Avtal om behandling av uppgifter

mellan

……..

– den personuppgiftsansvarige – nedan kallad *kunden* –

och

ALSO Sweden AB

Finlandsgatan 14

164 74 Kista

– personuppgiftsbiträdet – nedan kallad *leverantören*

1. Instruktionens eller kontraktets föremål och varaktighet

(1) Föremål

Föremålet för den order eller det kontrakt som rör behandlingen av uppgifter är leverantörens utförande av följande tjänster eller uppgifter: teknisk support, orderhantering, IT-tjänster, kundtjänster och molntjänster.

(2) Varaktighet

Varaktigheten (löptiden) för denna order motsvarar löptiden för tjänsteavtalet inom ramen för respektive produkt-, tjänste-, inköps- och/eller arbetskontrakt.

2. Beskrivning av ordern eller kontraktet

(1) Typ och syfte med avseende på den avsedda behandlingen av uppgifter

Detaljerad beskrivning av föremålet med avseende på typen av och syftet med de tjänster som leverantören utför:

Typ av uppgifter	Syftet med behandlingen	Den registrerade
Personuppgifter: namn, adress, kontaktuppgifter, bankkontouppgifter	Behandling av ordern, teknisk support, IT-tjänster, kundtjänster, molntjänster	Den personuppgiftsansvariges anställda, affärspartner, kunder, säljare, berörda personer

Den enligt kontraktet avtalade behandlingen av uppgifter ska uteslutande utföras i en av Europeiska unionens (EU) medlemsstater, i en medlemsstat i Europeiska ekonomiska samarbetsområdet (EES) eller i ett land som tas upp i Europeiska kommissionens beslut om adekvat skyddsnivå. Varje överföring av uppgifter till en stat som inte är en medlemsstat i antingen EU eller EES kräver förhandstillstånd från kunden och ska bara ske om de särskilda villkoren i artikel 44 och efterföljande i GDPR har uppfyllts. En adekvat skyddsnivå i ett land som inte är medlem i EU bör garanteras enligt EU:s standardavtalsklausuler. (Art. 46.2 c och d i EU-GDPR)

(2) Typ av uppgifter

Föremålet för behandlingen av personuppgifter omfattar följande datatyper/datakategorier: personliga stamuppgifter (grundläggande personuppgifter), kontaktuppgifter, grundläggande kontraktsuppgifter (kontraktsmässiga/juridiska förhållanden, kontraktsmässiga eller produktrelaterade intressen), kundhistorik, uppgifter om kontraktsfakturor och betalningar, utlämnad information (från tredje parter, t.ex. kreditupplysningsbyråer eller från offentliga register), information om systemkonfigurationer och kundmiljöer.

(3) Kategorier av registrerade

Kategorierna av registrerade omfattar: den personuppgiftsansvariges anställda, affärspartner, kunder, potentiella kunder, prenumeranter, anställda, leverantörer, kontaktpersoner.

3. Tekniska och organisatoriska åtgärder

(1) Innan behandlingen inleds, ska leverantören dokumentera utförandet av de nödvändiga tekniska och organisatoriska åtgärder som fastställts, innan orden eller kontraktets tilldelas, särskilt med hänsyn till det detaljerade utförandet av kontraktet samt uppvisa dessa dokumenterade åtgärder för kunden för inspektion. När kunden godtar de dokumenterade åtgärderna, utgör dessa grunden för kontraktet. Om kundens inspektion/granskning visar att det behövs ändringar ska sådana genomföras efter ömsesidig överenskommelse.

(2) Leverantören ska säkerställa säkerheten i enlighet med artikel 28.3 c och artikel 32 i GDPR, i synnerhet jämfört med artikel 5.1 och 5.2 i GDPR. De åtgärder som ska vidtas är datasäkerhetsåtgärder och åtgärder som garanterar en skyddsnivå som lämpar sig för risken beträffande systemens konfidentialitet, integritet, tillgänglighet och motståndskraft. Den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter i den mening som avses i artikel 32.1 i GDPR, måste beaktas. [Detaljer i Bilaga 1]

(3) De tekniska och organisatoriska åtgärderna är föremål för tekniska framsteg och annan utveckling. I detta avseende får leverantören genomföra alternativa, adekvata åtgärder. I samband med detta får de definierade åtgärdernas säkerhetsnivå inte sänkas. Omfattande ändringar måste dokumenteras.

4. Rättelse, begränsning och radering av uppgifter

(1) Leverantören får inte på eget bevåg rätta, radera eller begränsa behandlingen av uppgifter som behandlas å kundens vägnar, utan bara efter dokumenterade instruktioner från kunden.
Om den registrerade kontaktar leverantören direkt gällande en rättelse, radering eller begränsning av behandlingen, ska leverantören omedelbart vidarebefordra den registrerades begäran till kunden.

(2) Om det ingår i tjänsternas omfattning ska raderingspolicyn, ”rätten att bli bortglömd”, rättelse, dataportabilitet och åtkomst säkerställas av leverantören i enlighet med dokumenterade instruktioner från kunden utan onödigt dröjsmål.

5. Leverantörens kvalitetssäkring och andra uppgifter

Utöver efterlevnad av reglerna i denna order eller detta kontrakt ska leverantören uppfylla de lagstadgade krav som avses i artiklarna 28–33 i GDPR. I enlighet därmed säkerställer leverantören, i synnerhet, efterlevnad av följande krav:

a) ☐ Utnämnt dataskyddsombud, som utför sina skyldigheter i enlighet med artiklarna 38 och 39 i GDPR.

☐Kunden ska informeras om hans/hennes kontaktuppgifter för att kunna etablera direkt kontakt. Kunden ska omedelbart informeras, om dataskyddsombudet byts ut.

☐Leverantören har utnämnt [ange: förnamn, efternamn, organisationsenhet, telefonnummer, e-postadress]
……
……
……
……t
ill dataskyddsombud. Kunden ska omedelbart informeras, om dataskyddsombudet byts ut.

☐Hans/hennes aktuella kontaktuppgifter ska alltid finnas tillgängliga och lätt kunna nås på leverantörens webbplats.

b) ☐ Leverantören är inte skyldig att utnämna ett dataskyddsombud. [Ange: förnamn, efternamn, organisationsenhet, telefonnummer, e-postadress]
……
……
……utses till kontaktperson å leverantörens vägnar.

c) ☐ Eftersom leverantören är etablerad utanför EU, utser denne följande företrädare inom unionen enligt artikel 27.1 i GDPR: [Ange: förnamn, efternamn, organisationsenhet, telefonnummer, e-postadress]
……
……
……

d) Konfidentialitet enligt led b andra meningen i artikel 28.3 samt artiklarna 29 och 32.4 i GDPR. Leverantören ska endast låta sådana anställda utföra behandlingen av uppgifter enligt detta kontrakt som omfattas av tystnadsplikt och som tidigare har bekantat sig med de dataskyddsbestämmelser som är relevanta för deras arbete. Leverantören och alla personer som agerar under dennes ansvar, som har åtkomst till personuppgifter, ska inte behandla dessa uppgifter, såvida inte instruktioner har erhållits från kunden, vilket inkluderar de befogenheter som beviljats i detta kontrakt, om inte detta krävs enligt lag.

e) Genomförande och efterlevnad av alla tekniska och organisatoriska åtgärder som krävs för denna order eller detta kontrakt i enlighet med led c andra meningen i artikel 28.3 och artikel 32 i GDPR [detaljer i Bilaga 1].

f) Kunden och leverantören ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dess uppgifter.

g) Kunden ska omedelbart informeras om eventuella inspektioner och åtgärder som utförs av tillsynsmyndigheten, i den mån de avser denna order eller detta kontrakt. Detta gäller också om leverantören håller på att utredas eller är part i en utredning som genomförs av en behörig myndighet i samband med överträdelser av civilrätt eller straffrätt, eller någon administrativ regel eller föreskrift gällande behandlingen av personuppgifter, i samband med behandlingen av denna order eller detta kontrakt.

h) Om kunden blir föremål för en inspektion från tillsynsmyndighetens sida, en administrativ eller summarisk överträdelse eller ett straffrättsligt förfarande, ett skadeståndskrav från en registrerad eller en tredje part eller något annat krav i samband med leverantörens behandling av uppgifter enligt ordern eller kontraktet, ska leverantören göra allt den kan för att hjälpa kunden.

i) Leverantören ska regelbundet övervaka de interna processerna samt de tekniska och organisatoriska åtgärderna, för att säkerställa att behandling inom dennes ansvarsområde sker i enlighet med kraven i tillämplig dataskyddslagstiftning och skyddet av den registrerades rättigheter.

j) Bestyrkande av de tekniska och organisatoriska åtgärder, som utförs av kunden som en del av kundens tillsynsbefogenheter, som tas upp i punkt 7 i detta kontrakt.

6. Anlitande av underleverantörer

(1) I detta avtal avses med anlitande av underleverantörer tjänster som direkt rör tillhandahållandet av den huvudsakliga tjänsten. Detta inkluderar inte anknutna tjänster, såsom telekommunikationstjänster, post-/transporttjänster, underhålls- och användarsupporttjänster eller bortskaffande av databärare, liksom andra åtgärder för att säkerställa konfidentialiteten, tillgängligheten, integriteten och motståndskraften hos databehandlingsutrustningens maskin- och programvara. Leverantören ska dock vara tvungen att upprätta lämpliga och juridiskt bindande kontraktsmässiga arrangemang och vidta lämpliga inspektionsåtgärder för att säkerställa dataskydd och datasäkerhet med avseende på kundens uppgifter, även när det rör sig om anknutna tjänster som har lagts ut på underleverantör.

(2) Ordrar kan vidarebefordras till underleverantörer inom ramen för de verksamheter som avtalas i ordern. Leverantören ska omsorgsfullt välja ut underleverantörer enligt deras lämplighet, i synnerhet med avseende på kraven i EU-GDPR, och inspektera dem regelbundet. Dessutom ska leverantören ingå avtal med underleverantörerna om orderhantering i enlighet med detta avtal. Leverantören ska informera kunden i förväg om alla avsedda ändringar med avseende på inblandning eller utbyte av underleverantörer, vilket ger kunden möjlighet att invända mot denna ändring. Om inga invändningar inkommer inom 14 dagar efter delgivningen, ska det betraktas som att ändringen godkänns.

(3) Överföringen av personuppgifter från kunden till underleverantören och påbörjandet av underleverantörernas databehandling ska endast ske efter det att samtliga krav har uppfyllts.

(4) Om underleverantören tillhandahåller den överenskomna tjänsten utanför EU, ska leverantören säkerställa efterlevnaden av EU:s dataskyddsbestämmelser genom lämpliga åtgärder. Detsamma gäller om tjänsteleverantörer ska användas i den mening som avses i den andra meningen i punkt 1.

(5) Vidare anlitande av underleverantörer kräver godkännande från huvudleverantören (åtminstone skriftligen). Alla kontraktsmässiga bestämmelser i kontraktskedjan måste också åläggas den andra underleverantören.

7. Kundens tillsynsbefogenheter

(1) Kunden har, efter samråd med leverantören, rätt att utföra inspektioner som utförs av en person som omfattas av tystnadsplikt, eller att få dem utförda av en revisor som utses i varje enskilt fall. Kunden har rätt att övertyga sig själv om att detta avtal följs av leverantören i samband med dennes affärsverksamhet genom slumpmässiga kontroller, som vanligtvis ska meddelas i god tid.

(2) Leverantören ska se till att kunden kan kontrollera efterlevnaden av leverantörens skyldigheter i enlighet med artikel 28 i GDPR. Leverantören åtar sig att ge kunden nödvändig information på begäran och, i synnerhet, att visa att de tekniska och organisatoriska åtgärderna utförs.

(3) Bevis på sådana åtgärder, som inte bara rör den särskilda ordern eller det särskilda kontraktet, kan ges genom efterlevnad av godkända uppförandekoder enligt artikel 40 i GDPR, certifiering enligt ett godkänt certifieringsförfarande i enlighet med artikel 42 i GDPR, aktuella intyg från revisor, rapporter eller utdrag ur rapporter från oberoende organ (t.ex. revisor, dataskyddsombud, IT-säkerhetsavdelning, dataskyddsrevisor, kvalitetsrevisor), en lämplig certifiering från en IT-säkerhets- eller dataskyddsrevision (t.ex. enligt BSI-Grundschutz [grundcertifiering för IT-säkerhet som tagits fram av den tyska federala byrån för IT-säkerhet, BSI] eller ISO/IEC 27001).

(4) Leverantören kan begära ersättning för möjliggörandet av kundinspektioner.

8. Information i händelse av att leverantören begår överträdelser

(1) Leverantören ska hjälpa kunden att uppfylla skyldigheterna gällande personuppgifternas säkerhet, rapporteringskraven för personuppgiftsincidenter, konsekvensbedömningar avseende dataskydd samt förhandssamråd, som avses i artiklarna 32–36 i GDPR. Detta omfattar följande:

a) Säkerställande av en lämplig skyddsnivå genom tekniska och organisatoriska åtgärder som tar hänsyn till behandlingens omständigheter och syfte liksom den förutspådda sannolikheten och allvarsgraden hos en möjlig överträdelse av lagen till följd av säkerhetssårbarheter och som gör det möjligt att omedelbart upptäcka relevanta överträdelser.
b) Skyldigheten att omedelbart rapportera en personuppgiftsincident till kunden.
c) Skyldigheten att hjälpa kunden med avseende på kundens skyldighet att tillhandahålla information till den berörda registrerade och att omedelbart förse kunden med all relevant information i detta avseende.
d) Ge kunden stöd i samband med dennes konsekvensbedömning avseende dataskyddet.
e) Ge kunden stöd med avseende på förhandssamråd med tillsynsmyndigheten.

(2) Leverantören kan begära ersättning för supporttjänster som inte ingår i tjänstebeskrivningen och som inte kan tillskrivas fel som leverantören ansvarar för.

9. Kundens befogenhet att utfärda instruktioner

(1) Kunden ska omedelbart bekräfta muntliga instruktioner (åtminstone skriftligen).
(2) Leverantören ska omedelbart informera kunden, om denne anser att en instruktion strider mot dataskyddsbestämmelserna. Leverantören ska då ha rätt att skjuta upp utförandet av de berörda instruktionerna, till dess att kunden bekräftar eller ändrar dem.

10. Radering och återlämnande av personuppgifter

(1) Kopior eller dubbletter av uppgifterna ska aldrig skapas utan kundens vetskap, med undantag av säkerhetskopior i den mån de är nödvändiga för att säkerställa korrekt behandling av uppgifterna, liksom uppgifter som krävs för att uppfylla de lagstadgade kraven för att behålla uppgifter.

(2) När det kontrakterade arbetet har slutförts, eller tidigare på kundens begäran (senast i samband med tjänsteavtalets utgång), ska leverantören lämna över till kunden eller – efter föregående godkännande från denne – förstöra alla handlingar, alla behandlings- och användningsresultat och datauppsättningar med anknytning till kontraktet som denne kommit över, på ett sätt som överensstämmer med dataskyddsbestämmelserna. Detsamma gäller för alla relaterade testmaterial samt överblivet och kasserat material, inklusive avfall. En logg över förstörelsen eller raderingen ska tillhandahållas på begäran.
(3) Dokumentation som används för att bevisa korrekt behandling av uppgifter i enlighet med ordern eller kontraktet ska lagras bortom kontraktets varaktighet av leverantören i enlighet med respektive lagringsperiod. Sådan dokumentation kan överlämnas till kunden, när kontraktet löper ut för att befria leverantören från dennes kontraktsmässiga skyldighet.

Kund: _____

_____
(ort/datum)

_____
(namnteckning/stämpel)

_____
(undertecknarens namn/funktion)

Leverantör:_____

_____
(ort/datum)

_____
(namnteckning/stämpel)

_____
(undertecknarens namn/funktion)

Bilaga – Tekniska och organisatoriska åtgärder

1. Konfidentialitet (artikel 32.1 b i GDPR)

- Kontroll av fysisk åtkomst
  Ingen obehörig åtkomst till databehandlingsanläggningar, t.ex.: magnet- eller chipkort, nycklar, elektroniska dörröppnare, säkerhetstjänster som rör anläggningen och/eller säkerhetspersonal vid ingången, larmsystem, videosystem/kameraövervakningssystem.
- Kontroll av elektronisk åtkomst
  Ingen obehörig åtkomst till databehandlings- eller datalagringssystemen, t.ex.: (säkra) lösenord, automatiska blockerings-/låsmekanismer, tvåfaktorsautentisering, kryptering av databärare/lagringsmedier.
- Kontroll av intern åtkomst (tillstånd för användarrättigheter för åtkomst till och ändring av uppgifter)
  Ingen obehörig läsning, kopiering, ändring eller radering av uppgifter inom systemet, t.ex. begreppet rättighetsautentisering, behovsbaserade åtkomsträttigheter, loggning av systemåtkomsthändelser.
- Kontroll av isolering
  Isolerad behandling av uppgifter, som samlas in för olika ändamål, t.ex. support för flera kunder, begränsat läge
- Pseudonymisering (artikel 32.1 a i GDPR och artikel 25.1 i GDPR)
  Behandling av personuppgifter med en sådan metod/på ett sådant sätt att uppgifterna inte kan associeras med en specifik registrerad utan ytterligare information, under förutsättning att denna ytterligare information lagras separat och är föremål för lämpliga tekniska och organisatoriska åtgärder.

2. Integritet (artikel 32.1 b i GDPR)

- Kontroll av uppgiftsöverföring
  Ingen obehörig läsning, kopiering, ändring eller radering av uppgifter med elektronisk överföring eller transport, t.ex.: kryptering, virtuella privatnät (VPN), elektroniska signaturer.
- Kontroll av datainmatning
  Kontroll av huruvida och av vem personuppgifter förs in i ett databehandlingssystem ändras eller raderas, t.ex.: loggning, dokumenthantering.

3. Tillgänglighet och motståndskraft (artikel 32.1 b i GDPR)

- Kontroll av tillgänglighet
  Förebyggande av förstörelse eller förlust genom olyckshändelse eller med avsikt, t.ex.: säkerhetskopieringsstrategi (online/offline, på plats/på annan plats), avbrottsfri kraftförsörjning (UPS), virusskydd, brandskydd, rapporteringsförfaranden och beredskapsplanering.
- Snabb återställning (artikel 32.1 c i GDPR)

4. Förfaranden för regelbunden testning, undersökning och utvärdering (artikel 32.1 d i GDPR och artikel 25.1 i GDPR)

- Hantering av dataskydd
- Incidenthantering
- Inbyggt dataskydd och dataskydd som standard (artikel 25.2 i GDPR)

- Kontroll av order eller kontrakt
  Ingen behandling av uppgifter får utföras av tredje part enligt artikel 28 i GDPR utan motsvarande instruktioner från kunden, t.ex.: klara och otvetydiga arrangemang, formaliserad orderhantering, strikta kontroller av valet av tjänsteleverantör, skyldighet att utföra förhandsutvärderingar, uppföljningskontroller av övervakning.