AVTALE OM NKS CHAT FOR SOSIALE TJENESTER-CHATBOT OG UINNLOGGET CHAT

Databehandleravtale

mellom

[Kommunens navn]
som Behandlingsansvarlig

og

Arbeids- og velferdsetaten (NAV)
som Databehandler

Sted og dato: _____

For Behandlingsansvarlig

_____
Behandlingsansvarlig kommune

For Databehandler

_____
Arbeids- og velferdsdirektoratet

Avtalen undertegnes i to eksemplarer, ett til hver part.

INNHOLDSFORTEGNELSE:

1 FORMÅLET MED DENNE DATABEHANDLERAVTALEN

1. Databehandleravtalens hensikt er å regulere rettigheter og plikter i henhold til Europaparlamentets- og rådsforordning (EU) 2016 av 27. april 2016 og lov om behandling av personopplysninger (LOV-2018-06-15-38).

2. Databehandleravtalen regulerer Databehandlers Behandling av Personopplysninger på vegne av Behandlingsansvarlig.
3.
4. Databehandleravtalen har tre vedlegg. Vedleggene er en del av Databehandleravtalen. I tilfelle uoverensstemmelse mellom Databehandleravtalen og vedleggene, skal vedleggene gis forrang.

5. Vedlegg 1 inneholder en beskrivelse av Behandlingens omfang, formål, art og hensikt, type Personopplysninger, kategorier av registrerte og varighet av Behandlingen.

6. Vedlegg 2 inneholder en beskrivelse av tekniske og organisatoriske sikkerhetstiltak.

7. Vedlegg 3 inneholder en oversikt over godkjente Underdatabehandlere.

2 DEFINISJONER

I Databehandleravtalen skal følgende ord og uttrykk ha denne betydning:

1. «**Personopplysninger»**: Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»). En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en eller flere identifikatorer. Slike identifikatorer kan f.eks. være et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet, se artikkel 4 nr. 1.

2. **«Behandling»:** Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Det omfatter også tilgang til å se på personopplysningene, aksessere, samt aksessering fra annen lokasjon (fjernaksess), og eller mulighet til å aksessere personopplysninger, selv om denne muligheten ikke faktisk benyttes, både fra fjern og nær lokasjon. Se artikkel 4 nr. 2.

3. **«Brudd på personopplysningssikkerheten»:** Brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet, se artikkel 4 nr. 12.

4. «**Underdatabehandler»**: En annen databehandler eller flere (underleverandører) som Databehandler engasjerer for å utføre spesifikke Behandlinger på vegne av Behandlingsansvarlig.

5. «**GDPR»**: General Data Protection Regulation. Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

6. **«Gjeldende personvernregler»**: Til enhver tid gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR.

7. «**Tredjestat»**: Et land utenfor EØS.

For øvrig skal ord og uttrykk ha samme mening som de er tillagt i GDPR.

3 OMFANG AV BEHANDLINGEN

1. Databehandleravtalen gjelder alle Personopplysninger som Databehandler skal behandle på vegne av Behandlingsansvarlig, f.eks. Personopplysninger som Databehandler har mottatt, er gitt tilgang til eller har generert i forbindelse med chat for sosiale tjenester.

2. Behandlingens omfang, formål, art og hensikt, type Personopplysninger, kategorier av registrerte og varighet av Behandlingen fremgår av Vedlegg 1.

3. Databehandler har ikke selvstendig råderett over Personopplysningene og kan ikke bruke opplysningene til andre formål enn det som fremgår av Vedlegg 1, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som Databehandleren er underlagt. I så fall skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før Behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning. Databehandleren skal ellers behandle Personopplysningene i samsvar med Behandlingsansvarliges dokumenterte instrukser.

4 GENERELLE PLIKTER

1. Databehandler plikter å utføre Behandlingen av Personopplysningene i samsvar med krav som stilles til databehandlere etter Gjeldende personvernregler.

2. Databehandler skal omgående varsle Behandlingsansvarlig skriftlig hvis Databehandler har rimelig grunn til å tro at:

   (i) en instruks fra Behandlingsansvarlig kan medføre at Databehandler bryter med Gjeldende personvernregler, eller
   (ii) gjeldende rett i EØS-området krever at Databehandler behandler Personopplysninger utover omfanget av Behandlingsansvarliges dokumenterte instrukser.

   I tilfelle av (i) eller (ii) skal Partene diskutere hvordan problemet kan løses uten at de registrertes rettigheter blir krenket.

3. Databehandler skal umiddelbart varsle Behandlingsansvarlig hvis den mottar forespørsel fra en myndighet om å utlevere Personopplysninger som er behandlet under Databehandleravtalen. Med mindre loven krever det, skal Databehandler ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra Behandlingsansvarlig.

4. Hvis Databehandler er underlagt godkjente atferdsnormer etter GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme etter GDPR artikkel 42, garanterer Databehandler at den vil etterleve slike atferdsnormer eller sertifiseringsmekanismer.

5. Dersom Databehandler er underlagt plikt om protokollføring som fremgår av GDPR artikkel 30 skal Databehandler føre skriftlig protokoll over alle kategorier av Behandlinger som utøves på vegne av Behandlingsansvarlig.

5 BISTAND TIL BEHANDLINGSANSVARLIG

1. Databehandler plikter å bistå Behandlingsansvarlig ved oppfyllelse av registrertes rettigheter etter GDPR kapittel III.

2. Databehandleren skal bistå Behandlingsansvarlig med forpliktelsene etter GDPR artikkel 32 til 36, herunder Behandlingsansvarliges forpliktelser til å gjennomføre tekniske og organisatoriske sikkerhetstiltak, å gi melding til registrerte og Datatilsynet om Brudd på personopplysningssikkerhet, vurdering av personvernkonsekvenser samt forhåndsdrøftinger med Datatilsynet.

3. Ved behov for bistand som nevnt i dette punkt 5 skal Behandlingsansvarlig sende en skriftlig henvendelse til Databehandler.

4. Databehandler skal umiddelbart videresende til Behandlingsansvarlig forespørsler eller klager som Databehandler eventuelt mottar fra den registrerte.

TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

1. Databehandler skal gjennomføre egnede tekniske, fysiske og organisatoriske sikkerhetstiltak for å beskytte Personopplysninger som omfattes av Databehandleravtalen mot utilsiktet eller ulovlig tilintetgjøring, tap, endring og ikke-autorisert utlevering eller tilgang. Databehandleren skal som et minimum gjennomføre de tiltakene som er påkrevd i henhold til GDPR artikkel 32, samt de tiltak som er angitt eller referert til i Vedlegg 2.

2. I henhold til GDPR artikkel 32 skal Databehandleren – uavhengig av Behandlingsansvarlig – også vurdere risikoene som Behandlingen utgjør for fysiske personers rettigheter og gjennomføre tiltak for å imøtegå disse risikoene. I forbindelse med denne vurderingen, skal Behandlingsansvarlig stille nødvendig informasjon til rådighet for Databehandleren som gjør vedkommende i stand til at identifisere og vurdere risikoene.

3. Databehandler skal ikke utlevere Personopplysninger til tredjeparter uten skriftlig forhåndsgodkjenning fra Behandlingsansvarlig. Unntak gjelder for overføring til eventuelle godkjente Underdatabehandlere (se avtalens punkt 8) når de har behov for Personopplysningene for å kunne utføre sine oppgaver.

4. Databehandler skal sikre at kun de personer som er autorisert til å behandle Personopplysninger, har tilgang til Personopplysningene som behandles på vegne av Behandlingsansvarlig.

6 TAUSHETSPLIKT

1. Databehandlers ansatte og andre som opptrer på Databehandlers vegne, har taushetsplikt om informasjon og Personopplysninger som vedkommende får tilgang til etter Databehandleravtalen. Taushetsplikten omfatter også ansatte hos Underdatabehandler som utfører oppdrag for Databehandler for å kunne levere tjenesten.

2. Ansatte og andre hos Databehandler pålegges taushetsplikt etter reglene i arbeids- og velferdsforvaltningsloven § 7 og sosialtjenesteloven § 44 jf. forvaltningsloven §§ 13 til 13 e. Taushetsplikten omfatter også opplysninger om fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted, jf. arbeids- og velferdsforvaltningsloven § 7, første ledd. NAVs taushetsplikterklæring skal undertegnes.

3. Taushetsplikten gjelder også etter Databehandleravtalens opphør. Ansatte og andre som fratrer sin tjeneste hos Databehandler skal pålegges taushet også etter fratredelse om forhold som nevnt ovenfor.

7 BRUK AV UNDERDATABEHANDLERE

1. Databehandler kan kun engasjere Underdatabehandlere etter forutgående skriftlig tillatelse fra Behandlingsansvarlig. Godkjente Underdatabehandlere er oppført i Vedlegg 3. Undertegnelse av nærværende databehandleravtale regnes for slik tillatelse for de underdatabehandlere som ved undertegnelsen er oppført i Vedlegg 3.

2. Databehandler skal kun engasjere Underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at Behandlingen oppfyller kravene etter Gjeldende personvernregler. Databehandler skal gjennomføre kontroller av Underdatabehandlere for å verifisere deres databeskyttelsesnivå. Databehandler skal kunne fremlegge rapporter fra slik kontroller for Behandlingsansvarlig.

3. Databehandler plikter å inngå skriftlig avtale med hver Underdatabehandler som regulerer Underdatabehandlers Behandling av Personopplysninger og pålegges å ivareta alle plikter med hensyn til vern av Personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen. Databehandler plikter å forelegge disse avtalene for Behandlingsansvarlig etter forespørsel.

4. Databehandler har fullt ansvar for Underdatabehandlers utførelse av sine forpliktelser på samme måte som om Databehandler selv sto for utførelsen.

5. Samtlige som på vegne av Databehandler utfører oppdrag der Behandling av de aktuelle Personopplysningene inngår, skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser og oppfylle disse.

8 OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJESTAT

1. Databehandler kan kun overføre Personopplysninger til en Tredjestat eller en internasjonal organisasjon etter dokumenterte instrukser fra Behandlingsansvarlig. Databehandler skal i den forbindelse også dokumentere gyldig overføringsgrunnlag.

2. Unntak kan skje dersom det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandler underrette Behandlingsansvarlig om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette Behandlingsansvarlig så snart dette er tillatt).

9 MELDING OM BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

1. Databehandler skal gi skriftlig melding til Behandlingsansvarlig ved Brudd på personopplysningssikkerheten, som sannsynligvis vil medføre en risiko for fysiske personers rettigheter og friheter. Samt bistå Behandlingsansvarlig med det som er nødvendig for at Behandlingsansvarlig skal kunne gi slik melding som nevnt i punkt 2 og 3 nedenfor.
   2. Melding skal gis uten unødvendig forsinkelse og senest innen 24 timer etter at Databehandler ble oppmerksom på bruddet, slik at Behandlingsansvarlig har mulighet til å melde bruddet til Datatilsynet innenfor tidsfristen på 72 timer.

3. Melding om Brudd på personopplysningssikkerheten bør inneholde en beskrivelse av:
   a. arten av bruddet, herunder kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt,
   b. de berørte registrertes identitet,
   c. navn og kontaktinformasjon til Personvernombudet eller et annet kontaktpunkt hos Databehandler for ytterligere innhenting av informasjon,
   d. de sannsynlige konsekvensene av Bruddet på personopplysningssikkerheten,
   e. tiltak som er truffet eller foreslått for å håndtere Bruddet på personopplysningssikkerheten, herunder tiltak for å redusere eventuelle skadevirkninger,
   f. annen informasjon som kreves for at Behandlingsansvarlig kan overholde Gjeldende personvernregler.

   Informasjonen som nevnt i bokstav a-f skal gis uten ugrunnet opphold, men den kan gis trinnvis i den grad det er nødvendig.

   Databehandler skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e ovenfor. I tillegg skal Databehandler gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende Brudd på personopplysningssikkerheten. Databehandler skal, så langt det er mulig, rådføre seg med Behandlingsansvarlig om de tiltak som skal gjennomføres samt overveie innspill fra Behandlingsansvarlig i den forbindelse.

4. Kun Behandlingsansvarlig har rett til å rapportere til Datatilsynet og til de berørte registrerte om Brudd på personopplysningssikkerheten.

10 REVISJON

1. Databehandler skal dokumentere og gjøre tilgjengelig for Behandlingsansvarlig, informasjon som er nødvendig for å påvise etterlevelse av Databehandleravtalen og Gjeldende personvernregler.

2. Databehandler skal muliggjøre og bidra ved revisjoner som utføres av Behandlingsansvarlig eller av en uavhengig tredjepart med fullmakt fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

3. Databehandleren skal foreta jevnlige revisjoner av sine Behandlinger. Dette kan Databehandler gjøre på egen hånd eller via en uavhengig tredjepart med fullmakt fra Databehandler. Behandlingsansvarlig skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.

4. Dersom en revisjon avdekker avvik fra forpliktelsene i Databehandleravtalen, skal Databehandler så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandler gjør det samme). Behandlingsansvarlig kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet. Ved særlig alvorlige brudd kan Behandlingsansvarlig kreve at Behandlingen stoppes og at Databehandleravtalen termineres.

11 VARIGHET OG OPPHØR

1. Databehandleravtalen gjelder fra den er signert med begge Parters underskrift og gjelder så lenge Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig.

2. Behandlingsansvarlig kan ved brudd på Databehandleravtalen eller bestemmelsene i Gjeldende personvernregler pålegge Databehandler å stoppe den videre Behandlingen av Personopplysningene med øyeblikkelig virkning.

3. Ved opphør av Databehandleravtalen plikter Databehandler å slette eller tilbakelevere alle Personopplysninger som forvaltes på vegne av Behandlingsansvarlig og som omfattes av Databehandleravtalen. Dette gjelder også eventuelle sikkerhetskopier. Behandlingsansvarlig bestemmer hvordan tilbakelevering av Personopplysninger skal skje, herunder hvilket format som skal benyttes.

4. Databehandler skal skriftlig bekrefte og dokumentere at sletting er foretatt. Bekreftelsen skal gis innen 14 dager etter at sletting er gjennomført i henhold til vedlegg 1.

12 LOVVALG OG VERNETING

Databehandleravtalen er underlagt norsk rett og Partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av Databehandleravtalen.

13 KONTAKTPERSONER

Alle meddelelser vedrørende Databehandleravtalen rettes skriftlig og adressert til følgende kontaktpersoner:

Hos Behandlingsansvarlig (kommunen):	Hos Databehandler (NAV):
Navn	Navn
Stilling	Stilling
e-post	e-post

14 VEDLEGG 1 DATABEHANDLINGENS OMFANG

Behandlingens formål
Formålet med behandlingen er at Arbeids- og velferdsdirektoratet, ved NAV kontaktsenter (NKS), kan bruke chat-tjenester til skriftlig veiledning innenfor sosiale tjenester. Ettersom ansvaret for sosiale tjenester er tildelt kommunen, utfører NKS oppgaver i denne tjenesten på vegne av kommunen. Dette gjøres gjennom chatbot, og uinnlogget chat med veileder. Chatbot leveres av Boost Ai og uinnlogget chat benytter systemet Salesforce.

Behandlingen bidrar også til anonymisert statistikk, analyse og innsamling av data til bruk i prognostisering av volum for bemanningsplanlegging. Anonymisert chatlogg med chatbot brukes for å trene opp chatboten.

Behandlingens art og hensikt
Databehandler skal på vegne av Behandlingsansvarlig levere chat-tjenester for brukere som besvarer generelle spørsmål om sosiale tjenester gjennom en helautomatisert chatbot og uinnlogget chat med veileder. Løsningen gir innbyggere med behov for informasjon om sosiale tjenester mulighet til enkel tilgang på veiledning.

Dersom det avtales med Styringsenheten til NAV Kontaktsenter, kan chatlogger (med eventuelle personopplysninger maskert) utgis til forskningsarbeid i forbindelse med master eller doktorgradsoppgaver. Forskerne må signere taushetserklæring.

Kategorier av registrerte
Alle brukere som har eller vil kunne ha behov for informasjon om tjenester etter sosialtjenesteloven som har valgt å benytte seg av tjenesten. Som følge av at løsningen har et fritekstfelt, vil brukeren kunne oppgi opplysninger om andre, for eksempel saksbehandler.

Administratorer av Boost Ai og Salesforce i Arbeids- og velferdsdirektoratet.

NKS-veileder.

Type Personopplysninger
Bruker bes om å ikke oppgi personlig informasjon, men som følge av at løsningen har fritekstfelt kan behandlingen omfatte alle typer personopplysninger, både om brukeren selv og andre brukeren omtaler i chat.

- Telefonnummer til bruker, hvis nødvendig.
- Epost – oppgis av bruker dersom kopi av chat ønskes tilsendt.
- Navn, epostadresse, telefonnummer til administratorer og AI-trenere.
- Navn og NAV-ident på NKS-veileder.

Type særlige kategorier av Personopplysninger
Som følge av at løsningen har fritekstfelt kan behandlingen omfatte opplysninger om rase, etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, genetiske opplysninger, biometriske opplysninger, helseopplysninger, seksuelle forhold og seksuell orientering, opplysninger om straffedommer og lovovertredelser.

Spesifikke sletteregler

Chatbot
I Chatbot vil alle identifiserbare personopplysninger sladdes automatisk innen 15 minutter etter avsluttet chat, så langt systemet klarer å identifisere personopplysningene. Sladdet samtale lagres i Boost Ai i et år.

Uinnlogget chat:
Chatlogg slettes umiddelbart fra Salesforce etter endt samtale dersom samtalen gjelder sosiale tjenester. En kopi av denne sendes automatisk til Boost Ai, men blir slettet derifra innen 15 minutter. Chatlogger som ikke omhandler sosiale tjenester slettes etter 15 dager.

Navn, epost og eventuelt telefonnummer til administratorer og AI-trenere, er lagret i brukerdatabasen til Boost Ai og i Salesforce frem til vedkommende slutter å være administrator eller AI-trener.

Bistand til Behandlingsansvarlig
I den grad det er mulig skal Databehandler bistå med å oppfylle følgende av de registrertes rettigheter på vegne av Behandlingsansvarlig:

- Retten til informasjon ved innsamling av personopplysninger fra den registrerte
- Retten til informasjon hvis opplysningene innhentes fra andre enn den registrerte
- Retten til å kreve innsyn i egne personopplysninger
- Retten til å kreve korrigeringer eller sletting av egne personopplysninger
- Retten til å kreve at behandlingen av egne personopplysninger begrenses
- Retten til innsigelse
- Retten til å motsette seg automatiske avgjørelser inkludert profilering

15 VEDLEGG 2 TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Databehandler skal som et minimum gjennomføre alle de tiltak som er angitt eller henvist til nedenfor. Databehandler kan ikke uten skriftlig samtykke fra Behandlingsansvarlig gjøre endringer i disse tiltakene som reduserer graden av datasikkerhet. Databehandler skal kontinuerlig arbeide for å forbedre sikkerhetstiltakene og sørge for at de oppdateres i takt med den teknologiske utviklingen.

Pseudonymiseringstiltak
Chatlogg med chatbot lagres inntil ett år i Boost Ai for å trene opp chatboten. Hvert kvarter kjøres en prosess som går igjennom chatloggene og maskerer alle gjenkjennbare persondata. Navn blir erstattet med <name>, nummer blir erstattet med <number>, epostadresser blir erstattet med <email>. Erstatningen er permanent, og kan ikke endres tilbake (opplysningene er anonymisert).

Krypteringstiltak
All data krypteres. Boost Ai benytter seg av Amazon Web Services Cloud. Detaljert informasjon om løsningen kan leses her: https://aws.amazon.com/service-terms/
Ansvarsmodell er tilgjengelig her: https://aws.amazon.com/compliance/shared-responsibility-model/

Alle data som overføres gjennom internett bruker SSL/TLS sertifikater for å etablere HTTPS-koblinger.

Salesforce bruker Salesforce Shield Platform Encryption. Detaljer kan leses her: https://www.salesforce.com/content/dam/web/en_us/www/documents/reports/wp-platform-encryption-architecture.pdf

Tiltak for å sikre Personopplysningenes fortrolighet (konfidensialitet)
Tilgang til chatloggene i Boost Ai er begrenset til systemadministratorer og AI-trenerne som jobber med å lære opp chatroboten.
Informasjon om administratorer i Boost Ai, inkludert passord, er lagret i et IAM-system i databasen. Passord er lagret som en hashed verdi og bruker salt for å sikre en sikker enveis-algoritme.

Chatloggene i Salesforce med informasjon om sosiale tjenester slettes umiddelbart etter at samtalen er avsluttet. Det vil si ingen har mulighet til å se denne i ettertid. Tilgang til tilgjengelige chatlogger i Salesforce er begrenset til systemadministratorer i NAV.

Tiltak for å sikre Personopplysningenes integritet
Eventuelle gjenkjennbare personopplysninger som oppgis i chat blir slettet så snart som teknisk mulig.

Tiltak for å sikre tilgjengeligheten til Personopplysningene
Eventuelle gjenkjennbare personopplysninger som oppgis i chat blir slettet så snart som teknisk mulig.

Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene
Databasen til Boost Ai tas backup av daglig, og disse backupene lagres i Amazon Web Services i 30 dager.

Boost Ai bruker Elastic Computer Cloud (EC2) som har autoskalering. Det vil si at om en instans går ned grunnet eksempelvis hardwarefeil, så brukes en AMI til å starte opp en ny instans for å kompansere. Databasene er konfigurert med Multi-AZ. Ved store kritiske feil startes opp en sekundær datahall som inneholder backup av løsningen inntil primærdatahallen er operativ igjen.

NAV benytter Salesforce datasenter i Frankfurt og Paris. Det er sanntids replikering mellom datasentrene og det tas backup daglig av begge sentrene.

Tiltak for fysisk sikring av lokaler hvor data behandles
All data i Boost Ai lagres i skyløsning. Spesifikasjoner for NAVs egne virtuelle server (Amazon Private Virtual Cloud) er tilgjengelig her:
https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

Ved behov for support fra Amazon Web Services benytter Boost Ai regionale tjenester for support i Irland.

Systemadministratorer og AI-trenere som har tilgang til data, må være pålogget et NAV-nett, altså være til stede på en NAV-eid lokasjon, eller logge seg på via NAVs mobilitetsløsning. Dette sikres ved IP whitelisting. Innlogging har 2-faktors autentisering.

Alle data i forbindelse med chatbot lagres av underleverandør i Amazon Web Services. Datasenteret til AWS har ISO 27001 sertifisering og har årlig SOC 1 testing. De er blitt evaluert til å være på DIACAP Level 2 for DoD-systemer.

Sikkerhetserklæringen til Salesforce kan leses her:
https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf

NKS har ingen supportavtale med Salesforce, det vil si at ansatte i Salesforce ikke har i tilgang til NAVs data.

Testdata
Boost Ai har avtalefestet at de ikke skal benytte NAVs data ovenfor sine andre kunder, uten spesifikk tillatelse fra NAV.

Andre datasikkerhetstiltak
Ikke relevant.

16 VEDLEGG 3 GODKJENTE UNDERDATABEHANDLERE

Organisatorisk struktur
NKS benytter seg av Salesforce og Boost Ai, som leveres gjennom underdatabehandlerne. NKS' underdatabehandlere er Sopra Steria, som leverer Salesforce, og Telenor, som gjennom sin underdatabehandler Netnordic, leverer Boost Ai.

Særskilte begrensninger knyttet til eksisterende avtaleforhold med leverandører av Chat og Chatbot
NKS har gjennom databehandleravtale og leveranseavtale med Sopria Steria, og videre gjennom Sopria Sterias avtaler med Salesforce, gitte rammer for sitt handlingsrom. NKS' oppfølging av nærværende avtale begrenses følgelig til nevnte handlingsrom.

NKS har gjennom databehandleravtale og leveranseavtale med Telenor, og videre gjennom Telenors eventuelle avtaler med NetNordic og Boost Ai, gitte rammer for sitt handlingsrom. NKS' oppfølging av nærværende avtale begrenses følgelig til nevnte handlingsrom. Relasjonen til Boost Ai, blant annet vedrørende regulering av Boost Ai sitt forhold til tredjeland, er under vurdering av Arbeids- og velferdsdirektoratet.

Nærværende avtale er tilstrebet å reflektere NKS' reelle handlingsrom, men grunnet avtalestrukturenes kompleksitet, kan avvik forekomme, for eksempel vedrørende anledningen til å kreve revisjoner fra underdatabehandler.

Liste over underdatabehandlere mv

Selskapets navn	Selskapets adresse	Behandlingssted	Beskrivelse av hvilken type Behandling
Sopra Steria AS	Biskop Gunnerus' gate 14A 0185 OSLO	Personopplysningene behandles av Sopra Steria sin underleverandør, Salesforce, se under.	Dialogløsning og relasjonshåndtering
Salesforce (underdatabehandler for Sopra Steria AS)	415 Mission ST 3rd Floor, San Francisco, California, USA	Frankfurt og Paris	CRM-tjenester og lagring av chatlogg i sky.
Telenor Norge AS	Snarøyveien 30 1360 FORNEBU	Personopplysningene behandles av Telenor og NetNordic AS sin underleverandør, Boots.ai, se under.	Produksjonsstyring og trafikkflyt av henvendelser til NKS
NetNordic AS (underdatabehandler for Telenor Norge AS)	Vollsveien 2B, 1366 Lysaker	EU/EØS	Løsningsintegrator
Boost Ai AS (underdatabehandler for NetNordic AS)	Grenseveien 21, 4313 Sandnes	Irland	Chatbottjenester og lagring av chatlogg i sky