

PERSONUPPGIFTSBITRÄDESAVTAL

Detta personuppgiftsbiträdesavtal ("**Avtalet**") är träffat (YYYY-MM-DD)mellan:

- (1) (Företagsnamn)organisationsnummer ("**Personuppgiftsansvarig**") och
- (2) (Företagsnamn), organisationsnummer ("**Personuppgiftsbiträde**")

Parterna 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 avtalets bilaga 1.

1. Syfte

- 1.1. Personuppgiftsbiträdets fullgörande av avtalet medför att personuppgiftsbiträdet behandlar personuppgifter åt personuppgiftsansvarigs vägar i enlighet med vad som stadgas i dataskyddsförordningen (EU 2016/679).
- 1.2. Detta avtal syftar till att uppfylla dataskyddsförordningens artikel 28 som föreskriver att det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för personuppgiftsansvarigs räkning samt vilken integritetsnivå som ska uppnås vid behandlingen.
- 1.3. Personuppgiftsbiträdet intygar att dennes verksamhet bedrivs på sätt som säkerställer att personuppgiftslagens bestämmelser och krav avseende adekvat skydd för personuppgiftsbehandlingar efterlevs.
- 1.4. Definitionerna motsvarar definitionerna i dataskyddsförordningen (EU 2016/679).

2. Personuppgiftsansvarig

- 2.1. Personuppgiftsansvarig är skyldig att under detta avtal säkerställa att behandlingen av personuppgifter är laglig i enlighet med gällande dataskyddslagstiftning. Personuppgiftsansvarig ska se över och uppdatera åtgärder vid behov.
- 2.2. Personuppgiftsansvarig får endast tillhandahålla personuppgiftsbiträdet personuppgifter som är nödvändiga för det i bilaga 1 angivna ändamålet med behandlingen.
- 2.3. Personuppgiftsansvarig ska tillhandahålla dokumenterade instruktioner och övriga uppgifter avseende föremål för personuppgiftsbehandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade.

3. Behandling av personuppgifter

- 3.1. Personuppgiftsbiträdet ska endast behandla personuppgifter som tillhandahållits av personuppgiftsansvarig i enlighet med detta avtal, dataskyddsförordningen, tillsynsmyndighetens föreskrifter och personuppgiftsansvarigs instruktioner.
- 3.2. Personuppgiftsbiträdet får inte behandla personuppgifter för egna eller andra ändamål än de ändamål som personuppgiftsbiträdet anlitas för av personuppgiftsansvarig.
- 3.3. Den registrerades rättigheter enligt dataskyddsförordningen ska tillgodoses. Personuppgiftsbiträdet är skyldigt att bistå den personuppgiftsansvarige i sådan omfattning att dessa rättigheter kan utövas och säkerställas.
- 3.4. Personuppgiftsansvarig ska få tillgång till all information för att

- i) kunna visa att de skyldigheter som åläggs personuppgiftsansvarig enligt dataskyddsförordningen uppfylls,
 - ii) kunna verifiera att personuppgiftsbiträdet vidtar lämpliga tekniska och organisatoriska säkerhetsåtgärder samt uppfyller övriga krav.
- 3.5. Personuppgiftsbiträde ska även när det är nödvändigt och vid förfrågan möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.
- 3.6. Med beaktande av typen av behandling och den information personuppgiftsbiträdet har tillgång till ska personuppgiftsbiträdet bistå personuppgiftsansvarig vid konsekvensbedömning avseende dataskydd samt vid förhandssamråd.
- 3.7. Personuppgiftsbiträdet ska utan onödigt dröjsmål underrätta personuppgiftsansvarig vid en personuppgiftsincident.
- 3.8. Personuppgiftsbiträdet ska skriftligen och i förväg informera personuppgiftsansvarige om planerade ändringar av behandlingsförfarandet, däribland tekniska och organisatoriska ändringar som kan påverka skyddet av personuppgifterna och personuppgiftsbiträdes efterlevnad av den gällande dataskyddslagstiftningen.
- 3.9. Innan genomförandet av sådana ändringar som avses ovan i 4.7 ska samtycke inhämtas av personuppgiftsansvarig.

4. Personuppgiftsbiträde

- 4.1. Personuppgiftsbiträdet ska säkerställa att kraven i dataskyddsförordningen är uppfyllda samt att den registrerades rättigheter skyddas.
- 4.2. Personuppgiftsbiträdet garanterar att denne besitter nödvändig teknisk och organisatorisk förmåga, inbegripet tekniska lösningar, kompetens, personal- och ekonomiresurser, rutiner och metoder, för att fullgöra sina skyldigheter enligt detta personuppgiftsbiträdesavtal och gällande dataskyddslagstiftning för att skydda de personuppgifter som behandlas.
- 4.3. I syfte att upprätthålla en lämplig säkerhetsnivå och för att skydda behandlingen av personuppgifterna mot obehörig åtkomst, förstörelse eller ändring ska personuppgiftsbiträdet vidta de tekniska och organisatoriska säkerhetsåtgärder som anges i bilaga 1.
- 4.4. Personuppgiftsbiträdet ska säkerställa att berörd personal följer personuppgiftsbiträdesavtalet, personuppgiftsansvarigs instruktioner samt att de hålls informerade om gällande dataskyddslagstiftning.
- 4.5. Personuppgiftsbiträdet får inte behandla personuppgifter på något annat sätt, för andra ändamål eller enligt andra instruktioner än vad som anges i bilaga 1. För det fall att personuppgiftsbiträdet bedömer att det saknas instruktioner som är nödvändiga för att genomföra avtalet ska personuppgiftsbiträdet utan dröjsmål informera personuppgiftsansvarig samt invänta vidare instruktioner från den personuppgiftsansvarige.
- 4.6. Om personuppgiftsbiträdet fastställer ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen.

5. Underbiträden

- 5.1. Personuppgiftsbiträdet har inte rätt att anlita underleverantör för behandling av personuppgifter enligt detta avtal, utan skriftligt godkännande från personuppgiftsansvarig.
- 5.2. Underbiträde får endast anlitas genom ingående av skriftligt avtal med underbiträdet, genom vilken denne åläggs samma skyldigheter som enligt detta avtal åligger personuppgiftsbiträdet.
- 5.3. Om underbiträdet inte uppfyller sina skyldigheter vad gäller behandling enligt ovan nämnda underbiträdesavtal ska personuppgiftsbiträdet förbli fullt ansvarig gentemot den personuppgiftsansvarige för utövandet av underbiträdets skyldigheter.

6. Överföring av personuppgifter till tredje land

- 6.1. Personuppgiftsbiträdet har inte rätt att överföra personuppgifter till tredje land, såvida inte personuppgiftsansvarig skriftligen godkänt sådan överföring och förutsättningarna i gällande dataskyddslagstiftning är uppfyllda.

7. Tekniska och organisatoriska åtgärder

- 7.1. Personuppgifterna ska av personuppgiftsbiträdet skyddas mot förstöring, ändringar, otillåten spridning, obehörig tillgång samt alla slag av otillåten behandling.
- 7.2. Personuppgiftsbiträdet ska genom lämpliga tekniska och organisatoriska åtgärder begränsa åtkomsten till personuppgifterna till personer som arbetar under dennes ledning och som behöver personuppgifterna för att utföra sina arbetsuppgifter för fullgörande av avtal ingångna mellan personuppgiftsansvarig och personuppgiftsbiträdet. Personuppgiftsbiträdet ska även tillse att sådan personal har erforderlig utbildning och i tillräcklig mån har instruerats att hantera personuppgifterna på ett ändamålsenligt och säkert sätt.
- 7.3. Personuppgiftsbiträdet ska se till att de personer som har åtkomst till personuppgifterna omfattas av sekretess enligt vad som framgår av avsnitt 8.
- 7.4. Behandlingssystemen och tjänsterna ska fortlöpande säkerställa sekretess, integritet, tillgänglighet och motståndskraft (*Används om det bedöms lämpligt*).
- 7.5. När datorutrustning och löstagbara datamedier hos personuppgiftsbiträdet inte står under uppsikt ska utrustningen och medierna låsas in/skyddas för att förhindra obehörig användning, påverkan och stöld. I annat fall ska personuppgifterna krypteras.
- 7.6. Personuppgiftsbiträdet ska tillhandahålla och vidta tekniska och praktiska lösningar för att utreda misstankar om att någon obehörigen behandlat eller haft obehörig åtkomst till personuppgifterna.
- 7.7. I det fall personuppgiftsbiträdet behandlar särskilda personuppgifter eller på annat sätt behandlar integritetskänsliga personuppgifter vilka exempelvis omfattas av sekretess, ställs särskilt höga säkerhetskrav innefattande exempelvis [tvåstegsautentisering och kryptering].
- 7.8. Personuppgifterna ska regelbundet överföras till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att personuppgifterna kan återställas för att säkerställa tillgänglighet och tillgång till personuppgifterna i rimlig tid vid en fysisk eller teknisk incident (*Används om det bedöms lämpligt*).

- 7.9. Personuppgiftsbiträdet ska fastställa ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska säkerhetsåtgärderna *(Används om det bedöms lämpligt)*.

8. SEKRETESS & SÄKERHET

- 8.1. Personuppgiftsbiträdet och de personer som arbetar under dennes ledning ska vid behandling av personuppgifter iaktta sekretess *(med beaktande av offentlighetsprincipen i enlighet lagen om offentlighet och sekretess (2009:400) samt övrig relevant lagstiftning)*. Det innebär att personuppgifter inte obehörigen får röjas för tredje man. Personuppgiftsbiträdet åtar sig att se till att de personer som arbetar under personuppgiftsbitrådets ledning och kommer att behandla personuppgifter enligt detta avtal iakttar och följer personuppgiftsbitrådets sekretessplikt.
- 8.2. Handlingar som personuppgiftsbiträdet erhåller enligt avtal mellan parterna, såsom personuppgifter, instruktioner, systemlösningar, beskrivningar eller andra handlingar som erhålls genom informationsutbyte får inte utnyttjas eller röjas för annat ändamål än vad som framgår av detta avtal, vare sig direkt eller indirekt, om inte ansvarig på förhand medgivit detta skriftligen.
- 8.3. Sekretessplikten omfattar inte information som part kan visa har varit allmänt känd eller som kommit till parts kännedom från tredje man utan att ha föregåtts av brott mot detta avtal.
- 8.4. Sekretessplikten gäller även om detta avtal i övrigt upphör

9. ANSVAR

- 9.1. I de fall en registrerad person riktar anspråk mot personuppgiftsansvarig för skada eller om en behörig myndighet utfärdar vite eller andra administrativa påföljder med anledning av personuppgiftsbehandling i strid med personuppgiftsansvariges instruktioner, detta biträdesavtal eller gällande dataskyddslagstiftning ansvarar personuppgiftsbiträde för att hålla personuppgiftsansvarige skadeslös.
- 9.2. *(Personuppgiftsansvarige ska ersätta personuppgiftsbiträdet för sådana anspråk på ersättning från en registrerad person, vite eller annan administrativ påföljd utfärdad av en behörig myndighet till följd av personuppgiftsansvariges bristfälliga instruktioner eller andra uttryckliga skyldigheter enligt detta avtal. (Används när det är lämpligt))*

10. AVTALSTID & UPPSÄGNING

- 10.1. Detta avtal gäller från dess undertecknande tills vidare. Vardera part har rätt att skriftligen säga upp avtalet. Vid uppsägning av avtalet gäller en uppsägningstid om *(fylls i vid tecknade)*
- 10.2. Part är berättigad att säga upp detta avtal till omedelbart upphörande om motparten:
- i) gör sig skyldig till väsentligt brott mot bestämmelse i detta avtal eller,
 - ii) försätts i konkurs, inleder ackordsförhandling eller annars är på obestånd.
- 10.3. Personuppgiftsbiträdet ska vid avslutad behandling *(återlämna, (när det är bedöms lämpligt))* personuppgifterna i ett allmänt och läsbart format till Personuppgiftsansvarige och därefter *(radera, (när det är bedöms lämpligt))*

personuppgifterna från sådana system som använts vid behandlingen, såvida inte detta är oförenligt med annan tvingande lag.

11. Lagval

11.1. Vid behandlingen av personuppgifter och vid tolkningen av detta avtal tillämpas svensk rätt.

Detta Avtal har upprättats i två (2) original, av vilka parterna har erhållit ett (1) original var. *(Avtalet finns även i elektroniskt format, om sådant upprättats.)*

.....
ORT

.....
ORT

.....
DATUM

.....
DATUM

.....
MYNDIGHET

.....
FÖRETAG

.....
UNDERSKRIFT

.....
UNDERSKRIFT

.....
NAMNFÖRTYDLIGANDE

.....
NAMNFÖRTYDLIGANDE

BILAGA 1 (Kompletteras vid avtalstecknande)
INSTRUKTIONER

Syftet med behandlingen

- Syftet/Föremålet med behandlingen är ...

Behandlingens art och ändamål

Ändamålet med behandlingen är att ...

Typ av behandling

Typ av personuppgifter

Känsliga personuppgifter (i förekommande fall):

Kategorier av registrerade

Varaktighet

Fr o m: [åå/mm/dd]

T o m: [åå/mm/dd]

Om period inte kan anges, specificera hur perioden ska avgöras:

...

Underbiträde

I förekommande fall, ange namn och kontaktuppgifter på Underbiträde:

...

Överföring till tredje land

I förekommande fall, ange om personuppgifterna överförs, direkt eller indirekt, till land/stat utanför EU/EES.

...

BEHANDLINGSSPECIFIKATION

Personuppgiftsansvarig och personuppgiftbiträde har vidtagit följande tekniska och organisatoriska åtgärder för inbyggt dataskydd:

...