

Vedlegg 14 - Bilag til Databehandleravtale

Tilknyttet RA-26-003-GR-Velferdsteknologi - Gjøvikregionen og Hadeland

Gjøvik kommune, Gran kommune, Nordre Land kommune og Søndre Land kommune

Samt eventuelle kommuner som tiltrer rammeavtalen i henhold til avtalens opsjonsbestemmelser

DETTE DOKUMENT BESTÅR AV FØLGENDE BILAG:

BILAG A – OPPLYSNINGER OM BEHANDLINGEN

BILAG B - BETINGELSER FOR DATABEHANDLERENS BRUK AV UNDERDATABEHANDLERE

BILAG C - INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

**BILAG D - ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER
ETTER AVTALEINNGÅElsen**

Bilag A, B, C, og D til Databehandleravtalen

A.	Opplysninger om behandlingen	3
A.1	Hovedavtalen og formålet med behandlingen av personopplysninger	3
A.2	Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige.....	3
A.3	Typer av personopplysninger	4
A.4	Kategorier av registrerte	4
A.5	Varighet av behandlingen	4
B.	Betingelser for Databehandlerens bruk og endring av eventuelle Underdatabehandlere	5
B.1	Behandlingsansvarliges godkjenning av bruk av Underdatabehandlere	5
B.2	Godkjente Underdatabehandlere	6
C.	Instruks vedrørende behandling av personopplysninger	7
C.1	Behandlingens omfang og formål	7
C.2	Sikkerhet ved behandlingen	7
C.2.1	Angivelse av sikkerhetsnivå	7
C.2.2	Styringssystem for informasjonssikkerhet	7
C.3	Dokumentasjon	8
C.4	Overføring av personopplysninger - Lokasjon for behandling og tilgang	8
C.5	Rutiner for revisjon og tilsyn	8
C.6	Sletting og tilbakelevering av personopplysninger ved avtalens opphør	10
C.7	Sektorspesifikke bestemmelser om behandling av personopplysninger	10
C.8	Kontaktinformasjon.....	10
D.	Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen	12

A. OPPLYSNINGER OM BEHANDLINGEN

A.1 Hovedavtalen og formålet med behandlingen av personopplysninger

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige er knyttet til å levere tjenester som beskrevet i Hovedavtalen.

Med Hovedavtalen menes følgende avtale(r) inngått mellom partene:

SAA-R Rammeavtale for velferdsteknologiske løsninger med tilhørende avropsavtaler:

- SSA-K Kjøpsavtale
- SSA-L Løpende tjenestekjøp
- SSA-D Driftsavtale
- SSA-V Vedlikeholdsavtale

Behandlingen har følgende formål:

Levering, drift, vedlikehold, support og forvaltning av velferdsteknologiplattform og tilhørende produkter og tjenester for oppdragsgivers helse- og omsorgstjenester.

A.2 Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige omhandler (karakteren av behandlingen):

Innsamling, registrering, lagring, tilgjengeliggjøring, overføring, oppdatering, journalføring, administrasjon og sletting av personopplysninger som behandles gjennom velferdsteknologiplattformen og tilhørende løsninger.

A.3 Typer av personopplysninger

Behandlingen omfatter følgende typer av personopplysninger om de registrerte (flere valg mulig):

☒	<i>Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1): Helseopplysninger knyttet til bruk av velferdsteknologiske tjenester.</i>
☒	<i>Andre opplysninger med særlig behov for beskyttelse: Fødselsnummer, brukeridentifikatorer og opplysninger om tjenestemottak.</i>
☒	<i>Andre personopplysninger: Navn, adresse, telefonnummer, e-postadresse, pårørendeinformasjon, alarmhendelser, loggopplysninger, brukerprofiler og administrative opplysninger.</i>

A.4 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

- Brukere av kommunens helse- og omsorgstjenester
- Pårørende og verge/fullmektig der dette er registrert
- Ansatte hos oppdragsgiver med tilgang til løsningene
- Eventuelle andre kontaktpersoner registrert i løsningen

A.5 Varighet av behandlingen

Databehandlers behandling av personopplysninger under Hovedavtalen kan påbegynne når Databehandleravtalen har trådt i kraft. Behandlingen har følgende varighet (velg ett alternativ):

☒	Behandlingen er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen.
☐	Behandlingen er tidsbegrenset, og gjelder frem til <i><angi dato eller kriterium for avslutning, eksempelvis avslutningen av et prosjekt. Merk at behandlingen normalt ikke kan avslutte før Hovedavtalen utløper></i> .

Ved opphør (av avtalen eller en behandling) skal personopplysninger tilbakeleveres og slettes i samsvar med Databehandleravtalen punkt 12 og instruksjonene i Bilag C. databehandlerens bruk av underdatabehandlere

B. BETINGELSER FOR DATABEHANDLERENS BRUK OG ENDRING AV EVENTUELLE UNDERDATABEHANDLERE

B.1 Behandlingsansvarliges godkjenning av bruk av Underdatabehandlere

Ved inngåelse av Databehandleravtalen godkjenner Behandlingsansvarlig bruk av de Underdatabehandlere som er oppført i punkt B.2. Merk at også mor-, søster- og datterselskaper til Databehandleren regnes som Underdatabehandlere hvis de bidrar til leveransen og behandler personopplysninger.

For endringer i bruk av Underdatabehandlere er det i tillegg avtalt følgende:

☐	Databehandleren kan benytte Underdatabehandler som i samme konsern (mor-søster- eller datterselskap) som er etablert i et land innenfor EØS-området. Databehandleren skal på forhånd informere Behandlingsansvarlige om bruken av slik Underdatabehandler. (Dette alternativet kan kombineres med et av de andre alternativene.)
☐	Databehandler kan gjennomføre endringer i bruken av Underdatabehandlere forutsatt at den Behandlingsansvarlige underrettes og gis mulighet til å motsette seg endringene. En slik underretning skal være mottatt av Behandlingsansvarlig senest 1 måned før endringen trer i kraft, med mindre annet er avtalt skriftlig mellom partene. Merk at endringer som medfører overføring av personopplysninger til land utenfor EØS-området (Tredjestater) uansett krever skriftlig godkjenning etter Databehandleravtalens punkt 10. Hvis Behandlingsansvarlig motsetter seg endringen skal Databehandler underrettes så snart som mulig. Den behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn.
☒	Databehandler kan kun gjennomføre endringer i bruken av Underdatabehandlere etter spesifikk og forutgående skriftlig godkjenning fra Behandlingsansvarlig. Underdatabehandleren kan ikke behandle personopplysninger under Hovedavtalen før slik godkjenning er gitt. Godkjenning kan ikke nektes uten saklig grunn.

B.2 Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere:

Navn	Org.nr.	Adresse	Beskrivelse av behandling	Behandlingssted	Kontaktinformasjon	Særlige kategorier personopplysninger
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	[Angi om det behandles særlige kategorier av personopplysninger]
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	

Databehandleren kan ikke bruke den enkelte Underdatabehandleren til en annen behandling enn avtalt eller la en annen Underdatabehandler utføre den beskrevne behandlingen i andre tilfeller enn det som følger av Bilag B, punkt B.1 om skifte av Underdatabehandler.

C. INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

C.1 Behandlingens omfang og formål

Personopplysningene skal utelukkende behandles i det omfang og for de formål som er beskrevet i

- Hovedavtalen
- Databehandleravtalen med bilag

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Databehandleravtalen, og kan ikke behandle disse til egne formål.

C.2 Sikkerhet ved behandlingen

C.2.1 Angivelse av sikkerhetsnivå

Ut fra en vurdering av omfanget av personopplysninger som blir behandlet, typen opplysninger og karakteren av behandlingen er det basert på en konkret risikovurdering fastsatt at behandlingen (velg ett alternativ):

☒ Krever et høyt sikkerhetsnivå. Begrunnelse:

Behandlingen omfatter helseopplysninger og andre personopplysninger knyttet til mottakere av kommunale helse- og omsorgstjenester. Opplysningene behandles i velferdsteknologiske løsninger der krav til konfidensialitet, integritet og tilgjengelighet er særlig viktige.

☐ Ikke krever et høyt sikkerhetsnivå. Begrunnelse:

C.2.2 Styringssystem for informasjonssikkerhet

Databehandleren skal ha et egnet styringssystem for informasjonssikkerhet. Databehandleren skal etablere og forvalte tilstrekkelige sikkerhetstiltak for å ivareta informasjonssikkerheten for behandling av personopplysningene, herunder (flere valg mulig):

☒	Sikkerhetskrav som beskrevet i Hovedavtalen: <i>Kravspesifikasjonens kapittel om informasjonssikkerhet, personvern, tilgangsstyring, logging, hendelsehåndtering og beredskap.</i>
☐	Sikkerhetskrav som beskrevet nedenfor: <i><Sett inn beskrivelse av relevante sikkerhetskrav></i>

C.3 Dokumentasjon

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som fremkommer av Gjeldende personvernregler og Databehandleravtalen, herunder kravene til informasjonssikkerhet. Slik dokumentasjon skal oppbevares og ajourholdes så lenge Databehandleravtalen består, og gjøres tilgjengelig for Behandlingsansvarlig eller tilsynsmyndigheter på forespørsel.

C.4 Overføring av personopplysninger - Lokasjon for behandling og tilgang

Behandling av de personopplysninger som avtalen omfatter kan ikke uten den Behandlingsansvarliges forutgående skriftlige godkjenning utføres på eller med tilgang fra andre lokasjoner enn de som er angitt i Bilag B.2. Med lokasjon menes:

- Sted det er mulig å få tilgang til personopplysningene fra (aksessering)
- Sted hvor personopplysningene bearbeides (prosesseres)
- Sted hvor personopplysningene lagres

Begrensningen ovenfor gjelder ikke Databehandlerens mor-, søster- og datterselskaper som er etablert innenfor EØS-området. Databehandleren skal imidlertid på forespørsel fra den Behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles

C.5 Rutiner for revisjon og tilsyn

For å kontrollere etterlevelse av Gjeldende personvernregler og Databehandleravtalen er det avtalt følgende (flere valg mulig):

☒	Behandlingsansvarlig har rett til å utføre revisjon på Databehandlers forretningssted for å verifisere Databehandlers etterlevelse av sine plikter i henhold til denne Databehandleravtalen eller Gjeldende personvernregler. Slike revisjoner skal:
-------------------------------------	---

	• Gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året, med mindre sikkerhetsbrudd hos Databehandler eller andre særlige forhold gir grunn for hyppigere revisjoner; • Foregå innenfor normal arbeidstid og ikke forstyrre Databehandlers virksomhet unødvendig; • Utføres av ansatte hos Behandlingsansvarlig eller av tredjepart som er godkjent av Partene og underlagt taushetsplikt. Databehandler plikter å stille til rådighet de ressurser som med rimelighet kan kreves for å gjennomføre revisjonen. Behandlingsansvarlig skal dekke kostnader for eventuelle tredjeparter som benyttes til å gjennomføre revisjonen. For øvrig dekker Partene sine egne kostnader ved gjennomføring av revisjonen. Dersom revisjonen avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler likevel dekke Behandlingsansvarliges rimelige kostnader ved revisjonen.
☐	Databehandleren skal benytte ekstern revisor til å attestere at sikkerhetstiltak er etablert og virker etter hensikten. Slik revisjon skal: - gjennomføres én gang årlig, - utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402. - utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring Rapportene skal fremlegges for Behandlingsansvarlig på forespørsel. Databehandler skal i tillegg gi slik informasjon og bistand som er nødvendig for at Behandlingsansvarlig kan etterleve sine forpliktelser etter Gjeldende personvernregelverk.
☐	For standardiserte tredjepartstjenester som leveres av Underdatabehandler kan det fremlegges tredjepartsrevisjon forutsatt at revisjonen er gjennomført etter alminnelig anerkjente prinsipper og av sertifisert revisor.
☒	<i>Oppdragsgiver kan ved behov be om innsyn i relevante revisjonsrapporter, sertifiseringer, sikkerhetserklæringer og dokumentasjon knyttet til informasjonssikkerhet og personvern hos Databehandler og godkjente Underdatabehandlere.</i> <i>Leverandøren skal uten ugrunnet opphold oversende slik dokumentasjon når oppdragsgiver ber om dette.</i>

C.6 Sletting og tilbakelevering av personopplysninger ved avtalens opphør

Partene har avtalt følgende om sletting/tilbakelevering av personopplysninger (velg ett alternativ):

☐	Alle personopplysninger som behandles under denne Databehandleravtale skal slettes uten ugrunnet opphold og senest innen 90 kalenderdager etter opphør av Hovedavtalen. Dette samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig.
☐	Alle personopplysninger som behandles under denne Databehandleravtale, samt eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig, skal tilbakeleveres ved opphør av Hovedavtalen. Etter tilbakelevering er skjedd, plikter Databehandler å slette alle personopplysninger og annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig innen 30 kalenderdager. Tilbakelevering skal skje på følgende måte: <i>Tilbakelevering skal skje i et strukturert, alminnelig anvendt og maskinlesbart format, herunder CSV, XML eller annet avtalt format. Tilhørende dokumentasjon, metadata og nødvendige eksportbeskrivelser skal inngå.</i>
☒	Se Bilag D – Endringer og suppleringer

C.7 Sektorspesifikke bestemmelser om behandling av personopplysninger

Behandlingen skal skje i samsvar med personopplysningsloven, personvernforordningen (GDPR), pasientjournalloven, helsepersonelloven, helseregisterloven og annen relevant lovgivning som gjelder for kommunale helse- og omsorgstjenester.

C.8 Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningssikkerheten eller endring i bruk av underdatabehandlere, skal følgende kanaler benyttes:

Hos Behandlingsansvarlig

Sikkerhetsbrudd:

Telefon: [Fyll ut]

Hos Leverandøren

Sikkerhetsbrudd:

Telefon: [Fyll ut]

Bilag A, B, C, og D til Databehandleravtalen

E-post [Fyll ut]

Andre henvendelser:

Navn: [Fyll ut]

Stilling: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]

E-post [Fyll ut]

Andre henvendelser:

Navn: [Fyll ut]

Stilling: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]

D. ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER ETTER AVTALEINNGÅELEN

Endring til punkt 12 (Sletting og tilbakelevering av opplysninger) og Bilag C punkt C.6:

Bestemmelsene om sletting og tilbakelevering suppleres med følgende:

1. Dataportabilitet Oppdragsgiver skal til enhver tid kunne hente ut egne data, inkludert historiske data og tilhørende metadata, i åpne, dokumenterte og maskinlesbare formater, uten tap av informasjon, struktur eller relasjoner.
2. Unngåelse av leverandørlåsing Leverandøren skal sikre at data og funksjonalitet ikke er bundet til leverandørens løsning på en måte som hindrer eller vesentlig vanskeliggjør overgang til annen leverandør eller løsning.
3. Tilgjengeliggjøring i avtaleperioden Leverandøren skal legge til rette for løpende tilgang til data gjennom standardiserte grensesnitt (API) eller tilsvarende mekanismer der dette er relevant og forholdsmessig.
4. Avvikling og migrering Ved avtalens opphør, eller på oppdragsgivers anmodning, skal leverandøren uten ugrunnet opphold bistå med utlevering og migrering av data til ny løsning.
Slik bistand skal:
 - være inkludert i avtalens vederlag, eller prises etter avtalte timepriser
 - ikke kreve tilleggslisenser eller separate produkter
 - gjennomføres på en måte som sikrer datakvalitet og integritet
5. Dokumentasjon Leverandøren skal stille nødvendig dokumentasjon til disposisjon for muliggjøre effektiv migrering, herunder:
 - datamodeller
 - formatbeskrivelser
 - systemavhengigheter
6. Datatilgang, struktur og migreringsprosess
Leverandøren skal dokumentere hvordan data lagres og struktureres, herunder datamodeller, relasjoner og relevante avhengigheter.

Videre skal leverandøren beskrive hvordan data kan eksporteres og migreres i praksis, inkludert hvilke formater, grensesnitt (API-er) og tekniske mekanismer som benyttes.

Løsningen skal teknisk støtte effektiv dataportabilitet, og eventuelle begrensninger skal fremgå tydelig.

Leverandøren skal på forespørsel kunne redegjøre for hvordan utlevering og migrering gjennomføres i praksis, herunder ved å gi et konkret eksempel på gjennomført eller simulert overgang til annen løsning.

7. Rangordning Ved motstrid går bestemmelsene i dette bilaget foran Databehandleravtalens punkt 12 og Bilag C punkt C.6.