DATABEHANDLERAVTALE

mellom
[NAVN] org. nr. []. («behandlingsansvarlig»)
og
No Isolation AS, org. nr. 815 716 272 («databehandler»)

1 Formål

Denne avtalen regulerer behandling av personopplysninger som databehandler gjør på vegne av behandlingsansvarlig i henhold til hovedavtalen, inngått [dato]. Avtalen skal sikre at personopplysninger behandles i samsvar med norsk personvernlovgivning.

2 Databehandlers plikter

Databehandleren skal:

a) kun behandle personopplysninger i samsvar med behandlingsansvarliges dokumenterte instruksjoner. Databehandler skal straks informere behandlingsansvarlig dersom instruksjonene er mangelfulle eller i strid med norsk personvernlovgivning;
b) sikre at ansatte og underleverandører eller andre tredjeparter som er autorisert til å behandle personopplysninger på vegne av den behandlingsansvarlige er underlagt taushetsplikt; c) gjennomføre hensiktsmessige tekniske og organisatoriske tiltak som kreves i henhold til GDPR artikkel 32. Informasjonssikkerhetstiltakene er nærmere beskrevet i vedlegg 2; d) iverksette dataminimerende tiltak, f. eks. pseudonymisering, for å begrense mengden av lagrede identifiserbare opplysninger;
e) sikre at det er inngått bindende avtale med eventuelle underdatabehandlere i henhold til GDPR artikkel 28 nr. 2 og 4;
f) varsle behandlingsansvarlig dersom personopplysninger skal overføres utenfor EØS og sikre at personopplysningene er adekvat beskyttet gjennom standard kontraktsvilkår utarbeidet av EU-kommisjonen eller andre grunnlag for overføring i henhold til GDPR;
g) gjøre all informasjon tilgjengelig på behandlingsansvarliges forespørsel (uten kostnad for behandlingsansvarlig) som er nødvendig for å dokumentere at behandlingsansvarlig og databehandler oppfyller GDPR artikkel 28. Databehandler skal legge til rette for at behandlingsansvarlig kan utføre revisjoner og inspeksjoner, enten av behandlingsansvarlig selv eller en tredjepart utpekt av behandlingsansvarlig;
h) føre protokoll (logg) over behandlingsaktiviteter denne utfører på vegne av den behandlingsansvarlige, som skal inneholde minimum den informasjon som er pålagt etter GDPR artikkel 30. Den behandlingsansvarlige kan til enhver tid kreve oversendt kopi av slik protokoll;
i) umiddelbart varsle den behandlingsansvarlige hvis databehandler mottar forespørsel fra en myndighet om å utlevere personopplysninger behandlet i henhold til denne avtalen. Databehandler plikter ikke å varsle dersom loven forbyr slik underretning. Med mindre loven krever det skal databehandleren ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra den behandlingsansvarlige;
j) bistå behandlingsansvarlig med å svare på forespørsler fra den registrerte i henhold til GDPR kapittel III (deriblant rett til informasjon, innsyn, retting og korrigering); og
k) bistå behandlingsansvarlig med å oppfylle sine forpliktelser i henhold til GDPR artikkel 32-36.

Databehandlerens plikt til å gi bistand til behandlingsansvarlig etter bokstav j) og k) skal vurderes opp mot behandlingens art og den informasjonen som er tilgjengelig for databehandleren. Databehandleren har rett til å fakturere behandlingsansvarlig for arbeid med å oppfylle pliktene i bokstav j) og k) etter de timesatser som er avtalt i hovedavtalen. Databehandler har ikke rett til å ta

betalt for å oppfylle øvrige forpliktelser i denne avtalen.

3 Varslingsrutiner

Ved datasikkerhetsbrudd skal databehandler gi melding til behandlingsansvarlig innen 48 timer. Meldingen skal minimum beskrive:

- arten av brudd på personopplysninger, herunder om mulig, kategoriene og omtrentlig antall berørte registrerte og kategoriene og omtrentlig antall berørte personopplysninger;
- navn og kontaktinformasjon til personvernansvarlig eller annet kontaktpunkt der mer informasjon kan fås;
- beskrive de sannsynlige konsekvensene av datasikkerhetsbruddet;
- beskrive tiltakene som er truffet eller foreslått for å ta hensyn til datasikkerhetsbruddet, herunder eventuelt tiltak for å redusere mulige bivirkninger.

Hvis ikke all informasjon ovenfor kan gis i første varsel, skal informasjonen gis så snart som mulig, og senest 72 timer innen datasikkerhetsbruddet har inntruffet. Behandlingssansvarlig skal sørge for at hendelsesrapporten sendes til Datatilsynet, dersom det kreves av GDPR artikkel 33.

4 Bruk av underleverandører og overføring utenfor EØS

Databehandleren har rett til å benytte underleverandører navngitt i vedlegg 1 som sine databehandlere.

Behandlingsansvarlig skal informeres om bytte av underdatabehandlere eller tillegg av nye underdatabehandlere, og skal ha mulighet til å nekte slike endringer. Dersom nektelsen ikke har en legitim grunn har databehandler rett til å få dekket direkte kostnader som følge av å ikke kunne foreta den varslede endringen.

Behandlingsansvarlig kan si opp denne avtalen og hovedavtalen dersom databehandler foretar endringer av underdatabehandlere som behandlingsansvarlig har nektet. Dersom nektelsen ikke har en legitim grunn har databehandler rett på et oppsigelsesgebyr tilsvarende <gebyr for de siste 12 månedene før avtalen ble sagt opp av behandlingsansvarlig>.

Behandlingsansvarlig har en legitim grunn til å nekte endring av underdatabehandlere ved begrunnet mistanke om at personvernet kan bli svekket som følge av endringen.

5 Revisjon

Hver av partene dekker sine egne kostnader forbundet med en revisjon. Hvis en revisjon avdekker ikke-uvesentlige avvik fra forpliktelsene i denne avtalen, skal alle kostnader forbundet med revisjonen dekkes av databehandleren, herunder den behandlingsansvarliges og eksterne revisorers rimelige kostnader.

6 Ansvar og erstatning

Partene er selv ansvarlig for å dekke administrative bøter og øvrige sanksjoner som ilegges som følge av brudd på personvernlovgivningen.

Dersom en part har blitt ilagt erstatningsansvar for et forhold som den andre parten står ansvarlig for skal den ansvarlige parten dekke erstatningskostnadene. Erstatningsansvaret er likevel begrenset til direkte kostnader, og ikke indirekte tap, i henhold til hovedavtalen.

7 Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig i henhold til hovedavtalen.

Ved databehandlers brudd på denne avtalen eller personvernlovgivningen kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

8 Tilbakelevering, sletting og/eller destruering ved avtalens opphør

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av behandlingsansvarlig.

Behandlingsansvarlig kan kreve at databehandler sletter eller destruerer alle personopplysningene som behandles etter denne avtalen. Behandlingsansvarlig kan be databehandler skriftlig bekrefte til behandlingsansvarlig at sletting er gjennomført. Slettingen skal gjennomføres senest 60 dager etter avtalens opphør. Sletting innebærer at personopplysningene slettes permanent fra alle systemer, med unntak av backup-systemet, se likevel punkt 5 i Vedlegg 1. Det er kun teknisk personale som har tilgang til backup-systemet.

9 Lovvalg og verneting

Lovvalg og verneting følger av hovedavtalen.

10 Signatur

Navn	Camilla Pilhjerta Falck-Pedersen
Tittel	CFO
Behandlingsansvarlig	No Isolation AS - databehandler

Databehandleravtale

Vedlegg 1: Omfanget av databehandlingen

1 Formålet med databehandlingen

Dataene vil bli behandlet for følgende formål:
For å autentisere brukerne:

For å autentisere PRO-brukerne, må PRO-brukeren opprette en brukerkonto. For å holde oversikt over KOMP-ene:

Om nødvendig kan informasjon om bruker knyttes til KOMP-ene. Dette vil også øke sikkerheten, ettersom det er lettere å huske et brukernavn/ initialer og deretter et serienummer.

Å tilby kommunikasjonstjenestene:

Bilder og meldinger må lagres slik at de kan vises på skjermen og i systemet. Videostrømmer settes opp fra ende-til-ende kryptert ved hjelp av systemene våre. En detaljert brukerlogg:

KOMP Pro gjør det mulig for databehandleren å opprettholde en detaljert logg over KOMP Pro-kommunikasjon for å hjelpe databehandleren med å oppfylle sine loggplikter som kreves i henhold til lov.

2 Kategoriene av de registrerte

- KOMP brukeren - den som har KOMP skjermen i sitt hjem/ på sitt rom
- KOMP Pro brukeren - den som bruker KOMP Pro systemet til å kommunisere med KOMP
- De personene som kan identifiseres på bilder eller i tekstbeskjeder sendt til KOMP

3 Typer av personopplysninger som blir behandlet

<u>Brukerkonto informasjon</u>
En profil settes opp av en bruker med:

- Navn
- E-post
- Profilbilde
- Unik bruker ID (automatisk generert)

Navn, e-post og profilbilde er synlige for brukere i samme organisasjon. Navnet og profilbildet vises på KOMP når noen ringer til KOMP´en slik at brukeren kan se hvem som ringer. Den unike bruker ID´en er linket til profilen og blir brukt til vedlikeholde brukerlogg.

KOMP brukerinformasjon
Informasjon som kan bli lagt til om KOMP brukeren for å holde oversikt over KOMP´ene:

- Navn
- Adresse

Denne informasjonen skal knytte riktig bruker til riktig serienummer for å sikre at du sender innholdet til riktig bruker. Dette er ikke obligatorisk å fylle ut, og systemet fungerer uten denne informasjonen. Det er også mulig å bruke navn som ikke er direkte identifiserbare, for eksempel romnummer på et sykehjem, eller bare initialene.

Bilder og beskjeder
Innholdet som blir sendt til KOMP kan inneholde informasjon som kan kobles til identifiserbare personer:

- Bilder
- Beskjeder

Meldingene og bildene er synlige for KOMP-brukeren og andre PRO-brukere med tilgang til KOMP. Brukeren kan velge varighetstid i systemene, og innholdet vil bli slettet fra KOMP etter utløpsdato/ tid.

Videostrøm
Videostrømmene er settes opp for en-til-en samtaler og er ende-til-ende-kryptert. Videostrømmen lagres ikke og det er ikke mulig å få tilgang til utenforstående. Kunden kan slå av videosamtale-funksjonalitet for en KOMP fra Pro-grensesnittet.

Brukerlogger
Loggene inneholder følgende informasjon:
- Tid og varighet for videosamtaler, og av hvem samtalen ble foretatt
- Når bildet ble sendt
- Når meldingen ble sendt
- Avsenderidentitet (navn og ID)
- Brukeridentitet (serienummer og navn)

Vi skiller mellom to typer logger; aktivitetsloggen og hele loggen for systembruk. Aktivitetsloggene er gitt i grensesnittet for PRO-brukere med tilgang til de samme KOMP-ene og inneholder ikke bare navnet på avsender-ID. Denne påloggingen brukes til å få en oversikt over aktiviteten på en bestemt KOMP. Systemloggen inneholder mer informasjon og blir gitt til kontrolleren på forespørsel.

4 Selve behandlingen

- PRO-brukerkontoinformasjonen og KOMP-brukerinformasjonen blir lagt til av behandlingsansvarliges ansatte gjennom PRO-grensesnittet.
- Bildene og meldingene er lagt til av PRO-brukerne. De starter også videostrømmer.

- Brukerloggene opprettes automatisk.
- Metadataene samles automatisk når KOMP-ene er i bruk.
- Brukerinformasjonen som trengs for støtte leveres av PRO-brukerne.

5 Varigheten av behandlingen

- Behandlingsansvarlig kan når som helst slette data i grensesnittet til KOMP Pro.
- Informasjon som ikke slettes av behandlingsansvarlig vil bli lagret i løpet av avtalen mellom partene. All informasjon vil bli slettet innen 62 dager etter at kontrakten er avsluttet. Databehandleren vil slette all personlig informasjon permanent fra alle systemer, inkludert backup-systemene (sikkerhetskopiene er grunnen til at det kan ta opptil 62 dager).
- Behandlingsansvarlig kan be databehandleren om en skriftlig bekreftelse på at all informasjon blir slettet.
- Systemloggene lagres i opptil 62 dager etter at kontrakten er sagt opp.
Behandlingsansvarlig må be om detaljert systemlogg hvis de vil lagre dem over lengre tid.

6 Databehandling hvor No Isolation er behandlingsansvarlig

Vi behandler metadata (se detaljert liste under) for å yte support til tjenesten. Hvis du kontakter oss eller vårt support team, må vi behandle din kontaktinformasjon. Vi er da behandlingsansvarlig for denne databehandlingen.

<u>Support data</u>
Følgende data blir behandlet for å sørge for kundesupport (av en administrator eller systembruker):

- Metadata:
    - Nettverksinformasjon (SSID og intern IP-adresse)
    - Status på KOMP (online, offline, ikke mulig å oppnå kontakt)
- Informasjon gitt av brukeren når man får support:
    - Navn
    - Telefonnummer
    - E-post

7 Underbehandlere og overføringer utenfor EU/ EØS

No Isolation bruker følgende underbehandler for å levere tjenesten:

- **Amazon Web Services EMEA SARL**

Vi bruker skytjenesteselskapet Amazon Web Services EMEA SARL som vår underbehandler. Amazon Web Services EMEA SARL er et europeisk selskap rent juridisk med servere i Frankfurt. Dette selskapet inkorporerer bruken av EUs standard kontraktsklausuler (Standard Contractual Clauses). Vi vil understreke at Amazon Web Services EMEA SARL er

et europeisk selskap som overholder EUs regler og reguleringer, men eies av det amerikanske Amazon-selskapet.

(Lenke: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf)

Databehandleravtale

Vedlegg 2: Sikkerhetstiltak

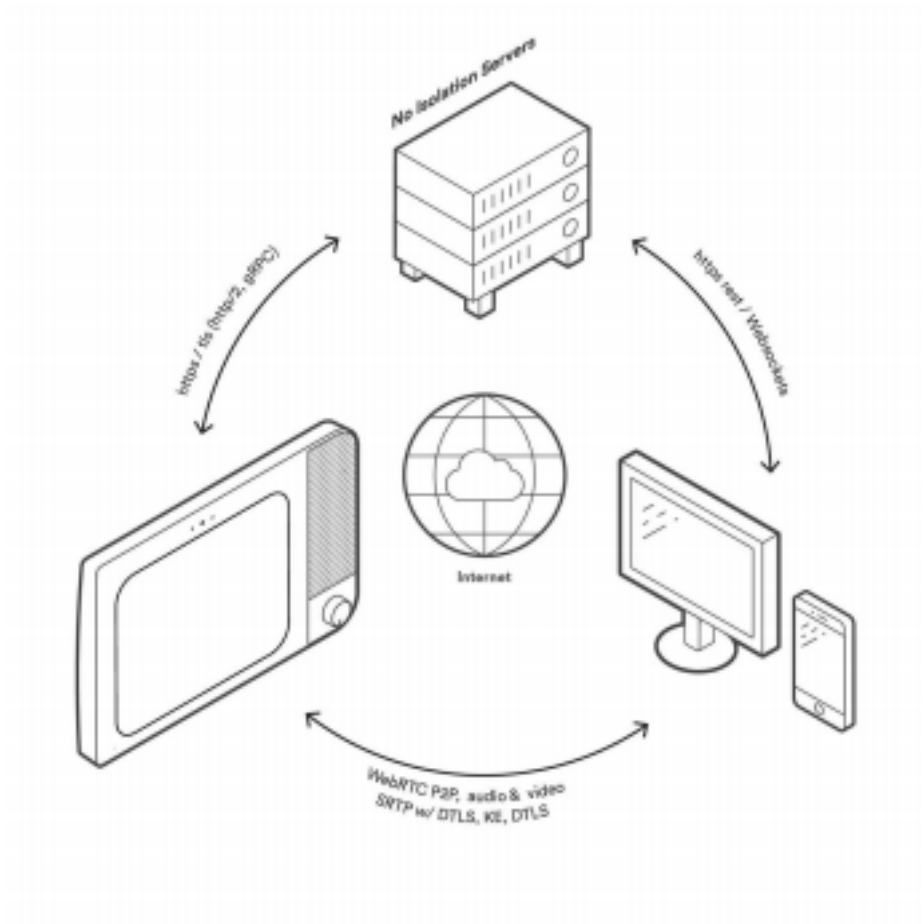
Pseudonymiseringstiltak

Alle metadata som er koblet til en KOMP, samt meldingene og bildene er koblet til KOMPs serienummer. Siden KOMP-brukerinformasjonen er frivillig å legge til, kan KOMP-brukeren være anonym for databehandleren. Det er også mulig å legge til initialer, et romnummer etc. i stedet for et fullt navn.

Krypteringstiltak

Vi bruker følgende krypteringstiltak:

A. Våre databaser og filservere har krypterte disker, sikkerhetskopier og kommunikasjon.
B. Videosamtaler er kryptert fra ende til ende. WebRTC-standarden brukes til å sette opp en videosamtale. Nøkkelutvekslingen gjøres med DTLS, og kommunikasjonen krypteres end-til-ende med disse nøklene ved bruk av SRTP.
C. Bildene lastes opp til serverne våre og videreformidles og lagres i Amazon S3. All kommunikasjon er kryptert med TLS.
D. Meldingene lagres i databasen vår. All kommunikasjon er kryptert med TLS.
E. Metadata sendes kryptert med TLS mellom enhetene (apper og KOMP) og serverne våre. Man kan også beskrive WebRTC-signaler som "metadata". Disse overføres (TLS-kryptert) via serverne våre, men lagres ikke i systemene våre. Dette er en oversikt over kommunikasjonen og dataflyten:



Oversikt over kommunikasjonen via KOMP

Tilgangskontroll og rutiner for passord:

Tilgang til KOMP
For å kommunisere med KOMP trenger du en invitasjon fra systemadministratoren. Det er bare mulig å kontakte KOMP via PRO-grensesnittet eller familie-appen.

Vi bytter passordet regelmessig på KOMP, og uautorisert ekstern tilgang er ikke mulig.

KOMP Pro tilgangskontroll
Vi følger best practice angående autorisasjon og autentisering av brukere i KOMP Pro.

Tilgang til systemene våre
Internt er alle våre systemer som behandler personopplysninger beskyttet med tofaktorautentisering. Tilgang til systemet gis basert på “need-to-know” -prinsippet.

Skytjenester
Bare autorisert personell har tilgang til Amazons betjeningspanel. Innloggingen er sikret av unike brukere, sikre passord og tofaktorautentisering.

Tilgang til driftsutstyr er kun tilgjengelig via SSH og SSH-nøkler er

passordbeskyttet. Tilgang til kontorene våre

For å få tilgang til kontorene våre, må alle ansatte bruke et personlig, pin-beskyttet nøkkelkort. Gjestene må være ledsaget av en ansatt til enhver tid når de besøker.

Rutiner for kritiske hendelser

Skybaserte systemer
Alle systemene vi bruker er skybaserte, og normal drift kan derfor raskt gjenopprettes på et alternativt sted i tilfelle en fysisk katastrofe som brann, flom eller lignende. Vi har automatiske sikkerhetskopier av databaseserverne hver natt og kjører transaksjonslogger det siste døgnet. Sikkerhetskopier oppbevares i 14 dager, og gjenoppretting blir testet hver måned.

Overvåkning
Vi bruker tjenester som AWS Shield og Amazon GuardDuty og følger beste praksis når vi utvikler og kjører systemene våre. Vi har kontinuerlig overvåking av systemene med direkte varsler til operativt personell hvis systemene svikter.

Privat nettverk
Hele infrastrukturen vår er i et privat nettverk og tilgang til den håndheves av sikkerhetsregler som bare tillater trafikk fra autoriserte kilder. Det er bare mulig å ha direkte tilgang til ressursene fra No Isolation-kontoret i Oslo, og det er et minimalt sett med mennesker på Oslo-kontoret som har tilgang til å jobbe med ressursene. Dette er operativt personell som trenger tilgang for å kunne utføre systemvedlikehold.

Systemeksponering
Systemet er bare utsatt for et minimalt sett med endepunkter som må eksponeres for å tilby tjenester til kunder. De eksponerte endepunktene støtter bare HTTPS, og alle klienter (KOMP er et eksempel på en klient) må autentiseres av systemet før endepunktene kan brukes.

Hacking
Vi beskytter systemene våre for hacking og bruker for eksempel AWS Shield, en administrert DDoS-beskyttelsestjeneste (Distributed Denial of Service) som beskytter applikasjoner som kjører på AWS. Alle ansatte har mottatt informasjon om sosial hacking og hvordan de kan unngås.

Tiltak i organisasjonen

Intern kontroll
Vi har internkontrollsystemer som blant annet inkluderer en oversikt over sikkerheten i organisasjonen, mål og strategi for sikkerhet, risikoanalyse og rutiner.

Konfidensialitet
Alle arbeidskontrakter har klausuler om konfidensialitet. Arbeidstakeren er forpliktet til å bevare absolutt taushet om arbeidsgivers forretningsforhold, inkludert kundeforhold eller andre forretningsforbindelser. Taushetsplikten fortsetter etter at ansettelsen er avsluttet, og så lenge informasjonen er sensitiv. Dette gjelder også konsulenter selskapet ansetter.