Personuppgiftsbiträdesavtal

Personuppgiftsansvarig: Kund inom EU ("**personuppgiftsansvarig**")

och

	Personuppgiftsbiträde:
Företag:	One.com Group AB
Momsreg.nr.	559205-2400
Stad	Malmö
Registrerad i land:	Sverige

(**Personuppgiftsbiträdet**)
(separat kallad "**part**" och kollektivt "**parterna**")

har ingått detta:

PERSONUPPGIFTSBITRÄDESAVTAL

("**Avtalet**")
avseende personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning.

1. De behandlade personuppgifterna

1.1 Detta avtal har ingåtts i samband med att personuppgiftsansvariga använder personuppgiftsbiträdets tjänster som en del av prenumerationen och tilläggstjänster som beskrivs i "One.com villkor" (”**huvudavtalet”**).

1.2 Personuppgiftsbiträdet behandlar de typer av personuppgifter för den personuppgiftsansvariges räkning i förhållande till de relevanta registrerade personerna enligt **förteckning 1**. Personuppgifterna avser de registrerade som anges i **förteckning 1**.

1.3 Personuppgiftsbiträdet kan inleda behandling av personuppgifter för den personuppgiftsansvariges räkning efter det att avtalet har trätt i kraft. Behandlingen har den varaktighet som anges i anvisningarna i **förteckning 1** i avtalet.

1.4 Avtalet och huvudavtalet är beroende av varandra och kan inte sägas upp separat. Avtalet kan dock ersättas med ett annat giltigt personuppgiftsbiträdesavtal utan att huvudavtalet sägs upp.

2. Syfte

2.1 Personuppgiftsbiträdet får endast behandla personuppgifter för ändamål som är nödvändiga för att fullgöra personuppgiftsbiträdets skyldigheter och därigenom tillhandahålla de tjänster som anges i huvudavtalet.

3. Den personuppgiftsansvariges skyldigheter

3.1 Den personuppgiftsansvarige garanterar att personuppgifterna behandlas för legitima och objektiva ändamål och att personuppgiftsbiträdet inte behandlar fler personuppgifter än vad som krävs för att uppfylla sådana ändamål.

3.2 Den personuppgiftsansvarige ansvarar för att det finns en giltig rättslig grund för behandlingen vid tidpunkten för överföringen av personuppgifterna till personuppgiftsbiträdet.

På personuppgiftsbiträdets begäran åtar sig den personuppgiftsansvarige skriftligen att redogöra för och/eller tillhandahålla dokumentation av grunden för behandlingen.

3.3 Dessutom garanterar den personuppgiftsansvarige att de registrerade som personuppgifterna avser har fått tillräcklig information om behandlingen av deras personuppgifter.

4. Personuppgiftsbiträdets skyldigheter

4.1 All behandling av personuppgiftsbiträdet av de personuppgifter som tillhandahålls av den personuppgiftsansvarige måste ske i enlighet med instruktioner som utarbetats av den personuppgiftsansvarige, och personuppgiftsbiträdet är dessutom skyldigt att följa all dataskyddslagstiftning som gäller från tid till annan. Om unionsrätten eller unionsrätten i en EU-medlemsstat som personuppgiftsbiträdet är föremål för föreskriver att personuppgiftsbiträdet är skyldigt att behandla de personuppgifter som anges i **förteckning 1**, måste personuppgiftsbiträdet informera den personuppgiftsansvarige om detta rättsliga krav innan behandlingen. Detta gäller dock inte om denna lagstiftning förbjuder sådan information av viktiga skäl av allmänt intresse. Personuppgiftsbiträdet måste omedelbart informera den personuppgiftsansvarige om en instruktion enligt personuppgiftsbiträdet bryter mot EU:s allmänna dataskyddsförordning eller dataskyddsbestämmelserna i en EU-medlemsstat.

4.2 Personuppgiftsbiträdet måste vidta alla nödvändiga tekniska och organisatoriska säkerhetsåtgärder, inklusive eventuella ytterligare åtgärder, som krävs för att säkerställa att personuppgifterna inte oavsiktligt eller olagligt förstörs, förloras eller försämras eller förs till kännedom om obehörig tredje part, missbrukas eller på annat sätt behandlas på ett sätt som strider mot den dataskyddslagstiftning som är i kraft när som helst. Dessa åtgärder beskrivs mer i detalj i **förteckning 2**.

4.3 Personuppgiftsbiträdet måste se till att anställda som är behöriga att behandla personuppgifterna har åtagit sig sekretess eller omfattas av lämplig lagstadgad tystnadsplikt.

4.4 Om den personuppgiftsansvarige begär det måste personuppgiftsbiträdet ange och/eller dokumentera att personuppgiftsbiträdet uppfyller kraven i tillämplig dataskyddslagstiftning, inklusive dokumentation om personuppgiftsbiträdets dataflöden samt förfaranden/policyer för behandling av personuppgifter.

4.5 Med hänsyn till behandlingens art måste personuppgiftsbiträdet i möjligaste mån bistå den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder för att fullgöra den personuppgiftsansvariges skyldighet att besvara begäran om utövandet av den registrerades rättigheter i enlighet med kapitel 3 i den allmänna dataskyddsförordningen.

4.6 Personuppgiftsbiträdet eller ett annat personuppgiftsbiträde (personuppgiftsbiträde som underleverantör) måste skicka förfrågningar och invändningar från registrerade till den personuppgiftsansvarige för den personuppgiftsansvariges fortsatta behandling av dessa, såvida inte personuppgiftsbiträdet har rätt att hantera en sådan begäran själv. På begäran av den personuppgiftsansvarige måste personuppgiftsbiträdet hjälpa den personuppgiftsansvarige att besvara sådana förfrågningar och/eller invändningar.

4.7 Om personuppgiftsbiträdet behandlar personuppgifter i ett annat EU-land måste personuppgiftsbiträdet följa lagstiftningen om säkerhetsåtgärder i den medlemsstaten.

4.8 Personuppgiftsbiträdet måste meddela den personuppgiftsansvarige om verksamheten avbryts, misstanke om att dataskyddsregler har överträtts eller andra oegentligheter i samband med behandlingen av personuppgifterna förekommer. Personuppgiftsbiträdets tidsfrist för att meddela den personuppgiftsansvarige om en säkerhetsöverträdelse är 24 timmar från det att personuppgiftsbiträdet får kännedom om en säkerhetsöverträdelse. På begäran av den personuppgiftsansvarige måste personuppgiftsbiträdet bistå den personuppgiftsansvarige i

samband med att klargöra omfattningen av säkerhetsöverträdelsen, inklusive förberedelse av eventuella meddelanden till relevanta dataskyddsbyråer och/eller registrerade.

4.9 Personuppgiftsbiträdet måste göra all information som är nödvändig för den personuppgiftsansvarige tillgänglig för att visa att artikel 28 i den allmänna dataskyddsförordningen och avtalet följs. I detta sammanhang möjliggör och bidrar personuppgiftsbiträdet till revisioner, inklusive inspektioner, som utförs av den personuppgiftsansvarige eller annan revisor som bemyndigats av den personuppgiftsansvarige.

4.10 Utöver ovanstående måste personuppgiftsbiträdet hjälpa den personuppgiftsansvarige att säkerställa att den personuppgiftsansvariges skyldigheter enligt artikel 32–36 i dataskyddsförordningen uppfylls. Detta stöd kommer att ta hänsyn till behandlingens art och den information som personuppgiftsbiträdet har tillgång till.

5. Överföring av uppgifter till underleverantör eller tredje part

5.1 Personuppgiftsbiträdet måste uppfylla villkoren i artikel 28.2 och 4 i den allmänna dataskyddsförordningen för att anlita ett annat personuppgiftsbiträde (underleverantör). Detta innebär att personuppgiftsbiträdet inte får involvera ett annat personuppgiftsbiträde (underleverantör) till avtalets fullgörande utan föregående specifikt eller allmänt skriftligt godkännande från den personuppgiftsansvarige.

5.2 Den personuppgiftsansvarige ger härmed personuppgiftsbiträdet en allmän fullmakt att ingå avtal med personuppgiftsbiträden. Personuppgiftsbiträdet måste meddela den personuppgiftsansvarige om eventuella ändringar som rör tillägg eller utbyte av underleverantörer senast 30 dagar före ett nytt personuppgiftsbiträde påbörjar behandling av personuppgifterna. Den personuppgiftsansvarige kan göra rimliga och relevanta invändningar mot sådana ändringar inom 14 dagar från mottagandet av anmälan. Om personuppgiftsbiträdet fortsätter att vilja använda en underleverantör som den personuppgiftsansvarige har invänt mot, har parterna rätt att säga upp avtalet, se klausul 7.

5.3 När den personuppgiftsansvarige har godkänt att personuppgiftsbiträdet kan använda en underleverantör måste personuppgiftsbiträdet ålägga personuppgiftsbiträdet som är underleverantör samma skyldigheter som anges i avtalet. Detta verkställs genom ett avtal eller en annan rättsakt enligt EU-lagstiftningen eller en medlemsstats lagstiftning. Det måste t.ex. säkerställas att det finns tillräckliga garantier från personuppgiftsbiträdet som agerar underleverantör för att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i den allmänna dataskyddsförordningen (back-to-back"-villkoren).

5.4 Om underleverantören underlåter att uppfylla sina dataskyddsskyldigheter förblir personuppgiftsbiträdet fullt ansvarig gentemot den personuppgiftsansvarige för fullgörande av underleverantörens skyldigheter.

5.5 Utlämnande, överföring och intern användning av den personuppgiftsansvariges personuppgifter till tredje land eller internationella organisationer får endast ske i enlighet med dokumenterade instruktioner från den personuppgiftsansvarige – såvida det inte föreskrivs i EU-lagstiftningen eller lagstiftningen i en medlemsstat där personuppgiftsbiträdet är föremål för detta. Om så är fallet måste personuppgiftsbiträdet meddela den personuppgiftsansvarige om detta rättsliga krav före behandlingen, såvida inte lagen förbjuder sådan anmälan av viktiga skäl av allmänt intresse.

5.6 Om de personuppgifter som anges i **förteckning 1** överförs till personuppgiftsbiträden utanför EU/EES måste det i nämnda avtal anges att den dataskyddslagstiftning som gäller i den personuppgiftsansvariges land gäller för personuppgiftsbiträden. Om den mottagande underleverantören är etablerad inom EU/EES ska det vidare anges i nämnda databehandlaravtal att det mottagande EU-landets specifika lagstadgade krav på

personuppgiftsbiträden, t.ex. avseende krav på anmälan till nationella myndigheter ska efterlevas.

5.7 Personuppgiftsbiträdet är skyldigt att ingå skriftliga personuppgiftsbiträdesavtal med underleverantörer inom EU/EES. När det gäller personuppgiftsbiträden utanför EU/EES måste personuppgiftsbiträdet säkerställa tillräckliga överföringsmekanismer och ingå ett avtal om underleverantör genom att ingå standardavtal i enlighet med EU-kommissionens standardavtalsklausuler ("**Standardavtal**") baserade på 2021/914/EU av den 4 juni 2021.

5.8 När detta avtal undertecknas anlitar personuppgiftsbiträdet underleverantörerna som är listade i **förteckning 3**.

6. Ansvar

6.1 Parternas ansvar regleras av huvudavtalet.

6.2 Parternas skadeståndsansvar enligt detta avtal regleras av huvudavtalet.

7. Giltighetsdatum och uppsägning

7.1 Detta avtal träder i kraft samtidigt som huvudavtalet. Vid uppsägning av huvudavtalet kommer detta avtal också att upphöra. Personuppgiftsbiträdet omfattas dock av de skyldigheter som anges i detta avtal så länge personuppgiftsbiträdet behandlar personuppgifter för den personuppgiftsansvariges räkning.

7.2 Efter avslutad behandling är personuppgiftsbiträdet skyldigt att på begäran av den personuppgiftsansvarige radera eller returnera alla personuppgifter till den personuppgiftsansvarige samt att radera befintliga kopior, såvida inte lagring av personuppgifterna föreskrivs i EU-lagstiftningen eller nationell lagstiftning.

8. Reglerande lag och jurisdiktion

8.1 Varje fordran eller tvist som uppstår till följd av eller i samband med detta avtal måste avgöras av en behörig domstol i första instans i samma jurisdiktion och med samma rättsval som anges i huvudavtalet.

9. Underskrifter

För den personuppgiftsansvariges räkning:

_____

[Namn] [Titel]

För personuppgiftsbiträdets räkning:

Ronni Engelhardt VD

Förteckning 1
Kategorier av registrerade, typer av personuppgifter och instruktioner

1. Kategorier av registrerade:

- Personuppgiftsbiträdet kommer att behandla kontaktinformation om personuppgiftsansvarigs faktiska, potentiella eller tidigare kunder och eller medlemmar, anställda, leverantörer, affärs- och samarbetspartners och dotterbolag.
- Personuppgiftsbiträdet upplåter sitt system till den personuppgiftsansvarige som en host-tjänst, och det är inte möjligt för personuppgiftsbiträdet att bestämma alla kategorier av registrerade. Om den personuppgiftsansvarige lagrar uppgifter om ytterligare kategorier av registrerade hos personuppgiftsbiträdet är det den personuppgiftsansvariges skyldighet att registrera denna information.

2. Typer av personuppgifter:

- Kontakt- och identifieringsinformation inklusive e-postadress
- IP-adresser
- Domännamn
- Användarnamn
- Information om medlemskap
- Analys- och användningsdata
- Orderhistorik och information
- Kontrakt
- Kommunikation
- Stöd
- Bilder
- Ytterligare typer av personuppgifter kan förekomma

3. Instruktioner

Tjänster

Personuppgiftsbiträdet kan behandla personuppgifter om de registrerade i syfte att leverera, utveckla, hantera, administrera och hantera tjänsterna i huvudavtalet, inklusive säkerställa stabilitet och drifttid för våra servrar och uppfylla rättsliga krav.

Lagringstid

De personuppgifter som lagras/finns i våra system raderas eller anonymiseras inom rimlig tid efter det att den personuppgiftsansvarige helt har sagt upp huvudavtalet. Undantag är uppgifter där det finns ett rättsligt krav på att personuppgiftsbiträdet ska spara dem längre. Den här typen av data tas vanligtvis bort inom åtta veckor men kan tas bort tidigare. Andra typer av data som lagras i loggar etc. kommer att raderas efter en rimlig tid, vanligtvis inom 8 veckor, varefter de raderas hos personuppgiftsbiträdet.

Bearbetningens placering

Behandling av personuppgifter som omfattas av Avtalet får inte ske utan den personuppgiftsansvariges skriftliga medgivande i förväg på andra platser än personuppgiftsbiträdets adress och underleverantörens adress som anges i förteckning 3.

Inspektion av personuppgiftsbiträde

Personuppgiftsbiträdet måste en gång per år på egen bekostnad erhålla en revisions-/inspektionsrapport från en tredje part om personuppgiftsbiträdets efterlevnad av detta avtal och förteckningar. Rapporten eller annat revisionsformat ska vidarebefordras till den personuppgiftsansvarige eller offentliggöras på den personuppgiftsansvariges webbplats så snart som möjligt när den är förberedd.

Förteckning 2
Säkerhetsåtgärder

Domän	Praxis
Organisation av informationssäkerhet	**Säkerhetsansvarig**. One.com har utsett en säkerhetsansvarig med ansvar för samordning och övervakning av säkerhetsreglerna och säkerhetsrutinerna. En styrning bestående av individer på c-nivå bistår och vägleder säkerhetsansvarig.

Domän	Praxis
	Säkerhetsroller och ansvar. One.com-personal med tillgång till kunddata omfattas av sekretesskrav, vilket betonas vid anställning och ökar medvetenheten. **Riskhantering**. One.com utför kontinuerlig riskbedömning, en del av riskhanteringen, före behandling av kunduppgifter eller lansering av tjänster. Riskhanteringen möjliggör fokus på relevanta hot genom att prioritera, strukturera och minska risker utöver vad som anses vara acceptabelt. Säkerhetskopiering implementeras. Personuppgiftsbiträdet ska behålla sina säkerhetsdokument i enlighet med lagringskraven efter att de inte längre har någon verkan.
Hantering av tillgångar	**Inventering av tillgångar.** Personuppgiftsbiträdet upprätthåller en inventering av alla medier där kunduppgifter lagras. Tillgång till inventeringar av sådana medier är begränsad till personuppgiftsbiträdets personal som skriftligen har behörighet att ha sådan tillgång. **Hantering av tillgångar** -One.com klassificerar kunduppgifter för att hjälpa till att identifiera dem och för att möjliggöra att tillträdet till den begränsas på lämpligt sätt. - Personuppgiftsbiträdets personal måste erhålla auktorisering för behandling av uppgifter innan kunddata lagras på bärbara enheter, innan de får fjärråtkomst till kunddata eller får bearbeta kunddata utanför personuppgiftsbiträdets anläggningar.
Personalsäkerhet	**Säkerhetsutbildning**. One.com informerar sin personal om relevanta säkerhetsrutiner och deras respektive roller, samt tar itu med nya hot etc. där de anställda spelar en viktig roll.
Fysisk och miljömässig säkerhet	**Fysisk åtkomst till faciliteter**. One.com begränsar tillgången till anläggningar där informationssystem som behandlar kunddata finns, till identifierade behöriga personer. **Fysisk åtkomst till komponenter**. One.com säkerställer tillräckliga begränsningar av media som innehåller kunddata. **Skydd mot störningar**. One.com använder en mängd olika branschstandardsystem för att skydda mot förlust av data på grund av strömavbrott, översvämning, brand eller störningar i ledningar. **Komponenthantering**. One.com använder branschstandardprocesser för att ta bort kunddata när de inte längre behövs.
Kommunikations- och driftledning	**Verksamhetspolicy**. One.com upprätthåller säkerhetsdokument som beskriver säkerhetsåtgärder och relevanta förfaranden och ansvar för den personal som har tillgång till kunddata. **Förfaranden för dataåterställning** -One.com lagrar kopior av kunddata och dataåterställningsförfaranden på en annan plats än där den primära datorutrustningen som behandlar kunddata finns. -One.com har särskilda rutiner för tillgång till kopior av kunddata.

Domän	Praxis
	Skadlig programvara. One.com har kontroller mot skadlig kod för att undvika att skadlig programvara får obehörig åtkomst till kunddata, inklusive skadlig programvara som kommer från offentliga nätverk. Antivirus har också implementerats. **Händelseloggning**. One.com loggar eller gör det möjligt för kunder att logga, komma åt och använda informationssystem som innehåller kunddata, registrera åtkomst-ID, tid, auktorisering beviljad eller nekad och relevant aktivitet. **Kryptering**. Kommunikationen via internet mellan system som hanterar personuppgifter krypteras.
Åtkomstkontroll	**Åtkomstprincip**. One.com upprätthåller ett register över säkerhetsprivilegier för personer som har tillgång till kunddata. **Åtkomstauktorisering** - One.com inaktiverar autentiseringsuppgifter som inte har använts under en tidsperiod som inte får överstiga sex månader. - One.com identifierar den personal som kan bevilja, ändra eller avbryta behörig åtkomst till data och resurser. - One.com säkerställer att om mer än en individ har tillgång till system som innehåller kunddata har individerna separata identifierare/inloggningar. **Lägsta behörighet** - One.com begränsar åtkomsten till kunddata till endast de individer som behöver sådan åtkomst för att utföra sin jobbfunktion. **Integritet och konfidentialitet** - One.com instruerar sin personal att inaktivera administrativa sessioner när de lämnar lokaler eller när datorer på annat sätt lämnas obevakade. - One.com lagrar lösenord på ett sätt som gör dem obegripliga medan de är i kraft. **Autentisering** - One.com använder branschstandardpraxis för att identifiera och autentisera användare som försöker komma åt informationssystem. - När autentiseringsmekanismer baseras på lösenord kräver databehandlaren att lösenorden förnyas regelbundet. - One.com säkerställer att avaktiverade eller utgångna identifierare inte beviljas andra personer. - One.com övervakar, eller gör det möjligt för kunder, att övervaka, upprepade försök att få tillgång till informationssystemet med ett ogiltigt lösenord. - One.com upprätthåller branschstandardprocedurer för att inaktivera lösenord som har skadats eller oavsiktligt avslöjats. - One.com använder branschstandard för lösenordsskydd, inklusive metoder som är utformade för att upprätthålla

Domän	Praxis
	lösenordens konfidentialitet och integritet när de tilldelas och distribueras och under lagring. **Nätverksdesign.** One.com har kontroller för att undvika att individer antar åtkomsträttigheter som de inte har tilldelats för att få tillgång till kunddata som de inte har behörighet att komma åt.
Hantering av incidenthantering av informationssäkerhet	**Incidentsvarsprocess** - One.com upprätthåller ett register över säkerhetsöverträdelser med en beskrivning av överträdelsen, tidsperioden, konsekvenserna av överträdelsen, reporterns namn och till vilken överträdelsen rapporterades och förfarandet för att återställa data. - För varje säkerhetsöverträdelse som är en säkerhetsincident kommer anmälan från One.com att göras utan onödigt dröjsmål och under alla omständigheter inom 72 timmar. - One.com spårar, eller gör det möjligt för kunden att spåra, utlämnande av kunddata, inklusive vilka uppgifter som har lämnats ut, till vem och vid vilken tidpunkt.
Hantering av kontinuitet i verksamheten	- One.com upprätthåller beredskaps- och beredskapsplaner för de anläggningar där databehandlares informationssystem som behandlar kunddata finns. - One.com har redundant lagring och procedurer för återställning av data är utformade för att försöka rekonstruera kunddata i sitt ursprungliga eller senast replikerade tillstånd från innan det förlorades eller förstördes.

Förteckning 3
Lista över underleverantörer

Leverantör	Plats	Funktion	Uppdaterad
Global Connect A/S	DK	Datacenter	20/2 2021
Interxion	DK	Datacenter	12/4 2021
Interxion	DK/UK/NL/FR/DE	PoP (Närvaropunkt)	12/4 2021
Equinix	SE	PoP (Närvaropunkt)	12/4 2021