Ordning och reda i molnet

Bilaga 1

Personuppgiftsbiträdesavtal

2019-03-28

Online Partner AB (härefter benämnd "Online Partner" eller "Personuppgiftsbiträdet"), och
Kunden (härefter benämnd "Kunden" eller den "Personuppgiftsansvarige")
(benämns härefter gemensamt som "Parterna")

Parterna har ingått detta personuppgiftsbiträdesavtal ("Avtalet").

1. Bakgrund

1.1 Parterna har tidigare – eller i samband med detta Avtal – ingått avtal avseende tjänster som Online Partner emellanåt utför (härefter benämnt "Tjänsteavtalet"), till vilken Online Partners Allmänna villkor [för tjänster och mjukvaror] är gällande.

1.2 Inom åtagandena som följer av Tjänsteavtalet kan Online Partner komma att behandla personuppgifter samt annan information åt Kundens vägnar.

1.3 Med anledning av detta ingår Parterna detta Avtal för att reglera förutsättningarna för Online Partners behandling av personuppgifter vid utförande av tjänsterna som regleras i Tjänsteavtalet (härefter benämnt "Tjänsterna"). Detta Avtal gäller för samtliga mellan Parterna tecknade avtal där Online Partner är Personuppgiftsbiträde till Kunden och Avtalet gäller så länge Online Partner behandlar personuppgifter för Kundens räkning.

2. Definitioner

2.1 De definitioner som anges i artikel 4 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ("Dataskyddsförordningen") ska äga tillämpning på detta Avtal.

2.2 I övrigt ska nedan uppräknade begrepp ha nedanstående innebörd:
"Dataskyddslagstiftning" avser Dataskyddsförordningen jämte tillhörande europeiska och nationella genomförandeförfattningar, samt instruktioner och bindande beslut från EU:s dataskyddsmyndigheter.

”Underbiträde” avser sådant personuppgiftsbiträde (underleverantör) som anlitats av Personuppgiftsbiträdet och som behandlar personuppgifter för den Personuppgiftsansvariges räkning.

3. Avtalets omfattning

3.1 Personuppgiftsbiträdet tillhandahåller tjänster som avtalas om med den Personuppgiftsansvarige från tid till annan. Personuppgiftsbiträdets huvudsakliga verksamhetsställe är i Sverige.

3.2 Tjänsten innefattar lagring och överföring av användaruppgifter och innehåll som tillhandahålls av användarna av tjänsten. Dessa uppgifter kan direkt eller indirekt identifiera en fysisk person.
3.3 Personuppgiftsbiträdet kommer endast att behandla personuppgifter som tillhandahålls genom den Personuppgiftsansvarige för att kunna utföra åtaganden som följer av Tjänsteavtalet.

3.4 De personuppgifter som kan komma att behandlas av Personuppgiftsbiträdet åt den Personuppgiftsansvariges vägnar ska raderas permanent och automatiskt när Tjänsteavtalet upphör att gälla (såvida inte lagring av personuppgifterna krävs enligt nationell lagstiftning eller unionsrätten).

3.5 Parterna är eniga om att behandlingen, de kategorier av personuppgifter som behandlingen gäller, de registrerade eller behandlingens syfte närsomhelst genom en överenskommelse kan förtydligas avseende specifikation och/eller utvidgas avseende omfattning. Sådana ändringar ska göras skriftliga för att vara giltiga så snart som det är möjligt efter att de har blivit kända. Villkoren i detta avtal ska tillämpas på sådana ändringar, om inte parterna kommer överens om annat.

4. Personuppgiftbiträdets ansvar/skyldigheter

4.1 Den Personuppgiftsansvarige ska ha fullständig befogenhet över personuppgifterna.

4.2 Personuppgiftsbiträdet förbinder sig att:

a) endast behandla personuppgifter som omfattas av den Personuppgiftsansvariges dokumenterade instruktioner (”Instruktioner”), inbegripet överföringar av personuppgifter till ett tredjeland eller en internationell organisation, för de syften som anges i Tjänsteavtalet och är i enlighet med detta avtal och gällande lagstiftning på området,

b) genomföra de säkerhetsåtgärder som anges i Avtalet,

c) inte göra anspråk på några rättigheter till personuppgifterna,

d) inte använda personuppgifterna för något annat syfte än för utförandet av de förpliktelser som följer av detta Avtal, Tjänsteavtalet eller för felsökning i Personuppgiftbiträdets system, samt

e) inte behandla personuppgifter för sitt egna syfte utan föregående skriftligt intyg från den Personuppgiftsansvarige.

4.3 Om Personuppgiftsbiträdet anser att någon instruktion från den Personuppgiftsansvarige står i strid med Dataskyddsförordningen eller annan dataskyddslagstiftning, äger Personuppgiftbiträdet

rätt att avvakta utförandet av instruktionen tills lagenligheten har bekräftats av behörig person utsedd av den Personuppgiftsansvarige eller tills instruktionen har skrivits om.

4.4 Personuppgiftsbiträdet ska bistå den Personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, med beaktande av behandlingens art och den information som är tillgänglig för Personuppgiftsbiträdet, så att den Personuppgiftsansvarige ska kunna fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III i Dataskyddsförordningen.

4.5 Personuppgiftsbiträdet ska bistå den Personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32-36 i Dataskyddsförordningen fullgörs, med beaktande av typen av behandling och information som Personuppgiftsbiträdet har att tillgå.

5. Anmälningsskyldighet för Personuppgiftsbiträdet

5.1 Personuppgiftsbiträdet ska omedelbart anmäla till den Personuppgiftsansvarige om Personuppgiftsbiträdet får kännedom om att någon obehörig åtkomst till personuppgifter och/eller oavsiktlig eller avsiktlig utlämnande av personuppgifter till tredje part har skett.

5.2 Personuppgiftsbiträdet ska omedelbart anmäla till den Personuppgiftsansvarige om varje väsentlig överträdelse av gällande dataskyddslagstiftning som den får kännedom om som har koppling till detta Avtal.

5.3 Om Personuppgiftsbiträdet anser att en instruktion från den Personuppgiftsansvarige strider mot Dataskyddslagstiftningen ska den omedelbart anmäla detta till den Personuppgiftsansvarige.

6. Personuppgiftsansvariges ansvar

6.1 Den Personuppgiftsansvarige ska tillhandahålla Personuppgiftsbiträdet instruktioner för behandlingen av personuppgifter. Instruktionerna måste vara skriftliga (antingen fysiska eller elektroniska).

6.2 I instruktionerna ska bl.a. framgå föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade.

6.3 Den Personuppgiftsansvarige har det enskilda ansvaret att informera den registrerade om behandlingen av personuppgifter som utförs av Personuppgiftsbiträdet och att säkerställa att den registrerade har kännedom om sina rättigheter enligt gällande lagstiftning.

6.4 Den Personuppgiftsansvarige är skyldig att utföra sina förpliktelser enligt gällande Dataskyddslagstiftning. Inget i detta Avtal ska tolkas som en överlåtelse av den Personuppgiftsansvariges ansvar, som följer av gällande dataskyddslagstiftning, till Personuppgiftsbiträdet.

7. Överföring till tredje land

7.1 I syfte att tillhandahålla de avtalade Tjänsterna har Personuppgiftsbiträdets servrar placerade i Finland och i ytterligare cirka 5 länder (både inom EU och i tredjeland).

7.2 Den Personuppgiftsansvarige är medveten om och accepterar att servrar som är placerade i tredjeland är omfattade av avtal för samlokalisering (co-location agreement) med samarbetspartners. Dessa parter har inte rätt att få åtkomst till personuppgifter på servrarna och begränsad rätt till materiell åtkomst till servrarna. När personuppgifter överförs mellan Personuppgiftsbiträdets servrar är personuppgifterna krypterade. Servrarna sköts av Personuppgiftsbiträdets underbiträde, direkt eller på distans.

7.3 Den Personuppgiftsansvarige åtar sig att tillse att de registrerade har fått information eller blir informerad om att hans eller hennes personuppgifter kan överföras till ett land utanför EU/EES innan Personuppgiftbiträdet påbörjar behandlingen av personuppgifterna.

7.4 Om överföringar av personuppgifter till ett tredjeland eller en internationell organisation krävs enligt unionsrätten eller en nationell rätt får Personuppgiftsbiträdet genomföra sådan behandling. I så fall ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida inte sådan information är förbjuden med hänvisning till ett viktigt allmänintresse enligt dataskyddslagstiftningen.

8. Revision

8.1 Personuppgiftbiträdet ska ge den Personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som följer av artikel 28 i Dataskyddsförordningen har fullgjorts och på den Personuppgiftsansvariges begäran tillåta granskning, inklusive inspektioner, för att se om Personuppgiftbiträdet uppfyller sina skyldigheter enligt dataskyddslagstiftningen och detta avtal. Personuppgiftbiträdet ska medverka och bistå den Personuppgiftsansvarige och den som utför granskningen så mycket som rimligen kan krävas i genomförandet av granskningen. Den Personuppgiftsansvarige är medveten om att det av säkerhetsskäl finns begränsningar och regleringar gällande vem som kan få tillträde till lokalerna där servrarna finns.

8.2 Parterna ska gemensamt komma överens om vilken organisation som ska utföra ovan granskning.

8.3 Den Personuppgiftsansvarige ska betala alla kostnader, avgifter och utgifter för den organisation som genomför granskningen.

9. Underbiträde

9.1 Den Personuppgiftsansvarige erkänner och samtycker till att, (a) bolag i samma koncern som Personuppgiftsbiträdet kan anlitas som Underbiträde; och (b) att Personuppgiftsbiträdet och bolag i samma koncern som Personuppgiftsbiträdet i sin tur kan ingå avtal med Underbiträden för att uppfylla leveransen av Tjänsterna. Personuppgiftsbiträdet har eller ska ingå skriftliga avtal med varje enskilt Underbiträde. Underbiträdet ska därvid åläggas att iaktta samma skyldigheter i fråga om dataskydd som fastställs i detta avtal. Underbiträdet ska i sådant personuppgiftsbiträdesavtal ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i Dataskyddsförordningen

9.2 Personuppgiftsbiträdet ska vid varje tid kunna tillhandahålla den Personuppgiftsansvarige en lista med fullständig, korrekt och uppdaterad information om samtliga Underbiträden. Denna lista ska inkludera Underbiträdens kontaktinformation och land det som det är placerat i. Om Personuppgiftsbiträdet ska anlita ett nytt Underbiträde ska den Personuppgiftsansvarige meddelas detta skriftligen innan det nya Underbiträdet får behörighet att behandla personuppgifter när den utför Tjänsterna.

9.3 Den Personuppgiftsansvarige kan invända mot användandet av ett nytt Underbiträde genom att skriftligen anmäla detta till Personuppgiftsbiträdet inom tio (10) arbetsdagar efter mottagandet av Personuppgiftsbiträdets meddelande. Om den Personuppgiftsansvarige har invänt mot ett nytt Underbiträde, ska Personuppgiftsbiträdet genom rimlig ansträngning tillgängliggöra en ändring av tjänsten för den Personuppgiftsansvarige eller rekommendera en kommersiellt rimlig ändring av användandet av Tjänsten för att undvika att det nya Underbiträdet behandlar personuppgifter, utan att det blir en oskälig belastning för den Personuppgiftsansvarige. Om Personuppgiftsbiträdet inte lyckas genomföra en sådan förändring inom en rimlig tid, som inte ska vara mer än trettio (30) dagar, kan den Personuppgiftsansvarige säga upp Tjänsteavtalet, genom ett skriftligt meddelande, avseende de tjänster som inte kan tillhandahållas av Personuppgiftsbiträdet utan användandet av det nya Underbiträdet.

9.4 För att den Personuppgiftsansvarige ska kunna invända mot ett Underbiträde enligt ovan ska den Personuppgiftsansvarige ha en befogad anledning till detta. Med befogad anledning avses omständigheter på det nya Underbiträdets sida som i betydande utsträckning påverkar, eller sannolikt riskerar att påverka, skyddet för den registrerades personliga integritet, såsom att det nya Underbiträdet inte uppfyller kraven i Dataskyddslagstiftningen.

9.5 Om Underbiträdet inte uppfyller de skyldigheter i fråga om behandling av personuppgifter som framgår av detta avtal, ska Personuppgiftsbiträdet förbli fullt ansvarig gentemot den Personuppgiftsansvarige för Underbiträdets underlåtelse att uppfylla skyldigheterna.

10. Säkerhet och sekretess

10.1 Personuppgiftsbiträdet har gett tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på sådant sätt att behandlingen av personuppgifter uppfyller kraven i dataskyddslagstiftningen samt säkerställer att den registrerades rättigheter skyddas.

10.2 Personuppgiftsbiträdet har implementerat och kommer upprätthålla åtgärder för att vidmakthålla säkerheten för Tjänsterna som de beskrivs i Tillägg A.

10.3 Parterna är överens om att de säkerhetsåtgärder som återges i Tillägg A till detta avtal är ändamålsenliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är adekvat gentemot potentiella risker, som skydd för personuppgifter gentemot oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. I beaktande härav tas den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

10.4 Personuppgiftsbiträdet förbinder sig att inte till tredje man lämna ut eller på annat sätt röja information om personuppgifter som omfattas av detta avtal. Sekretessåtagandet gäller även efter att detta avtal i övrigt upphört att gälla.

10.5 Om Personuppgiftsbiträdet är skyldig att röja personuppgifter till en tredje part eller myndighet för att uppfylla ett rättsligt krav eller svara på föreläggande eller beslut från relevant myndighet, ska Personuppgiftsbiträdet, såvida det inte är förbjudet enligt lag, utan opåkallat dröjsmål efter att skyldigheten att röja personuppgiften blivit känd, skriftligen underrätta den Personuppgiftsansvarige om det rättsliga kravet och vilken typ av röjande som är aktuellt. Personuppgiftsbiträdet ska, om det inte är förbjudet enligt lag, vänta på vidare instruktioner från den Personuppgiftsansvarige gällande röjandet.

10.6 Personuppgiftsbiträdet ska säkerställa att samtliga personer som givits behörighet att behandla personuppgifterna har ingått särskild sekretessförbindelse eller upplysts om att särskild tystnadsplikt föreligger enligt avtal eller gällande rätt.

10.7 Personuppgiftsbiträdet ska vidta alla åtgärder avseende säkerhet som krävs enligt artikel 32 i Dataskyddsförordningen.

11.Övrigt

11.1 Bestämmelserna i Online Partner's allmänna villkor gällande avtalstid och upphörande, ansvar, tillämplig lag och behörig domstol, tillämpas på detta Avtal.

11.2 Tillägg och ändringar på detta Avtal måste vara skriftliga för att vara gällande. Med undantag för eventuella ändringar av detta Avtal, kommer detta Avtal att vara gällande. Om det är en konflikt mellan detta Avtal och Tjänsteavtalet, har detta Avtal företräde.

Tillägg A: Tekniska och organisatoriska åtgärder

Online Partner kommer att genomföra som minst nedanstående listade åtgärder, eller likvärdiga, under Avtalets giltighetstid:

<u>Kontroll av åtkomst till lokalerna</u>
Personuppgiftsbiträdet kommer genomföra lämpliga åtgärder i syfte att förhindra att obehöriga personer får tillgång till utrustning som behandlar personuppgifter genom att införa eller upprätthålla följande:

- - Åtkomstkontroll och tillstånd för anställda och tredje parter
- - Skydd och restriktioner för in och utgångar (begränsade nyckelkort och/eller passerkort)
- - Skydd av relevanta lokaler (alarm och/eller säkerhetsvakter)

<u>Kontroll av åtkomst till personuppgifterna och användarkontroll</u>

- Personuppgiftsbiträdet är skyldig att tillse att alla anställda och/eller andra personer med åtkomst till personuppgifter endast har det till den grad som är nödvändig för att kunna tillhandahålla Tjänsterna i Tjänsteavtalet, genom:
- Samtliga personal använder förstärkt autentisering, 2FA för inloggning
- Krav på användarbehörighet och strikt åtkomstkontroll
- Sekretessförpliktelser
- Anpassad åtkomstbehörighet
- Kontrollerad förstöring och förflyttning av information på datalagringsmedier
- Loggbok av händelser och aktiviteter (uppföljning av försök av obehöriga att ta sig in eller få åtkomst)

- Utfärdande och säkringsförfarande av identifieringskoder
- Användande av kryptering där Personuppgiftsbiträdet bedömer det lämpligt
- Automatisk utloggning av användar-ID:n som inte har använts på en väsentlig tid
- Försäkran om att kunder endast har åtkomst till sina egna uppgifter

Överföring av uppgifter

- Personuppgiftsbiträdet kommer att skydda att personuppgifter som överförs och/eller behandlas enligt Tjänsteavtalet och Instruktioner, genom:
- Riktlinjer som styr framställningen av säkerhetskopior
- Dokumentation av överflyttnings-, hämtnings- och överföringsprogram
- Attestinstruktioner
- Kryptering av externa överföringar online
- Radering av information innan byte av datalagringsmedia
- Trafiken mellan användaren och tjänsten är med krypterad SSL certifikat
- Personuppgifter överförs inte till tredje part utan den Personuppgiftsansvariges skriftliga medgivande, om det inte är ett rättsligt krav

Organisatorisk kontroll

- Personuppgiftsbiträdet kommer att upprätthålla sin inre organisation på ett sätt som tillgodoser krav enligt dataskyddslagstiftning, genom att:
- Bindande interna riktlinjer för de anställda och/eller konsulter gällande säkerhet och behandling av personuppgifter, och/eller instruktioner
- Intern krisplan för återställande och skyddande av personuppgifter
- Begränsad behörighet att få åtkomst till personuppgifter endast till den nivå som är nödvändig
- Ingen kundinformation kommer att kopieras på externa enheter (USB-minne, CD etc.) utan nödvändiga säkerhetsåtgärder, som exempelvis kryptering eller lösenordsskydd.