BILAGA

PERSONUPPGIFTSBITRÄDESAVTAL

Detta PERSONUPPGIFTSBITRÄDESAVTAL (”**Biträdesavtal**”) är träffat mellan:

1. **Companyexpense Svenska AB,** organisationsnummer 556977-0075, (”**CSAB**”), och

2. **XXXX,** organisationsnummer xxxxxx-xxxx (”**Personuppgiftsansvarig**”).

   Härefter enskilt benämnd ”Part” och tillsammans ”Parterna”.

Detta Biträdesavtal ska anses utgöra en del av Huvudavtalet som slutits mellan Parterna.

1. BAKGRUND

1.1 CSAB är leverantör av en reseräkningstjänst, Companyexpense. CSAB lagrar kundens data på CSABs servrar. CSAB agerar *personuppgiftsbiträde* för dessa kunder som i sin tur är *personuppgiftsansvariga* (”**Personuppgiftsansvarig**”) för behandlingen av de personuppgifter CSAB behandlar för Personuppgiftsansvarigs räkning.

1.2 Detta biträdesavtal reglerar CSABs rättigheter och skyldigheter i egenskap av *personuppgiftsbiträde* till Personuppgiftsansvarig vid behandling av personuppgifter kopplade till CSABs leverans av Tjänsten (se Bilaga 1) till Personuppgiftsansvarig samt dess personal.

2. DEFINITIONER

2.1. Om inget annat anges ska definitioner angivna i detta Biträdesavtal anses ha samma innebörd som i Gällande Dataskyddsregler och med ”Gällande Dataskyddsregler” avses den allmänna dataskyddsförordningen (”GDPR”) (EU) 2016/679, Dataskyddslagen (2018:218) och Datainspektionens bindande föreskrifter och beslut.

2.2. Med ”**Tredje Land**” avses ett land som inte ingår i Europeiska Unionen eller är ansluten till Europeiska Ekonomiska Samarbetsområdet (”EES”.

2.3. Med ”**Underbiträde**” avses sådant personuppgiftsbiträde som anlitas av det Personuppgiftsbiträde som är Part i detta Biträdesavtal och som behandlar Personuppgifter för Personuppgiftsansvarigs räkning.

3. BILAGA TILL BITRÄDESAVTALET

3.1. Specifikation över behandlingen av personuppgifter finns Bilaga 1.

4. BEHANDLING AV PERSONUPPGIFTER

4.1. CSAB förbinder sig att endast behandla personuppgifter enligt dokumenterade instruktioner från Personuppgiftsansvarig såvida inte annat följer av tillämplig dataskyddslagstiftning. Instruktioner om behandlingens föremål och varaktighet,

behandlingens karaktär och ändamål, typ av personuppgifter och kategorier av registrerade anges i detta Biträdesavtal och i Bilaga 1.

4.2. Personuppgiftsansvarig bekräftar att CSABs skyldigheter enligt detta Biträdesavtal, inklusive Bilaga 1, utgör de fullständiga och kompletta instruktioner som ska följas av CSAB. Alla ändringar i Personuppgiftsansvarigs instruktioner ska förhandlas separat och ska, för att bli gällande, dokumenteras skriftligt i Bilaga 1 och undertecknas av båda parter, med undantag för sådana instruktioner som Personuppgiftsansvarig ska ha rätt att lämna på grund av ändringar i tillämplig dataskyddslagstiftning.

5. PERSONUPPGIFTSANSVARIGS ANSVAR

5.1. Personuppgiftsansvarig ska ansvara för att Behandlingen av Personuppgifter är laglig och sker i enlighet med Gällande Dataskyddsregler.

5.2. Personuppgiftsansvarig ska endast ge Personuppgiftsbiträdet tillträde till de Personuppgifter som är nödvändiga med hänsyn till ändamålet med Behandlingen.

5.3. Personuppgiftsansvarig ska omedelbart lämna Personuppgiftsbiträdet korrekta uppgifter i händelse av att instruktionerna är felaktiga, ofullständiga eller i övrigt behöver förändras.

6. UTLÄMNANDE AV PERSONUPPGIFTER

6.1. CSAB förbinder sig att inte utan föregående skriftligt medgivande från Personuppgiftsansvarig utlämna eller på annat sätt göra personuppgifter som behandlas enligt detta Biträdesavtal tillgängliga för tredje part, om annat inte följer av svensk eller europeisk lag, domstols- eller myndighetsbeslut.

6.2. Om registrerad person begär information från Personuppgiftsansvarig om behandlingen av personuppgifter ska Personuppgiftsansvarig utan onödigt dröjsmål hänskjuta sådan begäran till CSAB.

6.3. Om behörig myndighet begär information från CSAB om behandlingen av personuppgifter ska CSAB utan onödigt dröjsmål informera Personuppgiftsansvarig om detta. CSAB får inte i något avseende handla för Personuppgiftsansvarig och får inte utan föregående medgivande från Personuppgiftsansvarig överföra eller på annat sätt lämna ut personuppgifter eller andra uppgifter rörande behandlingen av personuppgifter till tredje part, om annat inte följer av svensk eller europeisk lag, domstols- eller myndighetsbeslut.

6.4. Om det enligt tillämpliga svenska eller europeiska lagar och regelverk begärs att CSAB ska utlämna personuppgifter som CSAB behandlar i enlighet med detta Biträdesavtal, är CSAB skyldigt att omgående meddela Personuppgiftsansvarig om detta, om annat inte följer av aktuell lag, domstols- eller myndighetsbeslut, och att i samband med utlämnandet begära att uppgifterna behandlas med sekretess.

7. UNDERBITRÄDEN OCH TREDJELANDSÖVERFÖRINGAR

7.1. CSAB förbinder sig att inte utan föregående skriftligt medgivande från Personuppgiftsansvarig anlita Underbiträden för att behandla personuppgifter enligt detta Biträdesavtal. Sådant medgivande ska dock inte nekas utan att

Personuppgiftsansvarig kan ange rimliga och sakliga skäl.

7.2. Något särskilt skriftligt medgivande enligt punkten 6.1 ovan behövs dock inte för Underbiträden som anlitas enbart som extra resurser och alternativ till egna anställda och där överföring av personuppgifter inte sker till Underbiträdet.

7.3. CSAB förbinder sig att inte utan föregående skriftligt medgivande från Personuppgiftsansvarig överföra personuppgifter till Tredje Land. 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.

8. DATASÄKERHET OCH SEKRETESS

8.1. CSAB är skyldigt att fullgöra sina rättsliga förpliktelser avseende informationssäkerhet under tillämplig dataskyddslagstiftning och ska i samtliga fall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

8.2. CSAB är skyldigt att säkerställa att endast sådan personal som direkt måste ha tillgång till personuppgifter för att kunna fullgöra CSABs skyldigheter enligt detta Biträdesavtal får tillgång till sådana uppgifter. CSAB ska säkerställa att sådan personal omfattas av en lämpliga sekretessförbindelser.

9. NOTIFIERINGAR VID DATAINTRÅNG

9.1. CSAB ska utan onödigt dröjsmål, dock senast inom 72 timmar, underrätta Personuppgiftsansvarig efter att ha fått vetskap om en personuppgiftsincident.

9.2. CSAB ska bistå Personuppgiftsansvarig med den information som rimligen kan krävas för att uppfylla lagstadgad skyldighet att anmäla personuppgiftsincidenter.

10. RÄTT TILL GRANSKNING

10.1. Personuppgiftsansvarig ska ha rätt att vidta rimliga erforderliga åtgärder för att verifiera att CSAB kan fullgöra sina skyldigheter enligt detta Biträdesavtal och att CSAB faktiskt har vidtagit de åtgärder som krävs för att säkerställa att dessa fullgörs.

10.2. CSAB förbinder sig att tillhandahålla Personuppgiftsansvarig all rimlig information som krävs för att visa att de skyldigheter som anges i detta Biträdesavtal efterlevs, samt att möjliggöra för och medverka till sådan granskning, inklusive kontroll på plats, som genomförs av Personuppgiftsansvarig eller annan auktoriserad och kvalificerad granskare som utsetts av Personuppgiftsansvarig under förutsättning att de personer som utför granskningen ingår av CSAB utformat sekretessavtal.

10.3. Personuppgiftsansvarig ska omedelbart informera CSAB om denne anser att en granskning enligt punkt 10.1 ovan från Personuppgiftsansvarig utvisar brister i

förhållande till Gällande Dataskyddsregler.

11. AVTALSTID

11.1. Bestämmelserna i detta Biträdesavtal ska gälla så länge som CSAB behandlar personuppgifter för vilka CSAB är personuppgiftsbiträde till Personuppgiftsansvarig.

12. ÅTGÄRDER NÄR BEHANDLINGEN AV PERSONUPPGIFTER AVSLUTATS

12.1. När detta Biträdesavtal upphör ska CSAB, beroende på vad Personuppgiftsansvarig väljer, radera eller återlämna alla personuppgifter som behandlats enligt detta Biträdesavtal inom trettio (30) dagar, om inte lagring av personuppgifterna krävs enligt svensk eller europeisk lagstiftning.

12.2. På begäran av Personuppgiftsansvarig ska CSAB skriftligen bekräfta vilka åtgärder som vidtagits avseende personuppgifterna efter behandlingens avslutande enligt punkt 12.1 ovan.

13. ERSÄTTNING

13.1. CSAB har rätt till ersättning enligt CSAB vid var tid gällande prislista för det arbete som utförts på grund av skyldigheterna i punkterna 5.3, 9.2, 10 och 12 i detta Biträdesavtal.

Bilaga 1
Instruktioner för databehandlingen

Ändamål Ange alla ändamål för vilka personuppgifterna ska behandlas av CSAB	CSAB samlar uppgifter om Användarna i syfte att tillhandahålla Tjänsten till Användarna. Tjänsten är en s.k utläggstjänst där Användarna registrerar sina tjänsteutlägg, traktamenten och milersättningar. Dessa uppgifter samt de personuppgifter Användaren registrerat och de uppgifter tjänsten automatiskt registrerar om Användarna lagras och behandlas av CSAB i Tjänsten och sammanställs i format som därefter registreras och lagras i bokförings- och lönesystem.
Kategorier av uppgifter Ange vilka personuppgifter som ska behandlas av CSAB	Registrerade personuppgifter om den anställde: Namn, mejladress, telefonnummer, personnummer, anställningsnummer, adress, organisationstillhörighet, språk, kontonummer, profilbild. Transaktionsdata: Kvitton, Fakturor, Vistelseorter och vistelsedatum/tid. Deltagaruppgifter vid representation. Browser/appuppgifter: Cookies, IP-adress, Geoposition.
Kategorier av registrerade Ange för vilka kategorier av registrerade som CSAB kommer att behandla personuppgifter om.	Användare: De som rapporterar tjänsteutlägg, traktamenten eller milersättningar i syfte att få ersättning för dessa Chefer/Attestanter: De som godkänner/Avstår utläggsrapporter: Redovisningskonsulter/Ekonomiansvariga: De som granskar och/eller bokför utlägg. Administratörer: De som administrerar sin

	organisation i tjänsten.
Behandlingsaktiviteter Ange vilka behandlingsaktiviteter som kommer att utföras av CSAB.	Registrering och lagring av utlägg, Traktamenten och milersättning Samanställning av ovanstående i utläggsrapporter. Vidarebefordran av utläggsrapporter till attestant(er) inom Tjänsten. Vidarebefordring av utläggsrapporter till bokförings- och/eller lönesystem. Långtidslagring av Personuppgifter, kvitton, fakturor, milersättning, traktamenten, utläggsrapporter.
Plats för behandling av personuppgifterna Ange alla platser där personuppgifter kommer att behandlas av CSAB.	Datacenter 1: Ekonomivägen 4, Askim Datacenter 2: Norra Stationsg 93, Stockholm Kontor 1: Engelbrektsgatan 18, Ludvika Kontor 2: Alströmergatan 22, Stockholm Kontor 3: Lilla bommen 6, Göteborg
Informationssäkerhet	Fysisk säkerhet: CSABs system är utlokaliserade till dedikerade datacenter. Fysisk åtkomst regleras till behörig personal av datacenteroperatören. För tillträde krävs inregistrering. Skalskyddet består av Intrångslarm, brandlarm, vattenlarm, videoövervakning, kodlås samt fysiska lås. Kommunikation och Drift: CSABs tjänster driftas uteslutande på egen infrastruktur i

form av fysiska och virtuella servrar.

Externa Nätverkskopplingar: Externa nätverkskopplingar härdas och konfigureras för att skydda mot obehörig trafik. Alla externa anslutningar till tjänsterna sker genom ett DMZ och registreras i en händelselog.

Systemåtkomst och loggning: Backend skyddas från obehörig åtkomst genom åtkomstkontrollistor, autentisering och kryptering via OpenVPN Access Server i DMZ. Endast systemoperatörer äger tillgång till Backend och dessa registreras i OpenVPN Access Server. All trafik går via DMZ.

Kryptering: All kommunikation till och från CSABs tjänster, system till system eller program till program, som går utanför backend krypteras. Överföring av information mellan internet och backend krypteras via HTTPS/SSL alternativt SSH.

Kontroller av skadlig kod: Kontroller för att upptäcka och förhindra att skadlig kod körs sker regelbundet med hjälp av applikationer för rootkitsdetektering.

Informationsdelning: CSABs data separeras i separata databastabeller och skyddas av åtkomstlistor i syfte att förhindra obehörig åtkomst till informationen ide fall information bearbetas på delade servrar. Brandväggar separerar Webb- och applikationsservrar från databasservrar.

Systemåtkomst: Åtkomst till produktionssystemets backend kan endast nås genom VPN. Tillgång till backend ges baserat på funktionella krav för tjänsten och

åtkomst begränsas till de resurser som krävs för att möta företagets behov.

Underleverantörer: Anlitade underleverantörer har endast tillgång till de delar av tjänsterna som är nödvändiga för att underleverantörerna skall kunna utföra den tjänst eller de tjänster de är anlitade för.