

Detta personuppgiftsbiträdesavtal ("DPA") är giltigt från och med det sista datumet för signatur mellan **Oxceed AB**, Reg. No. 559027-9120, Herrjärva Torg 4, 170 67 Solna, Sverige ("**Leverantören**") och den fysiska eller juridiska person ("**Kunden**") som ingår avtalet med Oxceed avseende nyttjande av Oxceeds molnbaserade tjänst för beslutsstöd och verksamhetsstyrning, samt tilläggstjänster ("**Tjänsteavtalet**").

PERSONUPPGIFTSBITRÄDESAVTAL

1. INLEDNING

- 1.1. Kunden och Leverantören (tillsammans "**Parterna**" och var för sig "**Part**") har ingått Tjänsteavtalet.
- 1.2. Leverantören (hädanefter "**Biträdet**") kommer med anledning av Tjänsteavtalet att behandla personuppgifter som personuppgiftsbiträde för följande organisationers räkning:
 - Kunden
 - De organisationer som specificeras i **Bilaga 3** (Kundbolag) (hädanefter "**Kundbolag**").Kunden och Kundbolag (om tillämpligt) hänvisas hädanefter till som "**Ansvarig**".
- 1.3. Med anledning av den behandling Biträdet utför för Ansvarigs räkning ingår Parterna detta DPA.
- 1.4. Detta DPA utgör en del av Tjänsteavtalet. Om villkor i detta DPA strider mot villkor i Tjänsteavtalet ska villkoren i detta DPA äga företräde.

2. FLERA PERSONUPPGIFTSANSVARIGA

- 2.1. Denna punkt 2 tillämpas endast om Ansvarig utgörs av fler än en juridisk person (se punkt 1.2 ovan).
- 2.2. Bitrådets rättigheter och skyldigheter ska gälla i förhållande till samtliga Ansvariga. Endast Kunden, inga Kundbolag, blir dock avtalspart till detta DPA. Skada som Biträdet åsamkar Kundbolag ska, i förhållandet till Biträdet, anses ha åsamkats Kunden, och skada som Kundbolag orsakar Biträdet ska anses ha orsakats av Kunden. Rättigheter och skyldigheter som Kundbolag har gentemot Biträdet under detta DPA ska kanaliseras via Kunden.
- 2.3. Kunden ansvarar för att Kundbolagen följer villkoren i detta DPA och är ansvarig för Kundbolags agerande och underlåtenhet.
- 2.4. Biträdet ska inte kommunicera direkt med Kundbolag. All kommunikation mellan Ansvarig och Biträdet under detta DPA ska ske via Kunden. Om det i detta DPA anges att Biträdet ska informera Ansvarig, ska Biträdet endast tillställa Kunden informationen. Det åligger Kunden att vidarebefordra nödvändig kommunikation mellan Biträdet och relevant Kundbolag.

3. AVTALSSTRUKTUR

- 3.1. Detta DPA ska tolkas mot bakgrund av den terminologi som används i Europaparlamentets och Rådets förordning (EU) 2016/679 ("GDPR").
- 3.2. Detta DPA består av detta huvuddokument och följande bilagor:

Bilaga 1	Behandling
Bilaga 2	Underbiträden
Bilaga 3	Kundbolag

4. ANSVARIGS INSTRUKTIONER

- 4.1. Biträdet får endast behandla personuppgifter på dokumenterade instruktioner från Ansvarig, såvida inte behandling krävs enligt lag som Biträdet omfattas av. Biträdet ska i så fall informera Ansvarig om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden enligt lag.
- 4.2. Ansvarig instruerar härmed Biträdet att behandla personuppgifter i enlighet med **Bilaga 1** (Behandling) och i den utsträckning det är nödvändigt för att leverera enligt Tjänsteavtalet.
- 4.3. Om tillägg eller ändringar (exempelvis genom change request eller tilläggstjänster) görs till eller i Tjänsteavtalet ska Parterna utan onödigt dröjsmål sörja för att detta DPA ändras i enlighet därmed, i den utsträckning det är nödvändigt.
- 4.4. Ansvarig har endast rätt att ge Biträdet instruktioner i enlighet med **Bilaga 1** (Behandling) och som har ett naturligt samband med de tjänster som tillhandahålls under Tjänsteavtalet. Ansvarig har rätt att ändra befintliga instruktioner eller ge ytterligare instruktioner om det är nödvändigt för att Ansvarig ska kunna följa GDPR. Ansvarig har inte rätt att överföra andra personuppgifter än de som anges i **Bilaga 1** (Behandling) till Biträdet.
- 4.5. Om Biträdet överträder GDPR genom att fastställa ändamålen med och medlen för behandling, ska Biträdet anses vara personuppgiftsansvarig för sådan behandling.

5. ANSVARIGS ÅTAGANDEN

- 5.1. Ansvarig ska ge Biträdet tydliga och nödvändiga dokumenterade instruktioner för behandlingen av personuppgifter. Om Biträdet begär förtydligande eller ytterligare instruktioner för att kunna utföra Ansvarigs instruktion, ska Ansvarig omedelbart ge förtydliganden eller ytterligare instruktioner. Biträdet har rätt att avvakta att vidta åtgärder eller fortsätta pågående åtgärder i väntan på Ansvarigs förtydligande eller ytterligare instruktion.
- 5.2. Ansvarig ska vid var tid följa tillämplig dataskyddslagstiftning inklusive GDPR (tillsammans "**Tillämplig Lag**"). Ansvarig ska inte ge Biträdet instruktioner som bryter mot GDPR eller annan tillämplig lag.
- 5.3. Om Biträdet informerar Ansvarig att Biträdet anser att instruktion strider mot tillämplig lag, ska Ansvarig omedelbart ändra sin instruktion i den utsträckning det är nödvändigt för att instruktionen inte ska strida mot tillämplig lag.

6. SÄKERHET

- 6.1. Biträdet ska, med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i enlighet med Artikel 32 GDPR.
- 6.2. I enlighet med ovanstående ska Biträdet implementera de säkerhetsåtgärder som anges i Tjänsteavtalet. Ansvarig bekräftar att denne tagit del av den beskrivning av säkerhetsåtgärder som återfinns i Tjänsteavtalet samt att säkerhetsåtgärderna utgör en lämplig säkerhetsnivå i enlighet med Artikel 32.
- 6.3. Biträdet har rätt att ensidigt uppdatera säkerhetsbeskrivningen i Tjänsteavtalet för att spegla de förändringar Biträdet gör i tjänsten eller säkerheten. Sådana förändringar får inte innebära en icke oväsentlig försämring av säkerheten.
- 6.4. Biträdet ska säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.
- 6.5. Biträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under Bitrådets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från Ansvarig, om inte tillämplig lag ålägger denne att göra annorledes.

7. ANLITANDE AV UNDERBITRÄDEN

- 7.1. Ansvarig ger härmed Biträdet rätt att anlita andra personuppgiftsbiträden ("**Underbiträden**") inom och utanför EU/EES för behandling av personuppgifter för Ansvarigs räkning under förutsättning att följande procedur följs.

Biträdet ska informera Ansvarig om avsikten att ersätta eller anlita nytt Underbiträde så att Ansvarig har möjlighet att invända mot förändringen. Ansvarig har endast rätt att invända mot ersättandet eller anlitandet av nytt Underbiträde om Ansvarig kan visa sakliga skäl för invändningen grundade i GDPR ("**Sakliga Skäl**"). Ansvarig ska tillstålla Biträdet sin eventuella invändning skriftligen tillsammans med skriftlig dokumentation som motiverar och ger stöd för Ansvarigs Sakliga Skäl inom sju (7) dagar från Bitrådets meddelande ("**Invändning**"). Ansvarigs uteblivna Invändning inom de (7) dagarna är att anse som Ansvarigs godkännande av Underbiträdet.

Om Underbiträdet endast ska användas för Ansvarig ska Biträdet vidta kommersiellt rimliga åtgärder för att åtgärda de Sakliga Skälen bakom Ansvarigs Invändning.

Om Biträdet inte med ovan beskrivna åtgärder, inom rimlig tid åstadkommer en kommersiellt rimlig lösning på de Sakliga Skälen, eller om Underbiträdet inte enbart ska användas för Ansvarig utan även för annan/andra av Bitrådets kunder som köper tjänsten i fråga, har Ansvarig, efter Bitrådets skriftliga meddelande om att Underbiträdet kommer att anlitas trots Invändningen, rätt att skriftligen säga upp de delar av Tjänsteavtalet som inte kan levereras utan Underbiträdet, med upphörande från och med förändringen av Underbiträde och få återbetalt betalning för förbetalda men icke utnyttjade tjänster. Ansvarig har utöver detta ingen rätt till kompensation eller andra påföljder.

- 7.2. Om Biträdet anlitar Underbiträde för utförande av behandling för Ansvarigs räkning ska Underbiträdet, genom ett avtal eller en annan rättsakt enligt EU-rätten eller enligt EU-medlemsstats nationella rätt, åläggas motsvarande skyldigheter i fråga om persondataskydd som de som fastställs i detta DPA.

8. BEHANDLING UTANFÖR EU/EES

- 8.1. Biträdet ansvarar för att Underbiträden som är etablerade i land utanför EU/EES (som inte säkerställer en adekvat skyddsnivå enligt Artikel 45.1 GDPR) omfattas av lämpliga skyddsåtgärder enligt Artikel 46 GDPR.

9. BITRÄDETS BISTÅND TILL ANSVARIG

- 9.1. Biträdet ska, med tanke på behandlingens art, hjälpa Ansvarig genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att Ansvarig kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter under kapitel III GDPR. Ansvarig ska i den mån det är möjligt fullgöra sina skyldigheter på teknisk väg utan Bitrådets hjälp.
- 9.2. Om Biträdet emottar en fråga, begäran eller av annan anledning kontaktas av en registrerad eller tillsynsmyndighet rörande behandling för vilken Ansvarig är personuppgiftsansvarig, ska Biträdet meddela Ansvarig detta, hänvisa den registrerade eller tillsynsmyndigheten till Ansvarig och underlåta att ge information eller vidta andra åtgärder med anledning av förfrågan eller begäran, om inte annat krävs enligt lag.
- 9.3. Biträdet ska, med beaktande av typen av behandling och den information som Biträdet har att tillgå, bistå Ansvarige med konsekvensbedömning avseende dataskydd och förhandssamråd i enlighet med Artikel 35 och Artikel 36 GDPR.
- 9.4. Biträdet har rätt till ersättning i enlighet med Bitrådets vid var tid gällande prislista för åtgärder vidtagna eller kostnader som uppstår under denna punkt 9 eller detta DPA i övrigt.

10. RADERING

- 10.1. Biträdet ska, beroende på vad Ansvarig väljer, radera eller återlämna alla personuppgifter till Ansvarig utan onödigt dröjsmål efter det att tillhandahållandet av behandlingstjänsterna har avslutats, samt radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt tillämplig lag. Om inte Ansvarig ger en instruktion innan behandlingstjänsterna har avslutats, ska Biträdet radera personuppgifterna efter Tjänsteavtalets upphörande. Oaktat föregående mening ska backuper skrivas över i enlighet med Bitrådets överskrivningsrutiner för backuper.

11. REVISION

- 11.1. Ansvarig har rätt till max en revision per avtalsår. Ansvarig ska begära revision skriftligen minst tre (3) månader i förväg. Begäran ska innehålla en detaljerad beskrivning av Ansvarigs avsedda syfte, föremål, metod och omfattning av revisionen (tillsammans "Revisionsföremålet"), för vilken eller vilka Ansvarigas räkning revisionen görs samt huruvida Ansvarig önskar använda en revisionsbyrå. Revisionsföremålet samt datum och tid för revisionen ska överenskommas mellan Parterna. Revision ska utföras av Ansvarig eller en globalt erkänd revisionsbyrå såsom KPMG, EY, PwC eller Deloitte.
- 11.2. Om Biträdet tillhandahåller Ansvarig en revisionsrapport, ska Ansvarig i första hand använda revisionsrapporten som underlag för sin revision av Biträdet.
- 11.3. I den utsträckning det krävs ytterligare information för att visa att de skyldigheter som fastställs i detta DPA och beskrivits i Revisionsföremålet har fullgjorts, har Ansvarig rätt till sådan ytterligare information endast i den utsträckning punkt 11.2 inte är tillräcklig.
- 11.4. I den utsträckning det krävs ytterligare granskning, inklusive inspektion, för att visa att de skyldigheter som fastställs i detta DPA och beskrivits i Revisionsföremålet har fullgjorts, har Ansvarig rätt till sådan ytterligare information endast i den utsträckning det är proportionerligt, absolut nödvändigt och punkt 11.2 och 11.3 inte är tillräckliga.

- 11.5. Biträdet kan neka begäran om information, inspektion eller revision i övrigt om den begärda revisionsåtgärden kan innebära en fara för säkerhet, eller andra kunders data, eller är känslig affärsinformation.
- 11.6. Resultatet och slutsatserna av revisionen ska delas med Biträdet i skriftlig form utan onödigt dröjsmål efter slutförande av revision.
- 11.7. Ansvarig och revisionsbyrå som utför revision ska, innan revisionens påbörjande, ingå sekretessavtal med Biträdet. Samtlig dokumentation, information eller data som insamlas eller resultat av revisionen utgör Bitrådets konfidentiella information och ska hållas konfidentiell av Ansvarig. Ansvarig får endast använda dokumentationen, informationen, datat, resultat eller slutsatser i syfte att utvärdera i vilken utsträckning Biträdet fullgör detta DPA och får endast göras tillgänglig för de anställda hos den eller de Ansvariga för vilkas räkning revisionen görs enligt punkt 11.1, i den utsträckning det är nödvändigt för detta syfte. Oaktat punkt 13, är Ansvarigs ansvar för brott mot denna punkt 11.7 obegränsat.
- 11.8. Ansvarig ska stå samtliga kostnader för revisionen.
- 11.9. Biträdet ska omedelbart informera Ansvarig om Biträdet anser att Ansvarigs instruktion under denna punkt 11 strider mot GDPR.

12. PERSONUPPGIFTSINCIDENTER

- 12.1. I händelse av en personuppgiftsincident ska Biträdet utan onödigt dröjsmål informera Ansvarig om personuppgiftsincidenten och ange namn och kontaktuppgifter till en kontaktperson från vilken Ansvarig kan erhålla mer information.
- 12.2. Biträdet ska, med beaktande av typen av behandling och den information som Biträdet har att tillgå, på Ansvarigs anmodan bistå Ansvarig med att se till att Ansvarig kan uppfylla sin skyldighet att informera registrerade om personuppgiftsincidenten. Om det inte är möjligt för Biträdet att tillhandahålla all information samtidigt, får informationen tillhandahållas i omgångar, vilket ska ske utan onödigt dröjsmål.
- 12.3. I den utsträckning personuppgiftsincidenten uppkommit på grund av Ansvarigs brott mot detta DPA, tillämplig lag eller Tjänsteavtalet, har Biträdet rätt till ersättning för kostnader som uppstått och åtgärder vidtagna med anledning av personuppgiftsincidenten.

13. ANSVAR

- 13.1. Part ska ersätta den andra Parten för direkt skada som Part åsamkar den andra Parten genom brott mot detta DPA, Tillämplig Lag eller, vad gäller Biträdet, Ansvarigs instruktion, inom ramen för den ansvarsbegränsning som anges i Tjänsteavtalet.
- 13.2. Om Underbiträde inte fullgör sina skyldigheter i fråga om dataskydd ska Biträdet vara fullt ansvarigt gentemot Ansvarig för utförandet av Underbitrådets skyldigheter.

14. AVTALSTID

- 14.1. Detta DPA ska gälla tills det senare av:
 - 14.1.1. upphörandet av Tjänsteavtalet; och
 - 14.1.2. när Biträdet inte längre behandlar (inklusive i backuper) personuppgifter för Ansvarigs räkning.

15. LAGVAL OCH TVISTLÖSNING

- 15.1. Tvister som uppstår i anledning av detta DPA ska slutligt avgöras i enlighet med den tvistelösningsmekanism som anges i Tjänsteavtalet.

- 15.2. Språket för förfarandet ska vara det språk som tillämpas på Tjänsteavtalet.
- 15.3. Tillämplig lag för tvisten ska vara den lag som tillämpas på Tjänsteavtalet.

BEHANDLING

1. BESKRIVNING AV BEHANDLINGEN

1.1. Föremålet för behandling:

Biträdet ska tillhandahålla en molnbaserad tjänst för beslutsstöd och verksamhetsstyrning, samt tilläggstjänster.

1.2. Ändamål med behandling:

Ansvarigs ändamål med behandlingen är beslutstöd och verksamhetsstyrning inom ramen för budgetering och uppföljning.

1.3. Behandlingens art:

Biträdet kommer att utföra datalagring, analys, strukturering, import och export av personuppgifter.

1.4. Behandlingens varaktighet:

Behandlingen kommer ske löpande under Tjänsteavtalets giltighet och upp till sextio (60) dagar därefter.

1.5. Kategorier av registrerade och typer av personuppgifter:

Kategori av registrerade	Typ av personuppgifter
Anställda och konsulter registrerade som användare av kund	Namn, e-postadress, personnummer (om Bank-ID-inloggning används), telefonnummer
Anställda som registrerats i personalbudgetmodul (tillägg)	Namn, födelseår, titel, lön, semesterrätt, pensionspremie, förmåner, tjänstgöringsgrad
Kunder (privatpersoner)	Namn, personnummer (om det används som organisationsnummer i källsystemet)
Leverantörer (privatpersoner)	Namn, personnummer (om det används som organisationsnummer i källsystemet)

Vissa av ovanstående personuppgifter avslöjar:

- ras eller etniskt ursprung politisk åsikt hälsa
 sexualliv / sexuell läggning genetisk uppgift medlemskap i fackförening
 religiös / filosofisk övertygelse biometrisk uppgift för att entydigt identifiera person

UNDERBITRÄDEN

Ansvarig godkänner att Bitrådet använder sig av följande Underbiträden (se tabell nedan).

Underbiträde (org.namn)	Org. Nr.	Etableringsland	Behandlingstjänst Underbitrådet tillhandahåller:
Microsoft Ireland Operations Ltd.	-	Irland	Infrastruktur, databaser och utvecklingsmiljö
Thrivesoft Technologies Pvt.Ltd.	-	Indien	Mjukvaruutveckling
Twilio Sendgrid	-	USA	E-posttjänst
Zendesk	-	USA	Supportsystem
Upsales Nordic AB	556641-2507	Sverige	CRM-system
GoClimate Sweden AB	559130-6583	Sverige	Hållbarhetsanalys
Lundatech AB	559101-8600	Sverige	ERP-integrationstjänster

För detaljer kring hantering av personuppgifter utanför EU/EES hänvisas till separat bilaga 'Hantering av Personuppgifter utanför EU/EES'

KUNDBOLAG

Biträdet kommer att behandla personuppgifter för de kundbolagen som kunden registrerat i tjänsten.