

## PERSONUPPGIFTSBITRÄDESAVTAL

### PARTER

Detta personuppgiftsbiträdesavtal ("Biträdesavtal") har ingåtts mellan:

[PERSONUPPGIFTSANSVARIG: \_\_\_\_\_],

organisationsnummer : \_\_\_\_\_, med adress :

\_\_\_\_\_ ("Personuppgiftsansvarig"), och

Datea AB, organisationsnummer 556646-3302, med adress Centrumplan 8, 33331

Smålandsstenar ("Personuppgiftsbiträde"),

var för sig benämnd "Part" och tillsammans "Parterna".

### 1. Definitioner

Om inget annat anges ska begrepp anses ha samma innebörd som i Gällande dataskyddsregler, vilka bland annat innebär:

Behandling, avser den åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, 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.

Gällande dataskyddsregler, avser t o m 24 maj 2018 rådsdirektiv 95/46/EG, införd i svensk rätt genom personuppgiftslagen (1998:204) och personuppgiftsförordningen (1998:1191). Fr o m 25 maj 2018 avses den allmänna dataskyddsförordningen (GDPR), (EU) 2016/679.

Känsliga personuppgifter, definieras i 13 § PUL samt fr o m 25 maj 2018 i artikel 9 GDPR.

Personuppgifter, varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad Registrerad), 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 lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsincident, avser 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 och i övrigt behandlas.

Registrerad, se Personuppgifter ovan.

Tredje land, avser ett land utanför Europeiska Ekonomiska Samarbetet ("EES").

Underbiträde, avser sådant personuppgiftsbiträde som anlitas av det Personuppgiftsbiträde som är Part i detta Biträdesavtal och som Behandlar Personuppgifter för Personuppgiftsansvarigs räkning.

## **2. Behandling av personuppgifter**

- 2.1. Biträdet ska endast behandla Personuppgifter i enlighet med detta Biträdesavtal, Gällande dataskyddsregler samt Personuppgiftsansvarigs vid var tid gällande instruktioner, se Bilaga 1.
- 2.2. Personuppgiftsbiträdet får inte behandla Personuppgifter för egna eller några andra ändamål än de som Personuppgiftsbiträdet anlitas för av Personuppgiftsansvarig.
- 2.3. Personuppgiftsbiträdet får inte överföra Personuppgifter till Tredje land såvida det inte är tillåtet enligt vad som framgår av Bilaga 1.
- 2.4. Personuppgiftsbiträdet ska utan oskäligt dröjsmål, dock senast trettio (30) dagar från Personuppgiftsansvarigs begäran, ge denne tillgång till Personuppgifter som Personuppgiftsbiträdet har i sin besittning samt genomföra en begärd ändring, radering, begränsning eller överföring av Personuppgifter. Har Personuppgiftsansvarig raderat, eller anvisat Personuppgiftsbiträdet om radering, ska den senare vidta sådana åtgärder som krävs för att Personuppgiften inte ska kunna återskapas.
- 2.5. Personuppgiftsbiträdet är skyldigt att upprätta ett register över den Behandling som sker på Personuppgiftsansvarigs uppdrag. Vid begäran ska ett registerutdrag överlämnas till Personuppgiftsansvarig eller behörig tillsynsmyndighet i ett läsbart format. Registret ska omfatta följande:
  - a) Namn och kontaktuppgifter för Personuppgiftsbiträdet och dess dataskyddsombud, om sådant finns, samt för Personuppgiftsansvarig för vars räkning Behandling utförs. I förekommande fall även kontaktuppgifter för Underbiträden;

- b) de kategorier av Behandling som utförs för Personuppgiftsansvarigs räkning;
- c) i tillämpliga fall, överföringar av Personuppgifter till Tredje land, information om vilket Tredje land som avses samt vilka lämpliga skyddsåtgärder som vidtagits; och
- d) en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som vidtagits för att uppnå en lämplig skyddsnivå.

### **3. Personuppgiftsansvarigs ansvar**

- 3.1. Personuppgiftsansvarig ska ansvara för att Behandlingen av Personuppgifter är laglig och sker i enlighet med Gällande dataskyddsregler.
- 3.2. Personuppgiftsansvarig ska omedelbart lämna Personuppgiftsbiträdet korrekta uppgifter i händelse av att instruktionerna är felaktiga, ofullständiga eller i övrigt behöver förändras.
- 3.3. Personuppgiftsansvarig ska endast ge Personuppgiftsbiträdet tillträde till de Personuppgifter som är nödvändiga med hänsyn till ändamålet med Behandlingen.

### **4. Kapacitet och förmåga**

- 4.1. Personuppgiftsbiträdet garanterar att denne besitter nödvändig teknisk och organisatorisk kapacitet och förmåga att fullgöra sina skyldigheter enligt detta Biträdesavtal och Gällande dataskyddsregler.
- 4.2. Personuppgiftsbiträdet ska på Personuppgiftsansvarigs begäran, eller oberoende tredje part som denna anlitat, visa att de skyldigheter som framgår av detta Biträdesavtal och Gällande dataskyddsregler uppfylls genom att utan onödigt dröjsmål tillhandahålla relevant dokumentation, hänvisa till relevant och godkänd uppförandekod eller certifiering, möjliggöra och bidra till granskningar och inspektioner av lokaler, IT-system och andra tillgångar och/eller tillhandahålla annan adekvat bevisning. Personuppgiftsbiträdet ska tillförsäkra Personuppgiftsansvarig motsvarande rättigheter i förhållande till anlitate Underbiträden.

### **5. Säkerhetsåtgärder**

- 5.1. Personuppgiftsbiträdet ska genom lämpliga tekniska och organisatoriska åtgärder begränsa tillgången till Personuppgifterna och endast ge behörighet till sådan

personal som behöver ha tillgång till Personuppgifterna för att fullgöra sina åtaganden enligt detta Biträdesavtal, samt att tillse att sådan personal har erforderlig utbildning och i tillräcklig mån har instruerats att hantera Personuppgifterna på ett ändamålsenligt och säkert sätt.

- 5.2. Personuppgifterna ska av Personuppgiftsbiträdet skyddas mot all typ av otillåten Behandling så som förstöring, otillåten spridning och obehörig tillgång.
- 5.3. Personuppgiftsbiträdet ska Behandla Personuppgifter med sekretess och tillse att personer med behörighet att Behandla Personuppgifterna hos Personuppgiftsbiträdet har ingått särskild sekretessförbindelse eller upplysts om att särskild tystnadsplikt föreligger enligt avtal eller gällande rätt.
- 5.4. I det fall Personuppgiftsbiträdet Behandlar Känsliga personuppgifter eller på annat sätt behandlar integritetskänsliga Personuppgifter vilka exempelvis omfattas av sekretess, ställs särskilt höga krav säkerhetskrav innefattande exempelvis tvåstegsautentisering och kryptering.
- 5.5. Personuppgiftsbiträdet ska utan oskäligt dröjsmål, dock senast inom tjugofyra (24) timmar från att det kommit Personuppgiftsbiträdet till kännedom, underrätta Personuppgiftsansvarig om förekomsten av eller risken för en Personuppgiftsincident. En sådan underrättelse ska innehålla all nödvändig och tillgänglig information som Personuppgiftsansvarig behöver för att kunna vidta lämpliga förebyggande åtgärder och motåtgärder samt uppfylla sina skyldigheter avseende anmälan av Personuppgiftsincidenter till behörig tillsynsmyndighet.

## **6. Samverkan**

- 6.1. Personuppgiftsbiträdet ska, med hänsyn taget till Behandlingens art, hjälpa Personuppgiftsansvarig genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att Personuppgiftsansvarig kan fullgöra sin skyldighet att svara på begäran om utövande av den Registrerades rättigheter.
- 6.2. Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig med att se till att skyldigheterna avseende Personuppgiftsincidenter och konsekvensbedömningar enligt Gällande dataskyddsregler fullgörs, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

- 6.3. Personuppgiftsbiträdet ska utan oskäligt dröjsmål underrätta Personuppgiftsansvarig om denne kontaktas av behörig tillsynsmyndighet eller annan tredje part i syfte att få tillgång till Personuppgifter som Personuppgiftsbiträdet, eller i förekommande fall Underbiträdet, har i sin besittning.
- 6.4. Personuppgiftsbiträdet ska skriftligen och i förväg informera Personuppgiftsansvarig om planerade ändringar av behandlingsförfarandet, däribland tekniska och organisatoriska ändringar som kan påverka skyddet av Personuppgifterna och Personuppgiftsbitrådets efterlevnad av Gällande dataskyddsregler. Innan sådana ändringar genomförs ska Personuppgiftsansvarig lämna sitt samtycke, vilket inte skäligen ska förvägras.

## **7. Underbiträde**

- 7.1. Personuppgiftsbiträdet får inte utan Personuppgiftsansvarigs skriftliga samtycke anlita ett Underbiträde för Behandling av de Personuppgifter som Personuppgiftsbiträdet Behandlar för Personuppgiftsansvarigs räkning. En sådan överlåtelse av behandlingen till ett Underbiträde sker på Personuppgiftsbitrådets egen risk och medför inga ändringar i den ansvarsfördelning som gäller mellan Parterna i detta Biträdesavtal.
- 7.2. Det är Personuppgiftsbitrådets ansvar att med lämpliga åtgärder säkerställa att ett anlitat Underbiträde uppfyller alla tillämpliga bestämmelser om skydd för Personuppgifter samt i väsentliga delar uppfyller de skyldigheter som regleras i detta Biträdesavtal.
- 7.3. Personuppgiftsansvarig kan efter eget val ge ett allmänt skriftligt godkännande för Personuppgiftsbiträdet att anlita ett Underbiträde för viss typ av personuppgiftsbehandling inom ramen för Biträdesavtalet. Om ett sådant allmänt godkännande har lämnats ska Personuppgiftsbiträdet informera Personuppgiftsansvarig om sina avsikter att använda eller byta ut ett Underbiträde i god tid så att Personuppgiftsansvarig har möjlighet att göra invändningar mot en sådan förändring. En sådan invändning medför hinder för Personuppgiftsbiträdet att genomföra föreslagna förändringar.

## **8. Överföring till tredje land**

- 8.1. I fall där Personuppgiftsbiträdet i samband med Behandlingen överför Personuppgifter till Tredje land som av Europeiska kommissionen inte anses uppfylla en adekvat skyddsnivå i förhållande till Gällande dataskyddsregler ska Parterna ingå ett tilläggsavtal avseende detta.

- 8.2. Har Personuppgiftsbiträdet anlitat ett Underbiträde med innebörden att Personuppgifter överförs till Tredje land som Europeiska kommissionen inte anser uppfylla en adekvat skyddsnivå i förhållande till Gällande dataskyddsregler ska Personuppgiftsbiträdet och Underbiträdet ingå ett tilläggsavtal. I förekommande fall ska Personuppgiftsbiträdet tillhandahålla Personuppgiftsansvarig en underskriven kopia av ett sådant tilläggsavtal som avses ovan.

## **9. Ansvar för skada**

- 9.1. Har en Registrerad riktat anspråk mot Personuppgiftsansvarig på ersättning för skada eller om en behörig myndighet utfärdar vite eller andra administrativa påföljder och om detta har orsakats av att Personuppgiftsbiträdet har behandlat personuppgifter i strid med Personuppgiftsansvarigs instruktioner, detta Biträdesavtal eller Gällande dataskyddsregler ska Personuppgiftsbiträdet hålla Personuppgiftsansvarig skadeslös.
- 9.2. Personuppgiftsbiträdet åtar sig att även i övrigt hålla Personuppgiftsansvarig skadeslöst för det fall Personuppgiftsansvarig drabbas av skada till följd av Personuppgiftsbiträdets behandling av Personuppgifter i strid med detta Biträdesavtal eller Gällande dataskyddsregler.
- 9.3. Har en Registrerad riktat anspråk mot Personuppgiftsbiträdet på ersättning för skada eller om behörig myndighet utfärdar vite eller andra administrativa påföljder med anledning av Personuppgiftsansvarigs Behandling av Personuppgifter i strid med detta Biträdesavtal eller Gällande dataskyddsregler ska Personuppgiftsansvarig hålla Personuppgiftsbiträdet skadeslös.

## **10. Avtalstid**

- 10.1. Detta Biträdesavtal är giltigt från dagen för signering av båda Parter tills Personuppgiftsbiträdets Behandling av Personuppgifterna upphör eller tills det ersätts av ett nytt biträdesavtal.
- 10.2. Personuppgiftsbiträdet ska vid avslutad Behandling återlämna eventuella Personuppgifter som biträdet har i sin besittning i ett allmänt och läsbart format till Personuppgiftsansvarig och därefter radera Personuppgifterna från sådana system som använts vid Behandlingen, såvida inte detta är oförenligt med annan tvingande lagstiftning.

## **11. Lagval och tvistlösning**

- 11.1. På detta Biträdesavtal tillämpas svensk rätt, utan hänsyn till dess lagvalsregler.
- 11.2. Tvister i anledning av detta Biträdesavtal ska slutligt avgöras i allmän domstol, med *[ange vald tingsrätt]* som första instans.

Detta Biträdesavtal har upprättats i två (2) exemplar varav Parterna tagit varsitt.

\_\_\_\_\_  
[PERSONUPPGIFTSANSVARIG]

\_\_\_\_\_  
Ort och datum

\_\_\_\_\_  
Underskrift

\_\_\_\_\_  
Namnförtydligande

\_\_\_\_\_  
Titel

**Datea AB** \_\_\_\_\_  
[PERSONUPPGIFTSBITRÄDE]

\_\_\_\_\_  
Ort och datum

\_\_\_\_\_  
Underskrift

\_\_\_\_\_  
Namnförtydligande

\_\_\_\_\_  
Titel

## Bilaga 1

### Instruktioner för behandling av personuppgifter

Till personuppgiftsbiträdesavtal mellan [PERSONUPPGIFTSANSVARIG] och Datea AB, signerat datum: \_\_\_\_\_.

#### **BILAGA INSTRUKTIONER**

Dessa instruktioner utgör en integrerad del av Biträdesavtalet och ska följas av Personuppgiftsbiträdet vid utförande av Behandling av Personuppgifter såvida inte annat uttryckligen anges i Biträdesavtalet. Dessa instruktioner kan ändras ensidigt av Personuppgiftsansvarig vid en senare tidpunkt genom att Personuppgiftsansvarig skriftligen meddelar Personuppgiftsbiträdet om ändringen. Ändringar träder ikraft tidigast 30 kalenderdagar efter att de avsänts av Personuppgiftsansvarig. Genom undertecknande av Biträdesavtalet har Personuppgiftsbiträdet bekräftat innebörden av dessa instruktioner.

#### **Ändamål**

Ändamålet med behandlingen är 1) att leverera IT-tjänster enligt avtal ingånget mellan Parterna nedan "Tjänsteavtal" och levererade tjänster "Tjänst" 2) supportera Tjänst till kund 3) på annat sätt uppfylla ansvar under Tjänsteavtalet.

#### **Typ av Behandling**

Registrering av användaruppgifter, lagring av Personuppgifter, lagring av användande av Tjänst, statistikanalyser, felsökningsanalyser och faktureringsuppgifter/underlag.

#### **Typ av Personuppgifter**

Följande typer av Personuppgifter kan behandlas

- ✓ Namn
- ✓ Lösenord
- ✓ E-post
- ✓ Användar-ID
- ✓ Telefonnummer
- ✓ IP-adress
- ✓ Användargenererad data
- ✓ Kraschrapporter för felsökningar

Utöver detta kan Personuppgiftsansvarigs användare ladda upp Personuppgifter i tjänst. Personuppgiftsansvarig godkänner vid uppladdning att Personuppgiftsbiträdet behandlar och lagrar dessa uppgifter.



## **Plats för Behandlingen**

All behandling sker inom EUs medlemsstater, EES eller godkända stater enligt EU som uppfyller adekvat skyddsnivå.

## **Behandlingens varaktighet**

Behandling varar så länge Personuppgiftsbiträdet representerar Personuppgiftsansvarig. Vid avslutat Tjänsteavtal raderas Personuppgifter ur aktiva system och fasas ut från backuper över tid. Dessa backuper har begränsad åtkomst och Personuppgifter kan maximalt finnas kvar i två (2) år.

## **Underbiträden**

Följande typer av Underbiträden används:

### 1) Felsökning och optimering av tjänst

Vid fel i tjänst lämnas vissa Personuppgifter ut till underleverantörer, så som Microsoft, för att genomföra felsökning och återställa Tjänst. Övervakning och statistikföring av Tjänst görs kontinuerligt för att kunna optimera användning av Tjänst och identifiera eventuella buggar där vissa Personuppgifter lämnas ut till underbiträden så som exempelvis Google Analytics och Sophos.

### 2) Återförsäljare

Om Personuppgiftsansvarige ingår Tjänsteavtal via en av Personuppgiftsbitrådets återförsäljare har sagda återförsäljare tillgång till Personuppgifter för att supportera Tjänst.

### 3) Serverhallar

Underbiträden nyttjas för viss hosting av servrar, dessa underbiträden har sin verksamhet inom EU.

### 4) Svarstjänster

För vissa specifika svarstjänster (Datea Jour) används underbiträden som då får tillgång till vissa Personuppgifter.

## **Utlämnande av Personuppgifter**

Personuppgifter kan komma att lämnas ut till:

- Myndigheter

Personuppgiftsbiträdet är skyldigt att, på begäran enligt lag och myndighetsbeslut, lämna ut den data som följer av beslutet -tex. till polisen.

- Räddningstjänst

Vid till exempel samtal till SOS alarm

Personuppgifter kan även lämnas ut till andra företag, myndigheter efter att Personuppgiftsansvarige har lämnat samtycke och/eller för att uppfylla specifik del av Tjänst enligt avtal som till exempel Licenshantering.

## **Överföring till tredje land**

Överföring till tredje land utanför EU/EES sker endast i enlighet med artikel 45, 46 eller 49 i dataskyddsförordningen, och den senare endast under förutsättningen att överföringen är nödvändig för att fullgöra avtal mellan Personuppgiftsbiträdet och Personuppgiftsansvarig eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.

## **DATASKYDD, SÄKERHET OCH SEKRETESS**

Personuppgiftsbiträdet har vidtagit nödvändiga tekniska och organisatoriska åtgärder för att garantera integritet och konfidentialitet av Personuppgiftsansvarigs uppgifter, vilket kan innefatta följande åtgärder:

### **Personal Sekretess**

Personuppgiftsbiträdet har vidtagit nödvändiga åtgärder för att garantera att personal som arbetar med Personuppgiftsansvarigs Personuppgifter har kvalificerad bakgrund och kompetens. Dessa åtgärder kan innefatta:

- Skriftlig överenskommelse om tystnadsplikt
- Följer Personuppgiftsbiträdet aktuella policies och arbetsrutiner
- Kontinuerlig utbildning och kompetenshöjande åtgärder
- Bakgrundskontroller i form av referenser och/eller utdrag från belastningsregistret

### **Fysisk säkerhet**

Personuppgiftsbiträdet säkerhetsställer att en adekvat fysisk säkerhetsnivå på området där Personuppgiftsansvarig Personuppgifter behandlas upprätthålls vilket kan innefatta:

- Begränsad och/eller övervakad tillgång till fysiska lokaler
- Övervakning i form av larm, video och/eller fysisk övervakning

### **Utrustning-, system- och nätverkssäkerhet**

Personuppgiftsbiträdet ska genomföra lämpliga och tidsenliga säkerhetsåtgärder och för hela Tjänsteavtalets period upprätthålla en tillräcklig säkerhetsnivå för alla system, nätverk och enheter som används för att leverera Tjänst till Personuppgiftsansvarig. Detta kan innefatta;

- Har adekvat brandväggsskydd
- Auditloggning för övervakning av Tjänst
- Autentiseringssystem för tillgång till Tjänst och System
- Rättighetssystem för tillgång till Tjänst och System
- Övervakning & kryptering av fysiska hårddiskar
- Processer & rutiner för att kontinuerligt utvärdera datasäkerhet
- Säkerhetsställa möjligheter till återskapning av Personuppgifter via backuper