

PERSONUPPGIFTSBITRÄDESAVTAL

Detta Personuppgiftsbiträdesavtal ("Avtalet") har ingåtts av och mellan TSHK ("Biträdet") och Kund (den "Ansvarige").

Biträdet och den Ansvarige benämns individuellt som "Part" och gemensamt som "Parterna".

BAKGRUND

- (A) Detta Avtal utgör en del av Bitrådets Allmänna villkor som i sin tur är del av ett tjänsteavtal mellan Biträdet och den Ansvarige ("Tjänsteavtalet"). Under tjänsteavtalet kommer Biträdet behandla personuppgifter för den Ansvariges räkning i syfte att tillhandahålla tjänster enligt Tjänsteavtalet.
- (B) Den Ansvarige är personuppgiftsansvarig för behandlingen av Personuppgifterna. Biträdet är personuppgiftsbiträde och behandlar Personuppgifterna för den Ansvariges räkning. Tjänsteavtal som innebär en behandling av personuppgifter för den Ansvariges räkning är specificerade i Bilaga 1 till Avtalet under punkt "Kategorier av personuppgifter".

1 DOKUMENT

Detta Avtal består av detta huvuddokument med följande bilagor:

Bilaga 1 – Den Ansvariges instruktioner för personuppgiftsbehandling i samband med relevant tjänst

Bilaga 2 – Säkerhetsåtgärder

Bilaga 3 – Godkända Underbiträden

2 DEFINITIONER

- 2.1 I detta Avtal har de termer som inleds med versal nedanstående betydelse. I övrigt gäller de definitioner som anges i Tillämplig Lagstiftning.

GDPR	betyder Europaparlamentets och Rådets Förordning (EU) 2016/679, inklusive eventuella framtida ändringar och tillägg.
Personuppgifterna	betyder de personuppgifter (såsom definieras i Tillämplig Lagstiftning) som specificeras i <u>Bilaga 1</u> .
Tillämplig Lagstiftning	betyder GDPR och tillämplig kompletterande lagstiftning till GDPR.
Tjänsteavtalet	betyder det avtal som angivits i ovan stycke Bakgrund (A) i detta Avtal.

3 INSTRUKTIONER

- 3.1 Biträdet ska behandla Personuppgifterna i enlighet med den Ansvariges dokumenterade instruktioner, vilka framgår av för respektive Tjänsteavtal relevant del av Bilaga 1. Instruktionerna ska åtminstone innehålla följande information:
- (i) Behandlingens ändamål,
 - (ii) Behandlingens karaktär,
 - (iii) Hur länge behandlingen ska pågå, eller hur den tiden bestäms,
 - (iv) Vilka kategorier av personuppgifter som ska behandlas, och
 - (v) Vilka kategorier av registrerade som inkluderas i behandlingen.
- 3.2 Biträdet får inte behandla Personuppgifterna för andra ändamål än vad som följer av den Ansvariges instruktioner. Parterna ska uppdatera Bilaga 1 vid nya eller ändrade instruktioner. Biträdet har rätt till ersättning på löpande räkning i enlighet med mellan Parterna särskilt överenskommen pris eller Bitrådets vid var tid gällande prislista för konsulttjänster för sådant arbete Biträdet utför i syfte att följa den Ansvariges förändrade instruktioner.
- 3.3 Oaktat ovanstående har Biträdet rätt att i skälig omfattning vidta löpande åtgärder utan den Ansvariges uttryckliga instruktion, under förutsättning att Biträdet agerar för och i enlighet med de ändamål som framgår av Bilaga 1.
- 3.4 För det fall Biträdet anser att en instruktion strider mot Tillämplig Lagstiftning ska Biträdet avstå från att följa instruktionerna, genast underrätta den Ansvarige och invänta ändrade instruktioner.

4 DEN ANSVARIGES SKYLDIGHET ATT BEHANDLA PERSONUPPGIFTER LAGLIGT

- 4.1 Den Ansvarige ska säkerställa laglig grund föreligger för behandlingen av Personuppgifterna. Den Ansvarige ska vidare uppfylla alla andra skyldigheter som åläggs personuppgiftsansvariga i Tillämplig Lagstiftning (inklusive krav på att informera de registrerade om behandlingen av Personuppgifterna).
- 4.2 Den Ansvariges instruktioner för behandlingen av Personuppgifterna ska vara förenliga med Tillämplig Lagstiftning. Den Ansvarige ansvarar för att Personuppgifterna är korrekta och att behandlingen och insamlingen av dem är laglig.

5 SÄKERHETSÅTGÄRDER

- 5.1 Biträdet ska upprätthålla adekvata säkerhetsåtgärder för att säkerställa att Personuppgifterna är skyddade mot förstörelse, modifikation och spridning. Biträdet ska vidare säkerställa att Personuppgifterna är skyddade mot obehörigt intrång och att åtkomst till uppgifterna loggas med spårbarhet. Säkerhetsåtgärderna är beskrivna i Bilaga 2. Den Ansvarige godkänner dessa säkerhetsåtgärder som adekvata, tillräckliga och lämpliga.
- 5.2 Biträdet ska säkerställa (i) att endast behöriga personer hos Biträdet har tillgång till Personuppgifterna, (ii) att de behöriga personerna endast behandlar Personuppgifterna i

enlighet med Avtalet och den Ansvariges instruktioner, samt (iii) att varje behörig person hos Biträdet är bunden av sekretess som motsvarar den sekretessförbindelse som följer av detta Avtal.

- 5.3 Biträdet ska underrätta den Ansvarige utan onödigt dröjsmål efter att ha fått kännedom om en personuppgiftsincident. Biträdet ska bistå den Ansvarige i fullgörandet av den Ansvariges skyldigheter att (i) dokumentera varje personuppgiftsincident, (ii) meddela tillämplig tillsynsmyndighet vid en personuppgiftsincident, och (iii) informera de registrerade om sådan personuppgiftsincident, i enlighet med Tillämplig Lagstiftning.

6 BITRÄDETS SKYLDIGHET ATT BISTÅ DEN ANSVARIGE

- 6.1 Biträdet ska med tanke på behandlingens art, hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den Ansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av registrerades rättigheter enligt kapitel III i GDPR. Dessa rättigheter omfattar (i) rätt att göra invändning mot behandling och få Personuppgifter raderade, (ii) rätt att begära information om och tillgång till Personuppgifterna, (iii) om tekniskt möjligt, rätt till dataportabilitet via direktöverföring av Personuppgifter till ny personuppgiftsansvarig, och (iv) rätt till rättelse av Personuppgifterna.

- 6.2 Biträdet ska vidare med beaktande av typen av behandling och den information som Biträdet har att tillgå, bistå den Ansvarige i dennes fullgörande av sina skyldigheter enligt artiklarna 32–36 i GDPR. Dessa skyldigheter inkluderar (i) säkerställande av att behandlingen är säker, (ii) konsekvensbedömningar avseende dataskydd och (iii) förhandssamråd med tillsynsmyndigheten.

7 UNDERBITRÄDEN

- 7.1 Biträdet får anlita tredje part för att utföra hela eller del av behandlingen av Personuppgifter enligt detta Avtal ("Underbiträde"), om Biträdet skriftligen informerar den Ansvarige därom och den Ansvarige inte har invänt skriftligen inom tio dagar efter att Biträdet lämnade informationen till den Ansvarige. I sådant fall blir Underbiträdet ett "Godkänt Underbiträde". Godkända Underbiträden anges i Bilaga 3 (vilken ska uppdateras vid ändringar av Godkända Underbiträden). Bilaga 3 ska omfatta följande information om varje Godkänt Underbiträde:

- (i) namn, kontaktinformation, företagsform och geografisk plats för det Godkända Underbiträdet,
- (ii) en beskrivning av tjänsten som det Godkända Underbiträdet tillhandahåller,
- (iii) geografisk plats för behandlingen av Personuppgifterna.

- 7.2 Biträdet ska ingå ett skriftligt avtal med varje Underbiträde enligt vilket Underbiträdet åtar sig skyldigheter som i vart fall motsvarar de som Biträdet har åtagit sig enligt detta Avtal.

- 7.3 För det fall den Ansvarige i enlighet med punkt 7.1 ovan invänder mot ett nytt Underbiträde, ska Biträdet avstå från att anlita detta Underbiträde för behandling av Personuppgifterna. Biträdet ska då söka vidta rimliga åtgärder för att förändra tjänsten till den Ansvarige, för att undvika att aktuellt Underbiträde behandlar Personuppgifterna. Om

Biträdets finner att en sådan ändring inte är praktiskt eller kommersiellt möjlig eller rimlig så får Biträdets säga upp Avtalet med 45 dagars varsel. Sådan uppsägning måste göras senast 45 dagar efter att den Ansvariges skriftliga invändning mot det nya Underbiträdets kom Biträdets tillhanda.

- 7.4 När den Ansvarige har godkänt ett Underbiträde saknar den Ansvarige rätten att invända mot Underbiträdets.

8 ÖVERFÖRINGAR TILL TREDJE LAND

Biträdets får inte överföra Personuppgifterna utanför EU/EES utan den Ansvariges skriftliga godkännande och oaktat sådant godkännande. Sådan överföring får vidare endast ske om någon av följande förutsättningar är uppfylld:

- (i) mottagarlandet säkerställer en adekvat skyddsnivå för personuppgifter enligt Europakommissionen,
- (ii) den Ansvarige bekräftar att den registrerade har givit sitt samtycke till överföringen,
- (iii) överföringen är föremål för Europeiska kommissionens standardavtalsklausuler för överföring av personuppgifter till tredje land,
- (iv) Biträdets är föremål för bindande företagsbestämmelser och mottagaren i det tredje landet är också föremål för bindande företagsbestämmelser, eller
- (v) vid överföringar till USA, mottagaren är certifierad enligt Privacy Shield.

9 INSYN

- 9.1 På den Ansvariges begäran ska Biträdets tillhandhålla den Ansvarige sådan information som visar att Biträdets efterlever sina skyldigheter enligt Tillämplig Lagstiftning.
- 9.2 Den Ansvarige har rätt att med 20 dagars skriftligt varsel genomföra en granskning av Biträdets behandling av Personuppgifterna och information som är relevant i det avseendet för att visa att Biträdets efterlever detta Avtal och Tillämplig Lagstiftning. Biträdets ska bistå den Ansvarige och tillgängliggöra information som är nödvändig för att den Ansvarige ska kunna genomföra sådan granskning. Den Ansvarige ska bära kostnaderna för sådan granskning.
- 9.3 Om en tillsynsmyndighet utför en granskning av Biträdets som involverar behandlingen av Personuppgifterna ska Biträdets genast meddela den Ansvarige om det.

10 ERSÄTTNING

- 10.1 Biträdets ska ha rätt till ersättning för behandlingen av Personuppgifterna i enlighet med mellan Parterna särskilt överenskommet pris eller Biträdets vid var tid gällande prislista för konsulttjänster för sådant arbete som Biträdets utför.
- 10.2 Den Ansvarige ska vidare ersätta Biträdets i enlighet med Biträdets vid var tid gällande prislista för konsulttjänster för att tillgodose förändringar av eller tillägg i den Ansvariges instruktioner, samt för att uppfylla den Ansvariges anvisningar avseende Personuppgifterna och behandlingen av dessa.

11 ANSVARSBEGRÄNSNING

Bitrådets ansvar under detta Avtal omfattas av ansvarsbegränsningen i Tjänsteavtalet.

12 SEKRETESS

- 12.1 Bitrådet åtar sig att iaktta sekretess och att inte röja eller dela Personuppgifterna, eller information som relaterar till Personuppgifterna, till tredje part. Godkända Underbiträden anses inte vara tredje parter i detta avseende.
- 12.2 Oaktat vad som anges i punkt 12.1 ovan får Bitrådet röja sådan information om Bitrådet är skyldigt att göra det enligt lag, domslut eller myndighetsbeslut. Bitrådet ska genast skriftligen underrätta den Ansvarige när sådan skyldighet uppkommer, om inte Tillämplig Lagstiftning förbjuder sådan underrättelse.
- 12.3 Skyldigheten att iaktta sekretess ska fortsätta att gälla även efter att detta Avtal har upphört att gälla.
- 12.4 För övrigt iakttar Bitrådet sekretess avseende Personuppgifterna i enlighet med punkt 13 i Allmänna villkoren.

13 RADERING AV PERSONUPPGIFTER

- 13.1 Vid Tjänsteavtalets upphörande ska den Ansvarige skriftligen instruera Bitrådet om Personuppgifterna ska överföras till den Ansvarige eller inte. Sådan överföring ska göras i ett allmänt använt och maskinläsbart format.
- 13.2 Bitrådet ska oaktat vad som anges i punkt 13.1 ovan radera Personuppgifterna från sina system tidigast 30 dagar och senast 40 dagar efter Tjänsteavtalets upphörande.

14 AVTALSTID

För samtliga Tjänsteavtal som har slutits före den 25 maj 2018 är avtalsdatum för Avtalet den 25 maj 2018. I alla övriga fall ingås Avtalet jämte Allmänna villkoren med samma datum som Tjänsteavtalet mellan Parterna.

Oaktat Tjänsteavtalets avtalstid ska detta Avtal träda i kraft när Bitrådet inleder behandlingen av Personuppgifterna för den Ansvariges räkning och ska upphöra när Bitrådet har raderat Personuppgifterna i enlighet med punkt 13 ovan.

BILAGA 1 – INSTRUKTIONER

Bitrådets behandling av Personuppgifterna ska ske i enlighet med följande instruktioner. För det fall Bitrådets behandling av Personuppgifterna sker i strid med dessa instruktioner ska Bitrådet anses vara personuppgiftsansvarigt för sådan behandling.

	INSTRUKTION
Behandlingens ändamål	Att fullgöra skyldigheter enligt Tjänsteavtalet.
Behandlingens karaktär	Bitrådet behandlar Personuppgifterna för den personuppgiftsansvariges räkning i syfte att tillhandahålla tjänster enligt vad som följer av Tjänsteavtalet. Behandlingen kan vid vissa av nedanstående tjänster omfatta känsliga personuppgifter, t.ex. i syfte att administrera löneutbetalningar, dessutom kan behandlingen omfatta personnummer. För vad som gäller i det enskilda fallet, se nedan i kategorier av personuppgifter för respektive tjänst.
Behandlingens tidsperiod	Behandlingen pågår under den tiden Tjänsteavtalet gäller.
Kategorier av registrerade personer	Beroende på Tjänsteavtalets karaktär och omfattning kan Bitrådet komma att behandla personuppgifter till kategorier av registrerade personer enligt följande: den Ansvariges anställda, den Ansvariges föreståndare (så som styrelsemedlemmar, VD och firmatecknare), den Ansvariges kontaktpersoner.
Kategorier av personuppgifter	Kategorier av personuppgifter som behandlas i samband med fullgörandet av Tjänsteavtalet kan i samband med relevant tjänst vara följande: <u>Samtliga tjänster:</u> Namn, e-postadress, telefonnummer. <u>Betalning av kundfakturor (redovisning):</u> Enligt ovan. <u>Lönehantering:</u> Titel, nationalitet, kön, födelsedatum, ålder, personnummer, annat nationellt identifikationsnummer (t.ex. CPR, socialförsäkringsnummer, skatteregistreringsnummer eller passnummer), postadress, personlig e-postadress, konto- och kreditkortsuppgifter, sjukdom, frånvaro (semester, föräldraledighet, tjänstledighet etc.), tidrapportering, löne- och HR-

	INSTRUKTION
	<p>dokumentation.</p> <p><u>Tjänster i samband med virtuellt kontor:</u></p> <p>Titel, nationalitet, kön, födelsedatum, ålder, personnummer, annat nationellt identifikationsnummer, postadress, personlig e-postadress, konto- och kreditkortsuppgifter.</p>
Andra instruktioner	Ingen uppgift.

BILAGA 2 – SÄKERHETSÅTGÄRDER

Tekniska och organisatoriska säkerhetsåtgärder

Biträdet har ansvaret för de tekniska och organisatoriska säkerhetsåtgärderna i Bitrådets system. Biträdet arbetar kontinuerligt med dataskyddsfrågor avseende program, tjänster och processer.

Det innebär att Biträdet ser till att det finns den lämpliga säkerheten vid exempelvis kryptering, behörighetsstyrning etc. Biträdet har ett koncept för borttagning/radering av uppgifter samt uppfyller övriga krav på dataskydd och integritet.

Tillgång till lokaler

Biträdet behandlar personuppgifter i egna lokaler. Tillgång till lokalerna sker genom ett personbunden chipsystem som tillåter olika tillgångsbehörigheter. Lokalerna är skyddade med larmsystem. Endast behöriga medarbetare har tillgång till respektive lagring av personuppgifter och/eller servrar. Besökare mottas av receptionen och har inte tillträde till avdelningar, där behandling av personuppgifter sker. Lokalerna är brandskyddsanpassade.

Tillgång till data-system

Samtliga rättigheter administreras endast av Bitrådets IT-stöd. Samtliga datasystem är lösenordsskyddade och kraven på skyddsnivån är reglerade i en intern policy. Tillgång till datasystem har endast med ärendet befattad personal som har olika restriktiva behörigheter.

Lagring och backuper

Biträdet har egna servrar i Bitrådets lokaler. Lagringen av backuper sker på två separerade platser i Stockholm med full redundans och backup tas dagligen. Endast godkänd personal har fysisk tillgång till serverna. Serverna och Bitrådets nätverk skyddas av brandvägg samt antivirussoftware.

Kunskap- och informationsskydd

Bitrådets personal är informerad om dataskydd och dataintegritet samt bunden av ett sekretessavtal som förhindrar spridning av data, information, samt Bitrådets kunders och användarens personuppgifter. Endast behörig personal har tillgång till uppgifterna och behörigheten styrs av Bitrådets IT-stöd. Även externa leverantörer, så som städpersonal, är noggrant utvalda och bunden av sekretessavtal.

Säkerhetsincidenthantering

Vid en säkerhetsincident som påverkar eller kan påverka Ansvarig vidtar Biträdet omgående lämpliga åtgärder och rapporterar omgående till Ansvarigs kontaktperson.

BILAGA 3 – GODKÄNDA UNDERBITRÄDEN

Biträdet anlitar följande godkända underbiträden vid tjänster av de enskilda avdelningarna enligt nedan:

Avdelning Lönetjänster:

Flexapplications Sverige AB, Drottninggatan 22, 702 10 ÖREBRO

Org.nr: 556616-1948

Beskrivning av tjänst: Rapportering av tid och reseräkningar till lön

Personuppgifterna behandlas i Sverige.

Fortnox AB, Box 427, 351 06 VÄXJÖ

Org.nr: 556469-6291

Beskrivning av tjänst: Lönesystem

Personuppgifterna behandlas i Sverige

Avdelning Redovisningstjänster:

Fortnox AB, Box 427, 351 06 VÄXJÖ

Org.nr: 556469-6291

Beskrivning av tjänst: Redovisningssystem,

Personuppgifterna behandlas i Sverige