Databehandleravtale
Datakontrollør: Kunde i EU ("**Datakontrolløren**") og

	Databehandleren:
Bedrift:	One.com Group AB
Reg. nr.	559205-2400
By:	Malmö
Registreringsland:	Sverige

("**Databehandleren**")
(separat kalt "**Part**" og kollektivt kalt "**Partene**")

har avtalt følgende:

DATABEHANDLERAVTALE

(«**Avtalen**»)
omfatter Databehandlerens behandling av personopplysninger på vegne av Datakontrolløren.

1. De behandlede personopplysningene

1.1 Denne avtalen er inngått i forbindelse med at datakontrollørene bruker databehandlerens tjenester som en del av et abonnement og tilleggstjenester som beskrevet i "One.coms vilkår" («**Hovedavtalen**»).

1.2 Databehandleren behandler personopplysninger på vegne av Datakontrolløren på grunnlag av relevante data som spesifisert i **Vedlegg 1**. Personopplysningene er knyttet til de subjektene som er oppført i **Vedlegg 1**.

1.3 Databehandler kan igangsette behandling av personopplysninger på vegne av Datakontrolløren når avtalen har tredd i kraft. Behandlingens varighet er i henhold til det som er spesifisert i instruksjonene i **Vedlegg 1** i avtalen.

1.4 Avtalen og Hovedavtalen er knyttet til hverandre og kan ikke sies opp hver for seg. Avtalen kan imidlertid erstattes med en annen gyldig Databehandleravtale uten at Hovedavtalen blir sagt opp.

2. Formål

2.1 Databehandleren skal kun behandle personopplysninger som er nødvendig for å oppfylle Databehandlerens forpliktelser, og derigjennom yte de tjenestene som fremgår av hovedavtalen.

3. Datakontrollørens forpliktelser

3.1 Datakontrolløren garanterer at personopplysningene behandles for lovlige og objektive formål, og at Databehandleren ikke behandler flere personopplysninger enn det som er nødvendig for å oppfylle slike formål.

3.2 Datakontrolløren er ansvarlig for å sørge for at det foreligger et gyldig rettsgrunnlag for behandling på det tidspunktet personopplysningene overføres til Databehandleren. På Databehandlers anmodning, forplikter Datakontrolløren seg til å redegjøre skriftlig for og/eller fremlegge dokumentasjon for behandlingsgrunnlaget.

3.3I tillegg garanterer Datakontrolløren at de datasubjektene som personopplysningene gjelder, har fått tilstrekkelig informasjon om at deres personopplysninger blir behandlet.

4. Databehandlerens forpliktelser

4.1 Databehandlerens behandling av personopplysninger gitt av Datakontrolløren, må være i samsvar med instrukser utarbeidet av Datakontrolløren, videre er Databehandleren til enhver tid forpliktet til å overholde gjeldende personvernlovgivning. Hvis EU-direktiv eller loven i et EU-medlemsland, som Databehandleren er underlagt, fastsetter at Databehandleren er pålagt å behandle personopplysningene oppført i **Vedlegg 1**, må Databehandleren informere Datakontrolløren om det juridiske kravet før behandlingen. Det gjelder imidlertid ikke dersom lovgivningen forbyr slik informasjon på grunn av viktige allmenninteresser. Databehandleren må umiddelbart informere Datakontrolløren dersom Databehandleren mener en instruks bryter med EUs personvernforordning eller datavernbestemmelsene i et EU-medlemsland

4.2 Databehandleren må sette i verk alle nødvendige tekniske og organisatoriske sikkerhetstiltak, inkludert eventuelle tilleggstiltak, som kreves for å sikre at personopplysningene ikke ved uhell eller på ulovlig vis ødelegges, går tapt eller forringes, eller sendes videre til en uautorisert tredjepart, misbrukes eller på annen måte behandles i strid med den til enhver tid gjeldende datavernlovgivningen. Disse tiltakene er nærmere beskrevet i **Vedlegg 2**.

4.3 Databehandleren må sørge for at ansatte som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene konfidensielt, eller er underlagt relevant lovbestemt taushetsplikt.

4.4 Dersom Datakontrolløren ber om det, må Databehandleren opplyse om og/eller dokumentere at Databehandleren overholder kravene i gjeldende personvernlovgivning, inkludert dokumentasjon vedrørende dataflyten til Databehandleren samt prosedyrer/policyer for behandling av personopplysninger.

4.5 Ut fra behandlingens karakter, skal Databehandleren, så langt mulig, bistå Datakontrolløren med hensiktsmessige tekniske og organisatoriske tiltak, slik at Datakontrolløren på forespørsel kan bekrefte at forpliktelsen til å respektere subjektenes rettigheter som fastsatt i kapittel 3 i EUs personvernforordning overholdes.

4.6 Databehandleren, eller en annen Databehandler (underdatabehandler) må sende forespørsler og innsigelser fra datasubjektene til Datakontrolløren, for Datakontrollørens videre behandling av disse, med mindre Databehandler selv har rett til å håndtere en slik forespørsel. Hvis Datakontrolløren ber om det, må Databehandleren bistå Datakontrolløren i å svare på slike forespørsler og/eller innvendinger.

4.7 Dersom Databehandleren behandler personopplysninger i et annet EU-medlemsland, må Databehandleren overholde lovgivningen og iverksette de nødvendige sikkerhetstiltakene i dette medlemslandet.

4.8 Databehandleren skal varsle Datakontrolløren dersom det er driftsbrudd, mistanke om brudd på personvernet eller andre uregelmessigheter i forbindelse med behandlingen av personopplysningene. Databehandlerens frist for å varsle Datakontrolløren om sikkerhetsbrudd er 24 timer fra det øyeblikk Databehandleren blir oppmerksom på sikkerhetsbruddet. Hvis Datakontrolløren ber om det, må Databehandleren bistå Datakontrolløren i å avklare omfanget av sikkerhetsbruddet, inkludert å utarbeide en eventuell melding til det relevante datatilsynet og/eller datasubjektene.

Databehandleren må sørge for at all nødvendig informasjon i henhold til artikkel 28 i EUs personvernforordning og avtalen er tilgjengelig for Datakontrolløren og at det overholdes. I denne forbindelsen bidrar til og åpner Databehandleren for ettersyn, inkludert inspeksjoner, utført av Datakontrolløren eller annen kontrollør med mandat fra Datakontrolløren.

4.10 I tillegg til ovennevnte, må Databehandleren bistå Datakontrolløren i å sikre at Datakontrollørens forpliktelser i henhold til artikkel 32-36 i GDPR overholdes. Bistanden tar hensyn til behandlingens art og informasjonen som er tilgjengelig for Databehandleren.

5. Dataoverføring til underdatabehandlere eller tredjeparter

5.1 Databehandleren må overholde vilkårene fastsatt i artikkel 28, paragraf 2 og 4 i GDPR hvis en annen databehandler (underdatabehandler) skal engasjeres. Det innebærer at Databehandleren ikke kan engasjere en annen databehandler (underdatabehandler) til å utføre avtalen uten forutgående spesifikk eller generell skriftlig godkjenning fra Datakontrolløren.

5.2 Datakontrolløren gir derved Databehandleren fullmakt til å inngå avtaler med underdatabehandlere. Databehandleren skal varsle Datakontrolløren om eventuelle endringer i tillegg eller utskifting av underdatabehandlere senest 30 dager før en ny underdatabehandler starter behandlingen av personopplysningene. Datakontrolløren kan komme med rimelige og relevante innvendinger mot slike endringer innen 14 dager fra varselet er mottatt. Dersom Databehandleren fortsatt ønsker å benytte seg av en underdatabehandler som Datakontrolløren har motsatt seg, har partene rett til å si opp avtalen, jfr. paragraf 7.

5.3 Når Datakontrolløren har godkjent at Databehandleren kan benytte seg av en underdatabehandler, skal Databehandleren pålegge underdatabehandleren de samme forpliktelsene som er fastsatt i avtalen. Det skal gjøres i en kontrakt eller en annen rettsakt i henhold til EUs lovgivning eller lovgivningen i et medlemsland. Det må f.eks. foreligge tilstrekkelige garantier fra underdatabehandleren for å iverksette passende tekniske og organisatoriske tiltak på en slik måte at behandlingen oppfyller kravene i GDPR («samsvars»- vilkår).

5.4 Hvis underdatabehandleren ikke oppfyller sine datavernforpliktelser, er Databehandleren fortsatt fullt og helt ansvarlig overfor Datakontrolløren for underdatabehandlerens overholdelse av sine forpliktelser.

5.5 Offentliggjøring, overføring og intern bruk av Datakontrollørens personopplysninger til et tredjepartsland eller internasjonale organisasjoner kan kun skje i samsvar med dokumenterte instrukser fra Datakontrolløren – med mindre det er fastatt i et EU-direktiv eller lovverket i et EU-land som Databehandleren er underlagt. I så fall, må Databehandler varsle Datakontrolløren om det juridiske kravet før behandlingen, med mindre loven forbyr slik varsling av viktige hensyn til offentlige interesser.

5.6 Dersom personopplysningene, som er fastsatt i **Vedlegg 1,** overføres til underdatabehandlere utenfor EU/EØS, skal det angis i avtalen at datavernlovgivningen i Datakontrollørens land er gjeldende for underdatabehandlerne. Videre, dersom mottakende underdatabehandler er etablert innenfor EU/EØS, skal det fremgå av nevnte databehandleravtale at det mottakende EU-landets særskilte lovpålagte krav til databehandlere, f.eks. om meldingskrav til nasjonale myndigheter, gjelder.

5.7 Databehandleren plikter å inngå skriftlige databehandleravtaler med underdatabehandlere innenfor EU/EØS. Når det gjelder underdatabehandlere utenfor EU/EØS, må Databehandleren sørge for tilstrekkelige overføringsmekanismer og inngå en underdatabehandleravtale i form av en standardavtale i samsvar med EU-kommisjonens standardkontraktsvilkår ("**Standardkontrakter**") basert på 2021/914/EU av 4. juni 2021.

5.8 Når denne avtalen signeres, engasjerer Databehandleren underdatabehandlerne som er oppført i **Vedlegg 3**.

6. Ansvar

6.1 Partenes ansvar reguleres av hovedavtalen.

6.2 Partenes erstatningsansvar i henhold til denne avtalen er regulert av Hovedavtalen.

7. Dato for ikrafttredelse og oppsigelse av avtalen

7.1 Denne avtalen trer i kraft samtidig med Hovedavtalen. Ved oppsigelse av Hovedavtalen vil også denne avtalen opphøre. Databehandleren er imidlertid underlagt forpliktelsene fastsatt i denne avtalen, så lenge Databehandleren behandler personopplysninger på vegne av Datakontrollløren.

7.2 Når behandlingstjenestene opphører, er Databehandleren forpliktet til på anmodning fra Datakontrollløren, å slette eller sende tilbake alle personopplysninger til Datakontrollløren, samt å slette eksisterende kopier, med mindre oppbevaring av personopplysningene kreves av EU eller nasjonal lovgivning.

8. Gjeldende lov og jurisdiksjon

8.1 Alle krav eller tvister som oppstår fra eller i forbindelse med denne avtalen må behandles av en kompetent førsteinstansrett (tingrett) i samme jurisdiksjon og med samme lovgrunnlag som ligger til grunn for Hovedavtalen.

9. Signaturer

På vegne av datakontrollløren:

_____

[Name] [Title]

På vegne av databehandleren:

_____

Ronni Engelhardt CEO

Vedlegg 1
Datasubjektkategorier, personopplysningstyper og instruksjoner

1. Datasubjektkategorier:

- Databehandleren vil behandle kontaktinformasjon tilhørende datakontrollørens faktiske, potensielle eller tidligere kunder og/eller medlemmer, ansatte, leverandører, bedrifts- og samarbeidspartnere og tilknyttede enheter.
- Databehandlerens system er tilgjengelig for datakontrolløren som en vertsbasert tjeneste, og det er ikke mulig for databehandleren å bestemme alle datasubjektkategoriene. Hvis datakontrolløren hoster data om ytterligere datasubjektkategorier hos databehandleren er det datakontrollørens plikt å registrere denne informasjonen.

2. Personopplysningstyper:

- Kontakt- og identifikasjonsinformasjon inkludert e-post
- IP-adresser
- Domenenavn
- Brukernavn
- Medlemskapsinformasjon
- Analyser og bruksdata
- Bestillingshistorikk og informasjon
- Kontrakter
- Kommunikasjon
- Støtte
- Bilder
- Ekstra personopplysningstyper som kan forekomme

3. Instruksjoner

Tjenester

Databehandleren kan behandle personopplysninger om datasubjektene med det formål å levere, utvikle, administrere og administrere tjenestene i hovedavtalen, inkludert å sørge for servernes stabilitet og oppetid samt oppfylle juridiske krav.

Oppbevaringsperiode

Personopplysningene som er lagret/hostet i våre systemer slettes eller anonymiseres innen rimelig tid etter at datakontrolløren fullstendig har sagt opp hovedavtalen. Unntaket er data som databehandleren må lagre lenger fordi det er lovpålagt. Denne datatypen vil vanligvis bli slettet innen åtte uker, men kan slettes tidligere. Andre typer data som er lagret i logger osv. vil bli slettet etter rimelig tid, vanligvis innen 8 uker, deretter slettes de hos databehandleren.

Behandlingssted

Behandling av personopplysninger som omfattes av avtalen må ikke foretas uten datakontrollørens skriftlige forhåndssamtykke på andre steder enn databehandlerens adresse og adressen til underdatabehandlerne, som er oppført i vedlegg 3.

Databehandlerens inspeksjon

Databehandleren må en gang i året, for egen regning, innhente en revisjons-/inspeksjonsrapport fra en tredjepart vedrørende databehandlerens etterlevelse av denne avtalen og vedleggene. Rapporten eller annet revisjonsformat må sendes til datakontrolløren eller publiseres på datakontrollørens nettsted så snart som mulig når den er utarbeidet.

Vedlegg 2
Sikkerhetstiltak

Domene	Praksis
Organisering av informasjonssikkerhet	**Sikkerhetseierskap**. One.com har utnevnt en sikkerhetsansvarlig for å koordinere og overvåke sikkerhetsreglene og -prosedyrene. En styring bestående av individer på c-nivå bistår og veileder den sikkerhetsansvarlige. **Sikkerhetsroller og -ansvar**. One.coms ansatte med tilgang til kundedata er underlagt konfidensialitetsforpliktelser, det vektlegges ved ansettelse og kontinuerlig bevissthet. **Risikostyring**. One.com utfører kontinuerlig risikovurdering, det er en del av risikostyringen, før behandling av kundedata eller lansering av tjenester. Risikostyringens sporinger gjør det mulig å fokusere på relevante trusler ved å prioritere, strukturere og redusere risikoer der det er akseptert. Sikkerhetskopiering er implementert. Databehandler beholder sine sikkerhetsdokumenter i henhold til sine oppbevaringskrav etter at de ikke lenger er i kraft.
Forvaltning av eiendeler	**Oversikt over aktiva**. Databehandleren har en oversikt over alle medier der kundedata er lagret. Tilgang til aktiva i slike medier er

Domene	Praksis
	begrenset til databehandlerens ansatte som er skriftlig autorisert til å ha slik tilgang. **Håndtering av aktiva** - One.com klassifiserer kundedata for å bidra med å identifisere dem og for å tillate at tilgangen til dem begrenses på passende måte. - Databehandlerens ansatte må innhente databehandlerautorisasjon før de lagrer kundedata på bærbare enheter, fjerntilgang til kundedata eller behandler kundedata utenfor databehandlerens fasiliteter.
Sikkerhet vedrørende menneskelige ressurser	**Sikkerhetsopplæring**. One.com informerer sine ansatte om relevante sikkerhetsprosedyrer og deres respektive roller samt tar hånd om nye trusler osv. der de ansatte spiller en viktig rolle.
Fysisk og miljømessig sikkerhet	**Fysisk tilgang til fasilitetene.**. One.com begrenser tilgangen til fasiliteter, der informasjonssystemer som behandler kundedata befinner seg, til identifiserte autoriserte personer. **Fysisk tilgang til komponenter**. One.com sørger for tilstrekkelige restriksjoner til medier som inneholder kundedata. **Beskyttelse mot forstyrrelser**. One.com bruker en rekke industristandardsystemer for å beskytte mot tap av data på grunn av strømbrudd, flom, brann eller linjeforstyrrelser. **Avhending av komponenter**. One.com bruker industristandard prosesser for å slette kundedata når de ikke lenger trengs.
Kommunikasjons- og driftsadministrasjon	**Operasjonell policy**. One.com oppbevarer sikkerhetsdokumenter som beskriver sikkerhetstiltak og relevante prosedyrer og ansvar for de ansatte som har tilgang til kundedata. **Datagjenopprettingsprosedyrer** - One.com lagrer kopier av kundedata og datagjenopprettingsprosedyrer på et annet

Domene	Praksis
	sted enn der det primære datautstyret som behandler kundedataene befinner seg. - One.com har spesifikke prosedyrer på plass for tilgang til kopier av kundedata. **Skadelig programvare**. One.com har kontroller mot skadelig programvare for å unngå at skadelig programvare får uautorisert tilgang til kundedata, inkludert skadelig programvare som stammer fra offentlige nettverk. Antivirus er også implementert. **Hendelseslogging**. One.com logger, eller lar kunden logge, få tilgang til samt bruke informasjonssystemer som inneholder kundedata, registrering av tilgangs-ID, tidspunkt, autorisasjon gitt eller nektet og relevant aktivitet. **Kryptering**. Kommunikasjon over internett mellom systemer som håndterer personopplysninger er kryptert.
Tilgangskontroll	**Tilgangspolicy**. One.com oppbevarer en oversikt over enkeltpersoners sikkerhetsprivilegier for personer som har tilgang til kundedata. **Tilgangsautorisasjon** - One.com deaktiverer autentiseringslegitimering som ikke har blitt brukt på en periode, denne perioden tilsvarer seks måneder. - One.com identifiserer ansatte som kan gi, endre eller avlyse autorisert tilgang til data og ressurser. - One.com sikrer at de tilfeller der mer enn én person har tilgang til systemer som inneholder kundedata, har personene separate identifisering/innlogginger. **Minste privilegium** - One.com begrenser tilgang til kundedata til kun personer som trenger slik tilgang for å utføre jobbfunksjonen sin.

Domene	Praksis
	Integritet og konfidensialitet - One.com ber sine ansatte om å deaktivere administrative økter når de forlater lokalene eller når datamaskiner på annen måte blir stående uten tilsyn. - One.com lagrer passord på en måte som gjør dem uforståelige mens de er i kraft. **Autentisering** - One.com bruker praksis som følger industristandard for å identifisere og autentisere brukere som forsøker å få tilgang til informasjonssystemene. - I de tilfellene autentiseringsmekanismene baserer seg på passord, krever databehandleren at passordene fornyes regelmessig. - One.com sørger for at deaktiverte eller utløpte identifiseringer ikke gis til andre individer. - One.com overvåker, eller lar kunden overvåke, gjentatte forsøk på å få tilgang til informasjonssystemet ved å bruke et ugyldig passord. - One.com opprettholder bransjestandardprosedyrer for å deaktivere passord som har blitt ødelagt eller utilsiktet avslørt. - One.com bruker passordbeskyttelsespraksis som følger industristandard, dette inkluderer praksis som er utviklet for å opprettholde konfidensialiteten og integriteten til passordene når de tildeles og distribueres samt under lagring. **Nettverksdesign**. One.com har kontroller for å unngå at enkeltpersoner påtar seg tilgangsrettigheter de ikke har blitt tildelt, for å få tilgang til kundedata de ikke har autorisasjon til å få tilgang til.
Informasjonssikkerhet hendelsesstyring	**Hendelsesresponsprosess** - One.com fører en oversikt over sikkerhetsbrudd med en beskrivelse av

Domene	Praksis
	bruddet, tidsperioden, konsekvensene av bruddet, navnet på den som rapporterer og hvem bruddet ble rapportert til samt prosedyren for gjenoppretting av data. - For hvert sikkerhetsbrudd som er karakterisert som en sikkerhetshendelse vil bli varslet av One.com uten unødig forsinkelse og uansett innen 72 timer. - One.com sporer, eller gjør det mulig for kunden å spore avsløringer av kundedata, det omfatter informasjon om de data som er avslørt, til hvem og på hvilket tidspunkt.
Bedriftskontinuitetsstyring	- One.com oppbevarer nød- og beredskapsplaner for fasilitetene der databehandlerinformasjonssystemer som behandler kundedata befinner seg. - One.coms redundante lagring og prosedyrer for gjenoppretting av data er utformet for å forsøke å rekonstruere kundedata i sin opprinnelighet eller sist kopierte tilstand fra før det tidspunktet de ble tapt eller ødelagt.

Vedlegg 3
Liste over underdatabehandlere

Leverandør	Sted	Funksjon	Oppdatert
Global Connect A/S	DK	Datacenter	20.02.2021
Interxion	DK	Datacenter	12.04.2021
Interxion	DK/UK/NL/FR/DE	PoP (tilstedeværelsespunkt)	12.04.2021
Equinix	SE	PoP (tilstedeværelsespunkt)	12.04.2021