DATABEHANDLERAVTALE

1. BAKGRUNN OG FORMÅL

1.1 Dette databehandlingssupplementet ("**Databehandleravtalen**") er en del av Serverdriftsavtale ("**Hovedavtalen**") mellom KUNDEN (den "**Behandlingsansvarlige**") og SSC Networks Norge AS ("**Databehandleren**"), der begge utgjør en "**Part**", samlet benevnt som "**Partene**".

1.2 Formålet med denne Databehandleravtalen er å fastlegge Partenes rettigheter og plikter vedrørende Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige under Hovedavtalen.

1.3 Denne Databehandleravtalen erstatter alle tidligere avtaler og bestemmelser Partene imellom hva gjelder personvern.

1.4 Med unntak for det som er spesifisert her, skal Hovedavtalens betingelser gjelde. I tilfelle uoverensstemmelse mellom Hovedavtalen og denne Databehandleravtalen når det gjelder forhold spesifikt knyttet til personvernvern, skal Databehandleravtalen gis forrang.

2. DEFINISJONER

2.1 I denne Databehandleravtalen skal følgende ord og uttrykk ha den betydning som er angitt nedenfor.

2.2 "**Gjeldende personvernregler**": Gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR (fra og med 25. mai 2018).

2.3 "**GDPR**": EUs personvernforordning 2016/679.

2.4 "**Standardklausuler**": Standardklausuler for overføring av personopplysninger til databehandlere etablert i tredjestater, etablert ved EU-kommisjonens vedtak av 5. februar 2010 og/eller som etablert av EU-kommisjonen eller en relevant tilsynsautoritet i henhold til GDPR artikkel 28(7) eller 28(8);

2.5 "**Underdatabehandler**": En annen databehandler engasjert av Databehandleren.

2.6 "**Tredjestat**": Et land utenfor EØS som EU-kommisjonen ikke har fastslått at sikrer et tilstrekkelig beskyttelsesnivå.

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

3. OMFANG

3.1 Denne Databehandleravtalen gjelder alle personopplysninger som Databehandleren har mottatt, er gitt tilgang til eller har generert i forbindelse med Hovedavtalen.

3.2 Denne Databehandleravtalen skal, så langt den passer, også omfatte behandling av data som ikke er personopplysninger som Databehandleren har mottatt, er gitt tilgang til eller har generert i forbindelse med Hovedavtalen. Begrepet "personopplysninger" skal, så langt det passer, derfor også omfatte data som ikke er personopplysninger.

3.3 Databehandlingens formål og art, typen personopplysninger som behandles, samt kategorier av registrerte fremgår av Vedlegg 1.

4. GENERELLE PLIKTER

4.1 Databehandleren garanterer å ha gjennomført egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i henhold til gjeldende personvernregler og ivaretar de registrertes rettigheter, og at disse tiltakene vil etterleves i hele avtaleperioden.

4.2 Databehandleren skal behandle personopplysningene utelukkende for det formål og innenfor det omfang som er angitt i Vedlegg 1 og for øvrig i samsvar med den Behandlingsansvarliges dokumenterte instrukser.

4.3 Databehandleren skal omgående underrette den Behandlingsansvarlige skriftlig hvis den har rimelig grunn til å tro at (i) en instruks fra den Behandlingsansvarlige kan medføre at Databehandleren bryter med gjeldende personvernlovgivning, eller (ii) gjeldende rett i EØS-området krever at Databehandleren behandler personopplysninger utover omfanget av den Behandlingsansvarliges dokumenterte instrukser, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater det). I tilfelle av (i) eller (ii) skal Partene i god tro diskutere hvordan problemet kan løses uten at det negativt påvirker vernet av de registrertes rettigheter.

5. BISTAND TIL DEN BEHANDLINGSANSVARLIGE

5.1 Databehandleren skal, ved hjelp av egnede tekniske og organisatoriske tiltak, bistå den Behandlingsansvarlige i den grad det er mulig med å oppfylle den Behandlingsansvarliges plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i GDPR kapittel 3, herunder anmodninger om informasjon, innsyn, korrigering, sletting, begrensning av behandlingen, dataportabilitet, innsigelser, og det å ikke være underlagt automatiserte individuelle avgjørelser.

5.2 Med hensyn til behandlingens art og den informasjon som er tilgjengelig for databehandleren, skal Databehandleren bistå den Behandlingsansvarlige med forpliktelsene i henhold til GDPR artikkel 32 til 36, herunder forpliktelsene til datasikkerhet (som nærmere beskrevet i punkt 6), melding om brudd på personopplysningssikkerhet (som nærmere beskrevet i punkt 9), vurdering av personvernkonsekvenser, samt forhåndsdrøftinger.

5.3 Databehandleren skal ikke kommunisere direkte med de registrerte eller med tilsynsmyndigheter med mindre dette er forhåndsgodkjent av den Behandlingsansvarlige. Databehandleren skal umiddelbart videresende til den Behandlingsansvarlige forespørsler eller klager som den eventuelt mottar fra de registrerte. Databehandleren skal også umiddelbart videresende eventuelle forespørsler fra en tilsynsmyndighet som gjelder inspeksjoner, undersøkelser, eller tilgang til eller informasjon om personopplysninger, med mindre loven forbyr det (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart loven tillater det).

5.4 Bistand etter punkt 5 skal skje mot betaling i henhold til Databehandlerens alminnelige timepriser.

6. TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

6.1 Databehandleren skal gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak for å verne personopplysningene mot utilsiktet eller ulovlig tilintetgjøring, tap, endring, 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.

6.2 Databehandleren skal ikke utlevere eller tilgjengeliggjøre personopplysninger for tredjeparter uten skriftlig forhåndsgodkjennelse fra den Behandlingsansvarlige, med unntak for eventuelt godkjente underdatabehandlere i den utstrekning de har behov for opplysningene for å kunne utføre sine oppgaver.

6.3 Databehandleren skal påse at alle personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av slike personers signerte taushetsavtaler.

7. BRUK AV UNDERDATABEHANDLERE

7.1 Den Behandlingsansvarlige tillater at Databehandleren engasjerer underdatabehandlere. På forespørsel skal den Behandlingsansvarlige motta informasjon om hvem underdatabehandlerne er, samt hvor de behandler personopplysningene. Databehandleren skal underrette den Behandlingsansvarlige om eventuelle planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere og gi den Behandlingsansvarlige rett til å motsette seg slike endringer eller å kreve at denne Databehandleravtalen opphører.

7.2 I henhold til punkt 7.1 skal Databehandleren kun engasjere underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at databehandlingen oppfyller kravene etter gjeldende personvernregler og som sikrer de registrertes personvern. Databehandleren skal gjennomføre egnede kontroller av underdatabehandlerne for å verifisere deres databeskyttelsesnivå. Databehandleren skal fremlegge rapporter fra slike kontroller for den Behandlingsansvarlige.

7.3 Databehandleren skal inngå skriftlig avtale med hver underdatabehandler som pålegger egne forpliktelser med hensyn til vern av personopplysninger. Når underdatabehandleren er engasjert for å utføre spesifikke databehandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal den Behandlingsansvarlige ved skriftlig avtale pålegge underdatabehandleren de samme forpliktelsene med hensyn til vern av personopplysninger som fastsatt i denne Databehandleravtalen. På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av avtaler med underdatabehandlere. Forretningsmessig og annen forretningssensitiv informasjon kan dog sladdes.

7.4 Databehandleren har fullt ansvar for underdatabehandlerens utførelse av sine forpliktelser.

8. INTERNASJONAL DATAOVERFØRING

8.1 Databehandleren kan kun overføre personopplysninger til en tredjestat eller en internasjonal organisasjon etter dokumenterte instrukser fra den Behandlingsansvarlige. Databehandleren kan imidlertid gjøre dette hvis det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater dette).

8.2 Dersom bruk av en godkjent underdatabehandler krever overføring av personopplysninger til en tredjestat, og slike overføringer er godkjent av den Behandlingsansvarlige, gir den Benhandlingsansvarlige Databehandleren fullmakt til å inngå standardklausuler i uendret form med underdatabehandleren på vegne av den Behandlingsansvarlige dersom dette er nødvendig for å tilfredsstille krav etter gjeldende personvernregler. Så snart en slik avtale er inngått skal underdatabehandleren fremlegge en kopi av denne for den Behandlingsansvarlige. Alle slike standardklausuler skal automatisk opphøre ved opphøret av denne Databehandleravtalen.

9. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

9.1 Databehandleren skal gi skriftlig melding til den Behandlingsansvarlige om eventuelle brudd på denne Databehandleravtalen eller personopplysningssikkerheten. Meldingen skal gis senest 36 timer etter at Databehandleren ble oppmerksom på bruddet.

9.2 Melding om brudd på personopplysningssikkerheten må minst, i den grad det er relevant:

a. beskrive arten av bruddet, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt;

b. inneholde, når det er mulig, de berørte registrertes identitet;

c. formidle navn og kontaktinformasjon til personvernrådgiveren eller et annet kontaktpunkt hos Databehandleren for ytterligere innhenting av informasjon;

d. beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;

e. beskrive de tiltak som er truffet eller foreslått for å håndtere bruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger;

f. inkludere annen informasjon som kreves for at den Behandlingsansvarlige kan overholde gjeldende personvernregler.

9.3 Databehandleren skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e. ovenfor, samt gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende brudd på personopplysningssikkerheten. Databehandleren skal tillate den Behandlingsansvarlige å undersøke, fastlegge årsaken til og å verifisere de tiltak som er gjennomført eller foreslått av den Behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten. Databehandleren skal, så langt det er mulig, rådføre seg med den Behandlingsansvarlige med hensyn til de tiltak som skal gjennomføres samt overveie innspill fra den Behandlingsansvarlige i den forbindelse.

9.4 Kun den Behandlingsansvarlige har rett til å informere den relevante tilsynsmuligheten og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandleren skal avstå fra å informere allmennheten eller tredjepart om brudd på personopplysningssikkerheten.

10. REVISJON

10.1 Databehandleren skal dokumentere, samt gjøre tilgjengelig for den Behandlingsansvarlige, informasjon som er nødvendig for å påvise etterlevelse av denne Databehandleravtalen og gjeldende personvernregler.

10.2 Databehandleren skal muliggjøre og bidra ved revisjoner av Databehandlerens behandlingsaktiviteter som utføres av den Behandlingsansvarlige eller av annen inspektør på fullmakt fra den Behandlingsansvarlige. Databehandleren skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

10.3 Databehandleren skal, på egen hånd eller via annen inspektør på fullmakt fra Databehandleren, foreta jevnlige revisjoner av sine behandlingsaktiviteter. Databehandleren skal oversende kopi av revisjonsrapporter fra slike revisjoner til den Behandlingsansvarlige. Den Behandlingsansvarlige skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.

10.4 Databehandleren skal umiddelbart varsle den Behandlingsansvarlige hvis den mottar forespørsel fra en myndighet om å utlevere personopplysninger som er behandlet under denne Databehandleravtalen. Med mindre loven krever det, skal Databehandleren ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra den Behandlingsansvarlige.

10.5 Dersom en revisjon avdekker avvik fra forpliktelsene i denne Databehandleravtalen, skal Databehandleren så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandleren gjør det samme). Den Behandlingsansvarlige kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet.

10.6 Hver av partene dekker sine egne kostnader forbundet med en revisjon.

11. ANDRE BEHANDLINGSANSVARLIGE

11.1 Databehandleren anerkjenner at personopplysningene også kan behandles på vegne av den Behandlingsansvarliges konsernselskaper/kunder/klienter. Slike andre behandlingsansvarlige har samme rettigheter som den Behandlingsansvarlige som er avtalepart, og de kan håndheve denne Databehandleravtalen som om de var avtaleparter. Slik håndheving skal imidlertid skje gjennom den Behandlingsansvarlige som er avtalepart.

11.2 Den Behandlingsansvarlige kan videresende enhver instruks fra slike andre behandlingsansvarlige, og Databehandleren skal handle i samsvar med slike instrukser som om de var den Behandlingsansvarliges egne.

11.3 Den Behandlingsansvarlige kan videresende enhver dokumentasjon og informasjon mottatt av Databehandleren til slike andre behandlingsansvarlige.

12. VARIGHET OG OPPSIGELSE

12.1 Denne Databehandleravtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige i forbindelse med Hovedavtalen.

12.2 Ved opphør eller oppsigelse av Databehandleravtalen skal Databehandleren, dersom den Behandlingsansvarlige ønsker det, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige og slette eksisterende kopier, og bekrefte overfor den Behandlingsansvarlige at dette er gjort, med mindre gjeldende rett i EØS-området krever at Databehandleren lagrer personopplysningene (i så fall skal Databehandleren besørge sikker lagring, men ikke aktivt behandle, personopplysningene, og skal slette personopplysningene så snart loven tillater dette).

[signaturfelt på neste side]

For og på vegne af den Behandlingsansvarlige:

Signatur: _____

Navn:

Dato:

For og på vegne af Databehandleren:

Signatur: _____

Navn:

Dato:

VEDLEGG 1: DATABEHANDLINGENS OMFANG

Behandlingens formål

Formålet med databehandlingen er at Databehandleren skal kunne utføre sine forpliktelser i henhold til Hovedavtalen.

Behandlingens art og hensikt

IT-drift av behandlingsansvarlig sine servere og databaseløsninger samt backup av disse.
Dette er spesifisert i avtalens kontrakt.

Kategorier av registrerte

Personer som har eller har hatt eierforhold hos den Behandlingsansvarlige eller Behandlingsansvarlige kunder.

Typen personopplysninger

Navn, adresse, mobilnummer og annen relevant informasjon som kreves i kundeapplikasjonene på server. Detaljer spesifiseres i avtalens kontrakt.

VEDLEGG 2: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Krypteringstiltak

Databehandleren krypterer data mellom servere for å hindre uautorisert tilgang til data lagret som backup - utenfor driftsservere som er sikret med verifisering og brukerinnlogging.

Tiltak for å sikre personopplysningenes tilgjengelighet, fortrolighet og integritet.

Personopplysninger behandles kun av autoriserte personer på brannmursikrede systemer med personlig innlogging og uten tilgang for uautoriserte. Den behandlingsansvarlige har ansvar for og sørger for å straks slette eller rette personopplysninger som er uriktige.

Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene

Alle personopplysninger ligger på sikrede servere med disasterplan med daglig backup enten på egen lagringsserver i eget datasenter eller til ekstern lokasjon med samme sikkerhetstiltak som hovedlokasjon. Det gjennomføres periodiske katastrofesimuleringer med tilbakestilling av servere og data ved uventet systemkrasj.

Andre datasikkerhetstiltak:

All data lagres i databehandlers egen infrastruktur i datasenter med fysisk adgangskontroll. Samme gjelder for fysisk adskilt backuplokasjon. Ingen data lagres i tredjeparts skytjenester utenfor fysisk tilgjengelighet og egen rådighet. Databehandlers infrastruktur er i Norge.
Databehandlers datanett er sikret med preferert brannmur med tilgangskontroll, kontinuerlig sikkerhetsskanning og vedlikeholdsavtaler med sikkerhetsprodukter fra brannmurleverandør. Nettet er i tillegg overvåket av databehandlerens teknikere.
Selve lokalet er fysisk sikret mot brann, strømbrudd og temperatursvingninger.