personuppgiftsansvariges vid var tid meddelade instruktioner. Personuppgiftsbiträdet får inte behandla personuppgifterna som Personuppgiftsansvarig ansvarar för i något eget syfte jämte att tillhandahålla, underhålla och lämna support för leverans i enlighet med Tjänsteavtalet. Den Personuppgiftsansvarige ansvarar för att personuppgifter vilka ej omfattas av detta avtal, Tjänsteavtalet eller andra instruktioner inte behandlas inom ramen för tjänsten.

Personuppgiftsbiträdet åtar sig vidare att behandla personuppgifterna enligt Dataskyddsförordningen, samt tillsynsmyndighetens, eller relevant EU-organs föreskrifter, ställningstaganden och rekommendationer på personuppgiftsområdet, nedan gemensamt benämnda ”Tillämplig lag”.

Personuppgiftsbiträdet får inte överföra några personuppgifter till land utanför EU/EES-området eller till land som inte omfattas av undantagen till förbud mot överföring till tredje land enligt Dataskyddsförordningen, utan att ha den Personuppgiftsansvariges skriftliga samtycke i förväg och ha säkerställt att sådan överföring sker i överensstämmelse med tillämplig lag.

För de fall Personuppgiftsbiträdet misstänker alternativt upptäcker säkerhetsöverträdelse så som obehörig åtkomst, förstörelse, ändring eller liknande av personuppgifter, eller om Personuppgiftsbiträdet av någon annan anledning inte kan uppfylla åtaganden i detta personuppgiftsbiträdesavtal, ska Personuppgiftsbiträdet omedelbart undersöka incidenten och vidta lämpliga åtgärder för att läka incidenten och förhindra upprepning, och tillhandahålla Personuppgiftsansvarig en beskrivning av incidenten. Personuppgiftsbiträdet skall utan onödigt dröjsmål, och senast inom 24 timmar, påbörja incidentrapportering till personuppgiftsansvarig.

Beskrivning av incidenten ska åtminstone:

* Beskriva personuppgiftsincidentens art inbegripet, om så möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgifter som berörs
* Förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas
* Beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
* Beskriva de åtgärder som den personuppgiftsbiträdet har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella effekter.

Personuppgiftsbiträdet ska informera Personuppgiftsansvarige om Personuppgiftsbiträdet får kännedom om att personuppgifter behandlats i strid med Personuppgiftsansvariges instruktioner eller detta personuppgiftsbiträdesavtal.

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 hög risk för fysiska personers rättigheter och friheter ska Personuppgiftsbiträdet före behandlingen utförs vara Personuppgiftsansvarig behjälplig 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.

# Säkerhet och sekretess

Personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som åtminstone överensstämmer med Tillämplig lag och är lämplig med beaktande av:

* Vilka tekniska möjligheter som står till förfogande med beaktande av den senaste teknikutvecklingen
* Kostnaden som genomförandet medför
* Riskerna förknippade med personuppgiftsbehandlingen, med hänsyn tagen till bl.a.
	+ Konsekvenserna av förlust av riktighet, konfidentialitet och tillgänglighet till personuppgifterna vid såväl lagring och informationsöverföring som vid andra behandlingsaktiviteter
	+ Syftet med behandlingen i förhållande till riskerna
	+ Hur känsliga personuppgifterna är för fysiska personers rättigheter och friheter
	+ Mängden personuppgifter som behandlas
	+ Utsattheten hos de kategorier av registrerade som personuppgifterna avser

Avtalade åtgärder, vilka uppfyller denna punkt, ska åstadkomma en säkerhetsnivå som Personuppgiftsansvarig efter samråd med personuppgiftsombudet/dataskyddsombudet bedömer lämplig.

Personuppgiftsbiträdet skall vid utformandet av lämpliga säkerhetsåtgärder beakta allmänt vedertagna principer för informationssäkerhet genom tillämpning av ISO/IEC 27001 eller motsvarande standard.

Personuppgiftsbiträdet ska regelbundet och systematiskt utvärdera verkan av de säkerhetsåtgärder som vidtas för att skydda personuppgiftsbehandlingen som utförs för personuppgiftsansvarigs räkning.

Personuppgiftsbiträdet skall omedelbart meddela Personuppgiftsansvarig i händelse av att säkerheten ej kan upprätthållas avseende personuppgiftsbehandlingen.

Samtliga ändringar av tekniska och organisatoriska åtgärder ska dokumenteras av Personuppgiftsbiträdet.

Åtgärderna som vidtas skall inkludera följande åtgärdsområden i enlighet med Dataskyddsförordningen:

* pseudonymisering och kryptering av personuppgifter
* förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna
* förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
* ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Personuppgiftsbiträdet ska säkerställa att behörighetsstyrningen är korrekt och att konfidentialitet iakttas. Personuppgiftsbiträdet ska vidta de åtgärder som erfordras för att säkerställa att den mottagna informationen endast delges de personer inom den egna organisationen som berörs av ändamålet med Tjänsteavtalet. Personuppgiftsbiträdet ska tillse att samtliga anställda, konsulter, underleverantörer och övriga som Personuppgiftsbiträdet svarar för och som behandlar personuppgifterna är bundna av ett erforderligt sekretessåtagande samt att de är informerade om hur behandling av personuppgifterna får ske. Personuppgiftsbiträdet ansvarar för att de personer som har åtkomst till personuppgifterna är informerade och hur de får behandla personuppgifterna i enlighet med instruktioner från Personuppgiftsansvarig.

# Personuppgiftsansvarigs rätt till granskning av personuppgiftsbiträde

Personuppgiftsansvarige äger rätt att själv eller genom tredje man, genomföra revision gentemot Personuppgiftsbiträdet eller på annat sätt kontrollera att Personuppgiftsbiträdets behandling av personuppgifter följer detta personuppgiftsbiträdesavtal. Vid sådan revision eller kontroll ska Personuppgiftsbiträdet ge Personuppgiftsansvarige den assistans som behövs för genomförande av revision.

Personuppgiftsbiträdet ska på begäran av Personuppgiftsansvarige tillhandahålla all tillgänglig information avseende behandlingen av personuppgifter för att Personuppgiftsansvarige ska kunna uppfylla sina skyldigheter som personuppgiftsansvarig enligt Tillämplig lag.

För de fall registrerade personer, tillsynsmyndigheten eller annan tredje man begär information från Personuppgiftsansvarige eller Personuppgiftsbiträdet rörande behandlingen av personuppgifter ska Parterna samverka och utbyta information i nödvändig utsträckning. Personuppgiftsbiträdet får inte lämna ut personuppgifter eller information om behandlingen av personuppgifter utan medgivande i förväg från Personuppgiftsansvarig utom för det fall föreläggande finns därom från relevant myndighet eller om Personuppgiftsbiträdet är nödgad därtill enligt tvingande lagstiftning.

Personuppgiftsbiträdet ska vara Personuppgiftsansvarig behjälplig genom lämpliga tekniska och organisatoriska åtgärder, så att Personuppgiftsansvarig kan fullgöra sin skyldighet avseende de registrerades rättigheter i enlighet med kapitel III i Dataskyddsförordningen.

# Anlitande av underbiträde

Personuppgiftsbiträde har rätt att anlita underbiträden för att leverera tjänst i enlighet med Tjänsteavtalet.

Om Personuppgiftsbiträdet anlitar underbiträde enligt villkoren i Tjänsteavtalet, har Personuppgiftsbiträdet mandat och skyldighet att ingå särskilt personuppgiftsbiträdesavtal med sådant underbiträde vad avser underbiträdets behandling av personuppgifter. I sådant avtal ska föreskrivas att underbiträdet har motsvarande skyldigheter som Personuppgiftsbiträdet har enligt detta personuppgiftsbiträdesavtal.

Personuppgiftsbiträdet ska på Personuppgiftsansvariges begäran tillhandahålla kopia av de delar av Personuppgiftsbiträdets avtal med underbiträde som krävs för att utvisa att Personuppgiftsbiträdet uppfyllt sina åtaganden enligt detta personuppgiftsbiträdesavtal.

Personuppgiftsbiträdet ska vid var tid föra en korrekt och uppdaterad lista utvisande vilka underbiträden som anlitats för behandlingen av personuppgifter och var dessa är geografiskt belägna. Personuppgiftsbiträdet ska vidare på Personuppgiftsansvariges begäran utan dröjsmål tillhandahålla kontaktuppgifter till de underbiträden som behandlar personuppgifter.

Personuppgiftsbiträdet ska informera den Personuppgiftsansvarige om eventuella planer på att anlita nya underbiträden eller ersätta underbiträden, så att den Personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar. För de fall det finns rimligt fog för invändningen har Personuppgiftsansvarige rätt att med bindande verkan motsätta sig anlitandet av visst nytt underbiträde.

# Tvist, tillämplig lag och skadestånd

Tvist angående tolkning eller tillämpning av detta avtal ska avgöras enligt svensk lag och Tjänsteavtalets bestämmelse om tvist.

I händelse av att Personuppgiftsansvarig blir ersättningsskyldig gentemot tredje man till följd av Personuppgiftsbiträdets bristande efterlevnad av detta avtal eller Tjänsteavtalet skall Personuppgiftsansvarig hållas skadelös genom att Personuppgiftsbiträde till fullo ersätter Personuppgiftsansvarig för den skada som uppstått.

# Avtalets ikraftträdande, upphörande, ändringar och överlåtelse

Detta personuppgiftsbiträdesavtal träder i kraft när det undertecknats av båda Parter och gäller därefter mellan Parterna så länge Personuppgiftsbiträdet behandlar Personuppgifter för den Personuppgiftsansvarige i enlighet med Tjänsteavtalet. Detta personuppgiftsbiträdesavtal upphör automatiskt att gälla utan föregående uppsägning när Tjänsteavtalet upphör att gälla.

Ändringar och tillägg till detta avtal ska, för att vara giltiga, göras skriftligen och undertecknas av båda Parter. Sådana ändringar och tillägg till avtalet träder i kraft efter båda Parters undertecknande om inget annat är överenskommet. Denna punkt förhindrar inte att Personuppgiftsansvarig kan ändra eller utfärda ytterligare instruktioner i enlighet med vad som framgår av detta avtal.

Personuppgiftsbiträdet ska, beroende på vad Personuppgiftsansvarig väljer, omgående radera eller återlämna all data som innehåller personuppgifter på samtliga media som den är fixerad på efter att uppdraget enligt detta personuppgiftsbiträdes avslutats samt radera befintliga kopior.

Överlåtelse av detta personuppgiftsbiträdesavtal får ske i enlighet med bestämmelserna för överlåtelse i Tjänsteavtalet och endast i samband med överlåtelse av Tjänsteavtalet.

Ta bort nedanstående om detta avtal är del i t.ex. allmänna villkor.

Detta avtal har upprättats i var sitt exemplar för Personuppgiftsansvarig respektive Personuppgiftsbiträde.

**För Personuppgiftsansvarig:** **För Personuppgiftsbiträde:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Namn, Ort & Datum Namn, Ort & Datum