Databehandleravtale etter personopplysningsloven m.m

Databehandleravtale

I henhold til Lov om behandling av personopplysninger (Personopplysningsloven) av 2018.06.15.

Avtalen omhandler også håndtering av taushetsbelagt informasjon og data.

mellom

Kunde (Virksomhetsnavn)

HMS-Tjenesten AS

.....

Behandlingsansvarlig

og

Extend AS

.....

Databehandler

1 Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Lov om behandling av personopplysninger (Personopplysningsloven) av 2018.06.15 og EØS-avtalen vedlegg XI nr. 5e (forordning (EU) 2016/679) om vern av fysiske personer i forbindelse med behandling av personopplysninger.

Avtalen skal sikre at personopplysninger om de registrerte, ikke brukes urettmessig eller kommer uberettigede i hende.

Videre regulerer avtalen partenes rettigheter og plikter i forhold til behandling av data og informasjon som er underlagt taushetsplikt i medhold av lov eller avtale.

Avtalen regulerer Databehandlers bruk av personopplysninger og taushetsbelagt informasjon på vegne av den Behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

2 Omfanget av behandlingen

2.1 Kategorier av registrerte personer som som behandles iht. denne databehandleravtalen

Må avgrenses av behandlingsansvarlig (kunde). Kryss av i relevante bokser under:

☒ Ansatte hos behandlingsansvarlig

☒ Kunder, klienter, pasienter

☒ Samarbeidspartnere, leverandører

☐ Andre (spesfiser her eller i eget vedlegg):

2.2 Typer personopplysninger og taushetsbelagt informasjon som behandles iht. denne databehandleravtalen

Må avgrenses av behandlingsansvarlig (kunde). Kryss av i relevante bokser under:

☒ **Kontaktinformasjon**
Eksempler: Navn, Telefonnummer, E-postadresse, Arbeidsgiver

☒ **Legitimasjon / ID**
Eksempler: Fødselsnummer, Legitimasjon, Kopi av pass, førerkort

☐ **Adferdsmønster**
Eksempler: Hva og hvor du handler, hva du gjør på fritida, hvor du beveger deg, hva du søker opp på internett, etc.

☐ **Sensitiv informasjon**
Eksempler: Helseopplysninger, etnisitet, livssyn, politisk oppfatning, seksuelle forhold, rulleblad, etc.

2.3 Behandlingsoperasjoner som omfattes av denne databehandleravtalen

Behandlingen av personopplysninger som databehandleren gjør på vegne av den behandlingsansvarlige avhenger av type installasjonsavtale. Kryss av under:

☐ Lokal installasjon hos kunde

- å stille hele eller deler av datasystemet EQS til rådighet, samt å utføre, og/eller bistå behandlingsansvarlig (kunde) med å utføre nødvendig vedlikehold,oppdatering, feilretting og tilpasning av systemet
- operasjoner knyttet til innhenting, registrering, lagring, utlevering eller sletting av personopplysninger omfattes IKKE av denne databehandleravtalen

☒ Installasjon på server som driftes av Extend AS (SaaS)

- å stille hele eller deler av datasystemet EQS til rådighet, samt å utføre, og/eller bistå behandlingsansvarlig (kunde) med å utføre nødvendig vedlikehold,oppdatering, feilretting og tilpasning av systemet
- lagring, sletting og utlevering til Behandlingsansvarlig og i enkelte tilfeller også kobling av opplysninger/data

Databehandler har ikke råderett over personopplysningene og den taushetsbelagte informasjonen, og kan dermed heller ikke behandle disse til egne formål. Det er kun den Behandlingsansvarliges

formål som skal ligge til grunn for enhver behandling. Opplysningene kan kun utleveres til Behandlingsansvarlig og den/de han skriftlig bemyndiger som mottaker.

2.4 Særlig om taushetsbelagt informasjon

Denne bestemmelsen gjelder alle data som er å betrakte som taushetsbelagte, med mindre annet uttrykkelig fremkommer.

Databehandler er ansvarlig for å sikre at taushetsbelagt informasjon kan behandles i henhold til de retningslinjene i personopplysningslovgivningen som gjelder for behandling av sensitive personopplysninger, så langt dette passer.

3 Behandlingsansvarlig sine plikter

Den behandlingsansvarlige er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven.

Den behandlingsansvarlige har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen.

Den behandlingsansvarlige er ansvarlig for å kreve revisjon av denne databehandleravtalen dersom endringer i avgrensning av omfang (punkt 2) gjør dette påkrevd.

4 Databehandlers plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som Behandlingsansvarlig til enhver tid har bestemt at skal gjelde.

Databehandler plikter å bistå Behandlingsansvarlig, slik at Behandlingsansvarlig kan oppfylle de krav som fremkommer i personopplysningsloven med forskrifter, slik disse fremkommer til enhver tid.

Databehandleren skal ha et styringssystem som ivaretar informasjonssikkerheten i tjenesten og som dokumenterer Databehandlerens rutiner og tiltak for intern kontroll. Databehandler plikter å gi Behandlingsansvarlig tilgang til sine system og sin sikkerhetsdokumentasjon.

Databehandler plikter å gi nødvendig bistand til slik tilgang/slikt innsyn.

Databehandler har taushetsplikt om dokumentasjon, personopplysninger, annen taushetsbelagt informasjon og annen informasjon av betydning for informasjonssikkerheten som Databehandler får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

Databehandleren skal sikre at kun autoriserte personer har tilgang til opplysningene, og at databehandleren fratar tilgangen dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder for personen.

Databehandleren skal kun autorisere personer som av nødvendige grunner må ha tilgang til personopplysningene.

Databehandleren skal, etter anmodning fra den behandlingsansvarlige, kunne påvise at de autoriserte personene er underlagt fortrolighet eller taushetsplikt - for eksempel ved dokumentasjon.

4.1 Overføring av data til utlandet

Personopplysninger og andre taushetsbelagte opplysninger kan ikke uten skriftlig godkjennelse overføres til land utenfor EØS. Denne begrensningen gjelder også overføring til servicesenter eller andre funksjoner som ligger utenfor EØS-området eller utenfor de EU-godkjente mottakerstater. Begrensningen innebærer også at opplysningene ikke skal kunne aksesseres av personer i land utenfor EØS.

4.2 Underrettelsesansvar ved brudd på personopplysningssikkerheten

Databehandleren skal straks underrette den behandlingsansvarlige dersom det har skjedd eller skjer et brudd på personopplysningssikkerheten.

Dersom bruddet medfører en risiko for de registrertes rettigheter og friheter, må varselet til den behandlingsansvarlige inneholde den informasjonen som kreves for at den behandlingsansvarlige skal kunne gi en utførlig beskrivelse av bruddet til tilsynsmyndigheten.

Dersom bruddet medfører at den behandlingsansvarlige må varsle de registrerte, skal databehandleren gi den informasjonen som kreves for at den behandlingsansvarlige kan ivareta plikten til å gi slik underretning.

5 Bruk av underleverandør

Dersom Databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos Databehandler forblir Databehandler ansvarlig for deres behandling av personopplysninger og andre taushetsbelagte opplysninger.

Ved bruk av underleverandør blir også underleverandør å anse som Databehandler etter denne avtalen.

Oversikt over aktuelle underleverandører og tredjeparter/samarbeidspartnere ved avtalene oppstart, og som er godkjent av Behandlingsansvarlig, er gitt i tabell 1 nedenfor. Databehandleren plikter fortløpende å føre en oversikt over alle underleverandører / tredjeparter/samarbeidspartnere som benyttes i avtalen og fremlegge denne for Behandlingsansvarlig på begjæring.

Navn:	Org.nr.:	Leveranseområde
Itsjefen AS	980572714 MVA	Datasenter, serverdrift

Tabell 1. Oversikt over Databehandlers underleverandører og tredjeparter/samarbeidspartnere

Databehandleren har den behandlingsansvarliges generelle godkjennelse til å bruke andre databehandlere. Databehandleren må likevel underrette den behandlingsansvarlige ved eventuelle

planer om å skifte ut eller bruke nye databehandlere. Den behandlingsansvarlige må motta en slik underretning minimum 4 uker før endringen trer i kraft. Den behandlingsansvarlige har rett til å motsette seg endringene, og skal meddele databehandleren om dette senest 2 uker etter underretningen er mottatt.

6 Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter Lov om behandling av personopplysninger (Personopplysningsloven) av 2018.06.15 og EØS-avtalen vedlegg XI nr. 5e (forordning (EU) 2016/679) om vern av fysiske personer i forbindelse med behandling av personopplysninger..

Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene.

Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel. Kravet til dokumentasjon av rutiner og andre tiltak gjelder også for underleverandører og andre tredjeparter/samarbeidspartnere som Databehandler måtte benytte.

Databehandleren skal straks underrette den behandlingsansvarlige dersom det har skjedd eller skjer et brudd på personopplysningssikkerheten.

Dersom bruddet medfører en risiko for de registrertes rettigheter og friheter, skal varselet til den behandlingsansvarlige inneholde den informasjonen som kreves for at den behandlingsansvarlige skal kunne gi en utførlig beskrivelse av bruddet til tilsynsmyndigheten.

Dersom bruddet medfører at den behandlingsansvarlige må varsle de registrerte , skal databehandleren gi den informasjonen som kreves for at den behandlingsansvarlige kan ivareta plikten til å gi slik underretning på en tydelig måte.

Avviksmelding skal skje ved at Databehandler melder avviket til Behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet.

7 Sikkerhetsrevisjoner

Behandlingsansvarlig skal avtale med Databehandler at det skal gjennomføres sikkerhetsrevisjoner jevnlig for systemer og lignende som omfattes av denne avtalen. Revisjonen skal også omfatte eventuelle underleverandører og tredjeparter/samarbeidspartnere.

Sikkerhetsrevisjon kan omfatte gjennomgang av rutiner, stikkprøvekontroller, vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Revisjonen kan også omfatte mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik. Resultatet fra sikkerhetsrevisjon skal dokumenteres og legges frem for den Behandlingsansvarlige.

Avdekker revisjonen avvik i forhold til forsvarlig informasjonssikkerhet og gjeldende norsk rett, plikter Databehandleren å utbedre disse snares.

8 Avtalens varighet

Avtalen gjelder så lenge Databehandler og dennes underleverandører eller tredjeparter/samarbeidspartnere behandler personopplysninger og andre taushetsbelagte opplysninger på vegne av Behandlingsansvarlig. Den gjelder også for eventuelle personopplysninger og andre taushetsbelagte opplysninger som måtte forefinnes hos Databehandler etter avtalens opphør.

Ved brudd på denne avtale eller personopplysningsloven med forskrifter, kan Behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

9 Ved opphør av avtalen

Ved opphør av denne avtalen plikter Databehandler å tilbakelevere alle personopplysninger og andre taushetsbelagte opplysninger som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av denne avtalen. Opplysningene må overføres på et medium og med tilhørende programvare som gjør det mulig å lese av dataene.

Databehandler skal foreta sikker sletting eller forsvarlig destruering av alle dokumenter, data, disketter, cd-er mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Databehandler skal skriftlig dokumentere at sikker sletting og/eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Dersom Databehandler benytter underleverandør/andre tredjeparter/samarbeidspartnere er Databehandler ansvarlig for at underleverandør/andre tredjeparter/samarbeidspartnere tilsvarende tilbakeleverer til Behandlingsansvarlig alle personopplysninger og andre taushetsbelagte opplysninger som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av denne avtalen, samt sletter eller forsvarlig destruerer alle dokumenter, data, disketter, cd-er, sikkerhetskopier mv, som inneholder opplysninger som omfattes av avtalen, jf. beskrivelsen ovenfor.

10 Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til:

Behandlingsansvarlig (e-postadresse): elisabeth@hms-tjenesten.no

Databehandler (e-postadresse): kjell@extend.no

11 Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Trondheim tingrett som verneting. Dette gjelder også etter opphør av avtalen.

***

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Trondheim, 1/7-18

Behandlingsansvarlig	Databehandler
Elisabeth Lund	
(underskrift)	(underskrift)