AVTAL OM DATABEHANDLING

mellan
[NAMN] org. nr. [], (”personuppgiftsansvarig”)
och
No Isolation AS, org. nr. 815 716 272 (”personuppgiftsbiträde”)

1. Ändamål

Detta avtal reglerar behandlingen av personuppgifter som personuppgiftsbiträdet utför på uppdrag av personuppgiftsansvarig i enlighet med det huvudavtal som ingåtts den [datum]. Avtalets ändamål är att säkerställa att personuppgifter behandlas i enlighet med svensk lagstiftning.

2. Personuppgiftsbiträdets förpliktelser

Personuppgiftsbiträdet ska:

a) behandla personuppgifter endast i enlighet med personuppgiftsansvarigs dokumenterade anvisningar. Personuppgiftsbiträdet ska snarast informera personuppgiftsansvarig om anvisningarna är bristfälliga eller strider mot svensk lag;
b) försäkra sig om att anställda och underleverantörer eller annan tredjepart som är behörig att behandla personuppgifter för den personuppgiftsansvariges räkning är belagd med tystnadsplikt;
c) vidta lämpliga tekniska och organisatoriska åtgärder enligt GDPR artikel 32. Informationssäkerhetsåtgärderna finns närmare beskrivna i bilaga 2;
d) vidta dataminimerande åtgärder, t.ex. pseudonymisering, för att begränsa mängden lagrade identifierbara uppgifter;
e) försäkra sig om att bindande avtal ingåtts med eventuella personuppgiftsbiträden som anlitats av ordinarie personuppgiftsbiträde i enlighet med GDPR artikel 28, nr. 2 och 4;
f) meddela personuppgiftsansvarig om personuppgifter ska överföras utanför EES-området och försäkra sig om att personuppgifterna är adekvat skyddade genom standardmässiga avtalsvillkor som utarbetats av EU-kommissionen eller enligt annan grundlag för överförande enligt GDPR;
g) göra all information tillgänglig på personuppgiftsansvarigs begäran (utan kostnad för personuppgiftsansvarig) som är nödvändig för dokumentationen av att personuppgiftsansvarig och personuppgiftsbiträdet uppfyller kraven enligt GDPR, artikel 28. Personuppgiftsbiträdet ska göra allt material tillgängligt så att personuppgiftsansvarig kan utföra revisioner och inspektioner, som utförs av personuppgiftsansvarig eller tredjepart som anlitats av personuppgiftsansvarig;
h) protokollföra (föra logg) över de behandlingsaktiviteter denne utför på uppdrag av personuppgiftsansvarig som minimum ska innehålla den information som krävs enligt GDPR artikel 30. Personuppgiftsansvarig kan vid var tid infordra kopia av sådant protokoll;
i) omedelbart meddela personuppgiftsansvarig om personuppgiftsbiträdet mottar begäran från myndighet om att lämna ut personuppgifter som behandlats i enlighet med detta avtal. Personuppgiftsbiträdet är dock inte skyldig att meddela enligt ovan om det enligt lag är förbjudet att lämna meddelande. Såvida inte detta är ett krav enligt lag ska personuppgiftsbiträdet inte tillmötesgå en sådan förfrågan utan skriftligt förhandsgodkännande av personuppgiftsansvarig;
j) bistå personuppgiftsansvarig med att besvara förfrågningar från den registrerade i enlighet med GDPR kapitel III (bland annat om rätten till information, insyn, rättelse och korrigering); och
k) bistå personuppgiftsansvarig med att uppfylla sina förpliktelser i enlighet med GDPR artikel 32-36.

Personuppgiftsbiträdets förpliktelse att bistå personuppgiftsansvarig enligt j) och k) ska vägas mot behandlingens art och den information som finns tillgänglig för personuppgiftsbiträdet. Personuppgiftsbiträdet har rätt att fakturera personuppgiftsansvarig för sitt arbete med att uppfylla förpliktelserna enligt j) och k) enligt de timpriser som överenskommits i huvudavtalet. Personuppgiftsbiträdet äger inte rätt att ta betalt för att uppfylla övriga förpliktelser enligt detta avtal.

3. Meddelanderutiner

Vid brott mot datasäkerheten ska personuppgiftsbiträdet meddela personuppgiftsansvarig inom 48 timmar. Meddelandet ska beskriva:

- arten av brott mot bestämmelserna om personuppgifter, om möjligt kategori och ungefärligt antal berörda personuppgifter;
- namn och kontaktuppgifter till dataskyddsombudet eller annan kontakt som kan lämna mer information;
- de troliga konsekvenserna av brottet mot datasäkerheten;
- de åtgärder som vidtagits eller föreslagits för att åtgärda brottet mot datasäkerheten, bland annat eventuella åtgärder för att minska eventuella följdverkningar.

Om inte all information enligt ovan kan lämnas i första meddelandet ska kompletterande information lämnas snarast möjligt, senast 72 timmar efter det att brottet mot datasäkerheten har inträffat. Personuppgiftsansvarig ska försäkra sig om att rapporter om händelseförloppet översänds till Datainspektionen om detta är ett krav enligt GDPR artikel 33.

4. Användande av underleverantörer och överförande utanför EES-området

Personuppgiftsbiträdet har rätt att anlita underleverantörer. Dessa specificeras i bilaga 1 under Underbiträden.

Personuppgiftsansvarig ska informeras om byte av underbiträden eller vid tillskott med nya underbiträden, och ska ha möjlighet att säga nej till sådana ändringar. Om det inte finns legitim grund till att säga nej har personuppgiftsbiträdet rätt att få de direkta kostnader täckta som uppstått till följd av att denne inte kunnat genomföra den meddelade ändringen.

Personuppgiftsansvarig kan säga upp detta avtal och huvudavtalet om personuppgiftsbiträdet genomför ändringar som involverar underbiträde som personuppgiftsansvarig har sagt nej till. Om det inte finns legitim grund till att säga nej har personuppgiftsbiträdet rätt till en uppsägningsersättning motsvarande ”ersättning för de senaste 12 månaderna innan avtalet sagts upp av personuppgiftsansvarig”.

Personuppgiftsansvarig har legitim grund att säga nej till ändring av underbiträde vid befogad misstanke om att skyddet av personuppgifter kan bli försvagat som en följd av ändringen.

5. Revision

Endera av parterna ska täcka sina egna kostnader i samband med revision. Om det vid en revision framkommer ej oväsentliga försummelser av förpliktelserna enligt detta avtal ska alla kostnader i samband med revisionen täckas av personuppgiftsbiträdet, bland annat personuppgiftsansvarigs och extern revisors rimliga kostnader.

6. Ansvar och ersättning

Parterna ansvarar själva för straffavgifter och övriga sanktioner som kan åläggas på grund av brott mot dataskyddsförordningen.

Om en part har ålagts ersättningsansvar för ett förhållande för vilket den andra parten står som ansvarig, ska den part som står som ansvarig täcka ersättningskostnaderna för den andra parten. Ersättningsansvaret begränsas dock till direkta kostnader, inte indirekta förluster, enligt vad som föreskrivs i huvudavtalet.

7. Avtalets giltighetstid

Avtalet gäller så länge personuppgiftsbiträdet behandlar personuppgifter för personuppgiftsansvarigs räkning enligt huvudavtalet.

Vid personuppgiftsbiträdets brott mot detta avtal eller dataskyddsförordningen kan personuppgiftsansvarig anmoda personuppgiftsbiträdet att avbryta behandlingen av uppgifter med omedelbar verkan.

8. Återlämnande, radering och/eller förstörande vid avtalets upphörande

Vid detta avtals upphörande ska personuppgiftsbiträdet återlämna alla personuppgifter som denne mottagit för personuppgiftsansvarigs räkning.

Personuppgiftsansvarig kan kräva att personuppgiftsbiträdet ska radera eller förstöra alla personuppgifter som behandlas enligt detta avtal. Personuppgiftsansvarig kan anmoda personuppgiftsbiträdet att skriftligen bekräfta till personuppgiftsansvarig att raderingen utförts. Raderingen ska genomföras senast 60 dagar efter avtalets upphörande. Med radering menas att personuppgifterna raderats permanent från alla system med undantag av backup-systemet, se dock punkt 5 i Bilaga 1. Endast teknisk personal har tillgång till backup-systemet.

9. Gällande lag och laga domstol

Gällande lag och laga domstol framgår av huvudavtalet.

10. Undertecknande

_____	_____
Namn	Camilla Pilhjerta Falck-Pedersen
Titel	CFO
Personuppgiftsansvarig	No Isolation AS – personuppgiftsbiträde

Avtal om databehandling

Bilaga 1: Databehandlingens omfattning

1. Ändamål med databehandlingen

Data ska behandlas för följande ändamål:
För autentisering av användarna:

För autentisering av PRO-användarna, ska berörd PRO-användare upprätta ett användarkonto.

För att ha översikt över KOMP-enheterna:

Om det befinns nödvändigt kan uppgifter om användaren knytas till KOMP-enheterna. Detta ger också ökad säkerhet genom att det är lättare att komma ihåg ett namn/initialer samt ett serienummer.

Att erbjuda kommunikationstjänster:

Bilder och meddelanden ska lagras på ett sådant sätt att de kan visas på skärmen eller i systemet. Videoströmmarna är krypterade från ändpunkt till ändpunkt med hjälp av våra system.

En detaljerad användarlogg:

KOMP Pro möjliggör för personuppgiftsbiträdet att upprätta en detaljerad logg över KOMP Pro-kommunikationerna för att på så sätt kunna hjälpa personuppgiftsbiträdet att utföra sina loggningsuppgifter enligt vad som föreskrivs i lag.

2. Kategorier av registrerade

- KOMP-användaren – den som har KOMP-skärmen i sitt hem/rum
- KOMP Pro-användaren – den som använder KOMP Pro-systemet för att kommunicera med KOMP
- De personer som kan identifieras på bilder eller i textmeddelanden som skickats till KOMP

3. Typer av personuppgifter som behandlas

<u>Information om användarkonto</u>
En profil upprättas av en användare med:

- Namn
- E-postadress
- Profilbild
- Unikt användar-ID (automatiskt genererat)

Namn, e-postadress och profilbild är synliga för alla användare i samma organisation. Namnet och profilbilden visas på KOMP när någon ringer till KOMP-enheten så att användaren kan se vem som ringer. Det unika användar-ID: et är länkat till profilen och används vid underhåll av användarloggen.

<u>KOMP användarinformation</u>
Information som kan läggas till om KOMP-användaren för att ha översikt över KOMP-enheterna.

- Namn
- Adress

Denna information kopplar ihop användaren med rätt serienummer för att garantera att du skickar innehållet till rätt användare. Det är inte obligatoriskt att fylla i detta och systemet fungerar utan denna information. Det går också att använda namn som inte är direkt identifierbara, till exempel rumsnummer på ett sjukhus eller bara initialer.

Bilder och meddelanden
Det innehåll som skickas till KOMP kan innehålla information som kan kopplas till identifierbara personer:

- Bilder
- Meddelanden

Meddelandena och bilderna är synliga för KOMP-användaren och andra PRO-användare med tillgång till KOMP. Användaren kan välja varaktighetstid i systemen och innehållet raderas från KOMP efter utgånget giltighetsdatum/utgången tid.

Videoströmmar
Videoströmmarna är en-till-en-samtal och krypterade från ändpunkt till ändpunkt. Videoströmmen lagras inte och är inte tillgänglig obehöriga. Kunden kan slå av funktionen för videosamtal för en KOMP från Pro-gränssnittet.

Användarloggar
Loggarna innehåller följande information:

- Tid och varaktighet för videosamtal och vem som samtalat
- När en bild sändes
- När ett meddelande sändes
- Avsändarens identitet (namn och ID)
- Användarens identitet (serienummer och namn)

Vi skiljer mellan två slags loggar, aktivitetsloggen och hela loggen för systemändamål. Aktivitetsloggarna ligger i gränssnittet för alla PRO-användare med tillgång till samma KOMP-enheter och innehåller inte bara avsändar-ID. Denna inloggning används för att få en översikt över aktiviteten hos en viss bestämd KOMP-enhet. Systemloggen innehåller mer information och lämnas till kontrollanten på begäran.

4. Behandlingen

- PRO-användarkontoinformationen läggs till av personuppgiftsansvarigs anställda genom PRO-gränssnittet.
- Bilderna och meddelandena läggs till av PRO-användarna. De startar även videoströmmar.
- Användarloggarna upprättas automatiskt.
- Metadata samlas automatiskt när KOMP-enheterna används.
- Den användarinformation som behövs för att kunna ge support levereras av PRO-användarna.

5. Behandlingens varaktighet

- Personuppgiftsansvarig kan när som helst radera data via KOMP Pro-gränssnittet.
- Information som inte raderas av personuppgiftsansvarig kommer att lagras under avtalets löptid. All information raderas inom 62 dagar efter avtalets upphörande. Personuppgiftsbiträdet ska radera alla personliga uppgifter permanent från alla system, inklusive backup-systemen (säkerhetskopiorna är orsaken till att denna process kan ta upp till 62 dagar).

- Personuppgiftsansvarig kan anmoda personuppgiftsbiträdet att skicka en skriftlig bekräftelse på att alla uppgifter raderats.
- Systemloggarna lagras i upp till 62 dagar efter avtalets upphörande. Personuppgiftsansvarig kan begära att få en detaljerad systemlogg om de vill lagra dem under längre tid.

6. Databehandling med No Isolation som personuppgiftsansvarig

Vi behandlar metadata (se detaljerad lista nedan) för att ge support till tjänsten. Om du kontaktar oss eller vårt supportteam innebär det att vi behandlar dina kontaktuppgifter. Vi är därmed personuppgiftsansvariga för den aktuella databehandlingen.

<u>Supportdata</u>
Följande data behandlas för att ge kundsupport (av en administratör eller systemanvändare):

- Metadata:
    - Nätverksinformation (SSID och intern IP-adress)
    - Status på KOMP (online, off-line, inte möjligt att få kontakt)
- Information som lämnats av användaren vid support:
    - Namn
    - Telefonnummer
    - E-postadress

7. Underbiträden och överföringar utanför EES

No Isolation använder följande underbiträden för att leverera tjänsten:

- **Amazon Web Services EMEA SARL**

En molntjänsteleverantör som vi använder till våra servrar som lagrar information såsom metadata, bilder och meddelanden som skickats till KOMP samt kundinformation. Behandlingen sker inom EU/EES.

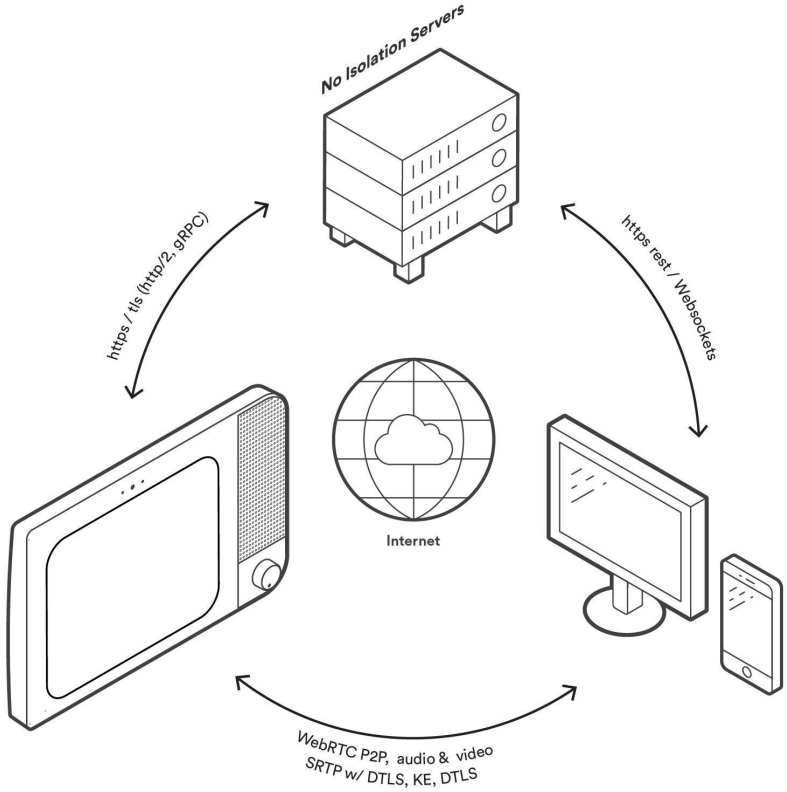
Pseudonymiseringsåtgärder

All metadata som är kopplade till en KOMP, samt alla meddelanden och bilder är kopplade till KOMP-enhetens serienummer. Genom att det är frivilligt att lägga till KOMP-användarinformation kan KOMP-användaren välja att vara anonym för databehandlaren. Det är också möjligt att lägga till initialer, ett rumsnummer etc. istället för ett fullständigt namn.

Krypteringsåtgärder
Vi använder följande krypteringsåtgärder:

A. Våra databaser och filservrar har krypterade diskar, säkerhetskopior och kommunikationer.
B. Videosamtalen är krypterade från ändpunkt till ändpunkt. WebRTC-standarden används för att sätta upp videosamtal. Nyckelutväxlingen görs med DTLS, och kommunikationen är krypterad från ändpunkt till ändpunkt med dessa nycklar vid användande av SRTP.
C. Bilderna laddas upp till våra servrar och vidarebefordras och lagras i Amazon S3. All kommunikation är krypterad med TLS.
D. Meddelandena lagras i vår MongoDB-databas. All kommunikation är krypterad med TLS.
E. Metadata skickas krypterat med TLS mellan enheterna (appar och KOMP) och våra servrar. Man kan också beskriva WebRTC-signaler som "metadata". De överförs (TLS-krypterat) via våra servrar, men lagras inte i våra system.

Översikt över kommunikationen och dataflödet:



Översikt över kommunikationen via KOMP

Tillgångskontroll och rutiner för lösenord:

Tillgång till KOMP
För att kommunicera med KOMP behöver du en inbjudan från systemadministratören. Du kommer i kontakt med KOMP endast via PRO-gränssnittet eller familje-appen.

Vi byter regelbundet lösenord på KOMP, och oauktoriserat tillträde är inte möjligt.

KOMP Pro tillgångskontroll
Vi följer bästa praxis angående behörighet och autentisering av användare i KOMP Pro.

Tillgång till våra system
Internt är alla våra system som behandlar personuppgifter skyddade genom tvåfaktorautentisering. Tillgång till systemet ges enligt principen ”need-to-know”.

Molntjänster
Endast behörig personal har tillgång till Amazons servicepanel. Inloggningen är skyddad genom unika användare, säkra lösenord och tvåfaktorautentisering.

Driftutrustningen är endast tillgänglig via SSH och SSH-nycklarna är lösenordskyddade.

Tillgång till våra kontor
För att få tillgång till våra kontor använder alla våra anställda ett personligt, PIN-skyddat nyckelkort. Besökare ledsagas av någon av våra anställda.

Rutiner för kritiska händelser

Molnbaserade system
Alla system som vi använder är molnbaserade vilket gör att vi snabbt kan återupprätta normala driftsförhållanden på alternativa platser i händelse av allvarliga incidenter såsom brand, översvämning eller liknande. Vi skapar automatiska säkerhetskopior av databasservrarna varje natt och kör transaktionsloggar för det senaste dygnet. Säkerhetskopiorna sparas i 14 dagar och funktionerna för återupprättande testas varje månad.

Övervakning
Vi använder tjänster som AWS Shield och Amazon GuardDuty och följer bästa praxis när vi utvecklar och kör våra system. Vi har kontinuerlig övervakning av systemen och meddelar den operativa personalen med ögonblicklig verkan om systemen inte fungerar som de ska.

Privat nätverk
Hela vår infrastruktur ligger i ett privat nätverk och tillgången styrs av säkerhetsregler som endast tillåter trafik från auktoriserade källor. Det är endast möjligt att ha direkt tillgång till resurserna från No Isolation-kontoret i Oslo, och det är så medarbetare som möjligt på Oslo-kontoret som har tillgång till och kan arbeta med resurserna – operativ personal som behöver ha tillgång till dem för att kunna utföra systemunderhåll.

Systemexponering
Systemet innehåller ett minimalt antal exponerade ändpunkter, dvs. endast det antal ändpunkter som behövs för att göra det möjligt att erbjuda våra tjänster till kunderna. De exponerade ändpunkterna stöder endast HTTPS, och alla klienter (KOMP är exempel på en klient) ska autentiseras av systemet innan ändpunkterna kan användas.

Hackning
Vi skyddar våra system mot hackning och använder till exempel AWS Shield, en administrerad DDoS-skyddstjänst (Distributed Denial of Service) som skyddar applikationer som körs på AWS. Alla medarbetare har fått information om social hackning och hur man skyddar sig mot detta.

Åtgärder i organisationen

Intern kontroll
Vi har internkontrollsystem som bland annat ger en översikt över säkerheten i organisationen, mål och strategier för säkerhet, riskanalyser och rutiner.

Konfidentialitet
Alla anställningsavtal innehåller klausuler om konfidentialitet. Alla medarbetare är förpliktade att iaktta absolut tystnadsplikt om arbetsgivarens verksamhet, inklusive kundförhållanden eller andra kontakter. Tystnadsplikten gäller även efter anställningens slut och så länge informationen är känslig. Detta gäller även konsulter som bolaget anlitar.