Databehandleravtale

I henhold til personvernforordningen Art. 28 nr. 3.

mellom

_____kommune

Org.nr.: _____

Behandlingsansvarlig

og

Digidrift as

Org.nr.: 921 903 499

Databehandler

1. Databehandleravtalens hensikt

Denne avtale, heretter omtalt som «**Databehandleravtalen**», regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig i henhold til gjeldende avtale mellom partene om drift av Orden i eget hus – i praksis, heretter omtalt som «**Avtalen**».

Databehandleravtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende og regulerer rettigheter og plikter etter den til enhver tid gjeldende personvernlovgivning, herunder

- L15.06.2018 nr. 38 Lov om behandling av personopplysninger (personopplysningsloven)
- med tilhørende forskrift
- Regulation (EU) 2016/679 (General Data Protection Regulation), her omtalt som «**Personvernforordningen**».

Det er den Behandlingsansvarlige som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Databehandleravtalen regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig.

Databehandleravtalen er ikke undergitt noen rangordning/underordningsforhold som følger av det øvrige avtaleforholdet mellom partene.

2. Formål med behandlingen

Databehandleren skal behandle de personopplysningene Databehandleren får tilgang til i sin rolle som leverandør av Orden i eget hus – i praksis, under Avtalen. Følgende behandlinger omfattes av Databehandleravtalen:

- Innsamling og registrering: Behandlingsansvarlig registrerer personopplysninger i Databehandlers system som samler inn disse opplysningene
- Sammenstilling: Databehandler systematiserer personopplysningene for å oppnå Behandlingsansvarliges formål om å drive kunnskapsbygging for å utarbeide beslutningsgrunnlag for felles prioritering av målgrupper og tiltak
- Lagring: Databehandler skal ta vare på de registrerte personopplysningene for å ivareta Behandlingsansvarliges behov for løpende tilgang til personopplysningene
- Utlevering: Databehandler gjør personopplysninger tilgjengelig til Behandlingsansvarlig til enhver tid under avtalens løpetid, i henhold til Behandlingsansvarlig sine til enhver tid gjeldende regler for utlevering, lagring og sletting

Informasjon om Behandlingsansvarliges ansatte og tilhørende metadata om deres bruksmønster av tjenesten er også underlagt Databehandleravtalens bestemmelser.

Databehandler har ikke selvstendig råderett til personopplysningene, og kan ikke behandle disse til egne formål, f.eks. i salg, markedsføring eller andre personprofileringsaktiviteter.

3. Hvilke opplysninger som behandles

Som følge av Avtalen vil Databehandleren behandle personopplysninger på vegne av den Behandlingsansvarlige. Behandlingsansvarlige angir følgende som en liste over personopplysninger som er omfattet:

Personlige identifikatorer

- Navn

Kontaktinformasjon

- Epost

Informasjon om arbeidsforhold

- Navn på arbeidsgiverkommune
- Rolle i administrasjonen av applikasjoner eller behandlinger i kommunen
- En sammenstilling av ovennevnte

4. Databehandlers plikter

Databehandleren skal følge de rutiner og instrukser for behandlingen som den Behandlingsansvarlige har bestemt skal gjelde og er underlagt den Behandlingsansvarliges instruksjonsmyndighet.

Databehandler skal uten ugrunnet opphold underrette Behandlingsansvarlig dersom Databehandleren anser at en instruks fra den Behandlingsansvarlige er i strid med gjeldende personvernregelverk. Hvis det foreligger godkjente atferdsnormer etter Personvernforordningen artikkel 40 eller godkjent sertifiseringsmekanisme etter artikkel 42, og hvor disse medfører strengere krav enn databehandleravtalens betingelser, plikter Databehandler å innrette virksomheten etter dette.

Personopplysningene skal kun benyttes av Databehandleren i forbindelse med levering av tjenesten til den Behandlingsansvarlige i henhold til Avtalen. Personopplysningene skal kun gjøres tilgjengelig for den/de av Databehandlerens ansatte som har tjenstlig behov for tilgang til personopplysningene for å kunne levere tjenesten.

Databehandlers ansatte samt innleid personell har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til gjennom tjenesten. Bestemmelsen om taushetsplikt gjelder også etter Avtalens opphør. Taushetsplikten gjelder tilsvarende for underleverandører.

Databehandleren skal bistå den Behandlingsansvarlige med ivaretakelse av rettighetene til de registrerte. Dette gjelder, men er ikke begrenset til, å gi informasjon om hvordan opplysningene behandles, håndtering av henvendelser som gjelder innsyn i egne personopplysninger og oppfyllelse av de registrertes rett til å kreve retting eller sletting av personopplysningene.

Behandlingsansvarlig har til enhver tid full rådighet over personopplysningene som behandles etter Avtalen. Databehandler skal ikke utlevere data eller personopplysninger i noen form av eget tiltak. Enhver henvendelse som rettes til Databehandler, fra andre enn Behandlingsansvarlig, om å få utskrift av rådata eller personopplysninger skal straks videreformidles til Behandlingsansvarlige som skal ha all kontakt med de registrerte. Behandlingsansvarlig vil vurdere hvorvidt opplysninger skal utleveres, og kan stille vilkår for slik utlevering.

Dersom Databehandler er underlagt plikt om protokollføring som fremgår av Personvernforordningen artikkel 30 skal Databehandler føre skriftlig protokoll over alle kategorier av behandlingsaktiviteter som utøves på vegne av Behandlingsansvarlig. Databehandler må selv undersøke om slik plikt foreligger etter artikkel 30 nr. 5.

Databehandler plikter å varsle Behandlingsansvarlig om alle forhold ved tjenesten som medfører endring i risikobildet. Hvis det er utarbeidet en servicehåndbok for tjenesten skal varslingen følge avtalte prosedyrer som er beskrevet i Servicehåndboken.

5. Den Behandlingsansvarliges plikter

Behandlingsansvarlig er ansvarlig for å sikre at all behandling av personopplysninger er forankret i et lovlig behandlingsgrunnlag og for å fastsette formålet og metoden for Databehandlers behandling av personopplysninger i henhold til Databehandleravtalen.

Behandlingsansvarlig plikter å varsle Databehandler om alle avvik som medfører risiko for de registrertes rettigheter, i den utstrekning det er nødvendig. Hvis det er utarbeidet en servicehåndbok for tjenesten skal varslingen følge avtalte prosedyrer som er beskrevet i Servicehåndboken.

6. Bruk av underdatabehandlere

Digidrift as er etablert som en forvaltningsorganisasjon for felleskomponenten Orden i eget hus i praksis og har knyttet til seg følgende underleverandører:

Telemark kompetanse as – utfører administrative oppgaver for Digidrift as herunder oppfølging og administrasjon av den enkelte bruker av løsningen Orden i eget hus. Utfører opplæringsaktiviteter for kommuner som tar i bruk løsningen.

Arkitektum as drifter løsningen teknisk i skyløsning Microsoft Azure pt.. Arkitektum har ansvar for teknisk support, brukeroppsett, feilretting og videreutvikling av løsningen. Arkitektum utfører også opplæringsaktiviteter for kommuner som tar i bruk løsningen.

Dersom underdatabehandlere benyttes i fremtiden, skal Databehandleren påse at alle underdatabehandlere er informert om og bundet av de samme kravene til informasjonssikkerhet og øvrige krav som fremgår av denne Databehandleravtalen og den til enhver tid gjeldende personvernregelverk. Eventuelle underdatabehandlere plikter å gi tilstrekkelige garantier for at det er gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller lovmessige krav.

Databehandler skal på forespørsel legge frem kopi av avtalen(e) som er inngått med underdatabehandler(ne) på forespørsel fra Behandlingsansvarlig. En slik avtale skal senest være inngått før behandlingen av opplysningene starter opp. Enhver avtale mellom Databehandleren og en underdatabehandler skal være underlagt norsk lovgivning og jurisdiksjon.

7. Overføring til land utenfor EU/EØS (tredjeland)

Personopplysninger skal ikke behandles i land som ikke er godkjent i henhold til Avtalen.

Databehandler skal ikke overføre personopplysninger uten instruks fra den Behandlingsansvarlige. Hvis utlevering kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett, som Databehandleren er underlagt, skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr en slik underretning.

8. Sikkerhet

Databehandler skal iverksette alle nødvendige tekniske og organisatoriske tiltak for å ivareta konfidensialitet, integritet og tilgjengelighet i behandlingen av personopplysninger, samt unngå at personopplysninger som Databehandleren behandler utsettes for uautorisert tilgang, spredning, endring, skade, ødeleggelse eller utilgjengelighet. Sikkerhetsnivået skal hensynta arten av personopplysninger og risiko for brudd på datasikkerhet for den registrerte.

Databehandleren skal bistå den Behandlingsansvarlige slik at vedkommende kan ivareta sitt eget ansvar for informasjonssikkerhet, avvikshåndtering og konsekvensanalyse etter Personvernforordningen artikkel 32 til 36 og den til enhver tid gjeldende personvernlovgivning.

På forespørsel fra den Behandlingsansvarlige plikter Databehandleren å bistå i dialogen med Datatilsynet der hvor personvernrisikoen, avdekket gjennom konsekvensutredninger, vanskelig lar seg håndtere på en hensiktsmessig måte.

Databehandler må ha:

- God tilgangskontroll, herunder rutiner for hvem som skal ha tilgang til opplysningene og rutiner for jevnlig evaluering av administratortilgang og andre tilganger,
- Gode internkontrollrutiner, og
- Opplæringstiltak.

Databehandler må også ha tekniske tiltak som nødvendig kryptering, logging av tilgang og bruk, nødvendig backup og redundans.

Databehandler skal kun benytte skarpe data i test og utvikling når det er strengt nødvendig.

Databehandler må sikre tilgjengelighet og sikkerhet gjennom fysiske sikringstiltak av bygg og anlegg for å unngå tjenestebortfall og/eller sikkerhetsbrudd som følge av strømbrudd el.

Databehandleren plikter å gi den Behandlingsansvarlige tilgang til sin sikkerhetsdokumentasjon, og bistå slik at den Behandlingsansvarlige kan ivareta sitt eget ansvar etter lov og forskrift.

9. Sikkerhetsbrudd

Databehandleren plikter å varsle den Behandlingsansvarlige uten ugrunnet opphold dersom Databehandleren har informasjon om, eller grunn til å tro, at det foreligger avvik. Dette gjelder for eksempel hvor Databehandlerens behandling av personopplysninger utsettes for: uautorisert tilgang, spredning, endring, skade, ødeleggelse, utilgjengelighet, annet sikkerhetsbrudd eller for øvrig brukes på uberettiget måte eller på annen måte håndteres i strid med regelverket for håndtering av personopplysninger og/eller vilkårene i denne Databehandleravtalen.

Varselet skal dokumentere sikkerhetsbruddet og skal som et minimum inneholde følgende opplysninger:

a) Beskrivelse av arten av bruddet på personopplysningssikkerheten, 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) Navnet på og kontaktopplysningene til Databehandlerens personvernombud eller et annet kontaktpunkt der ytterligere informasjon kan innhentes.

c) Beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten.

d) Beskrivelse av de tiltak som er truffet eller foreslås truffet for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Dersom ikke alle opplysninger kan gis i første varsel, skal opplysningene gis suksessivt så snart de foreligger.

I tilfelle sikkerhetsbrudd plikter Databehandleren å samarbeide med den Behandlingsansvarlige for å avdekke, begrense og utbedre bruddet.

Den Behandlingsansvarlige har ansvaret for å sende melding til Datatilsynet, og Databehandleren skal ikke sende slik melding eller kontakte Datatilsynet uten at den Behandlingsansvarlige har gitt skriftlig instruks om dette.

10. Sikkerhetsrevisjoner

Behandlingsansvarlig vil forbeholde seg retten til å gjennomføre sikkerhetsrevisjoner etter gjeldende personvernregelverk. Revisjonen kan omfatte gjennomgang av rutiner, stikkprøver, stedlige kontroller og eventuelle andre avtalte og egnede kontrolltiltak.

Databehandler plikter å gi Behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at Behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift. Sikkerhetsrevisjon vil kunne initieres på kort varsel.

Sikkerhetsrevisjoner skal være begrenset til Databehandlerens overholdelse av Databehandleravtalen og skal ikke forringe konfidensialiteten, integriteten og tilgangen til personopplysningene, ei heller påvirke konfidensialiteten, integriteten eller tilgjengeligheten for Databehandlerens interne rapporter, priser eller andre klienters opplysninger.

Dersom sikkerhetsrevisjonen gjennomføres ved bruk av uavhengige rådgivere på vegne av Databehandleren og/eller uavhengige ressurser utpekt av den Behandlingsansvarlige, er den Behandlingsansvarlige ansvarlig for å sikre at nevnte tredjeparter påtar seg en konfidensialitetsforpliktelse med hensyn til konfidensielle opplysninger mottatt fra Databehandleren i forbindelse med revisjonen.

Sikkerhetsrevisjoner skal skje for den Behandlingsansvarliges regning.

Dersom Behandlingsansvarlig etter Databehandlerens oppfatning krenker Gjeldende Personvernregelverk, skal Databehandleren varsle Behandlingsansvarlig uten ugrunnet opphold.

11. Avtalens varighet

Databehandleravtalen gjelder fra den er signert av alle Parter og gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig for gjeldende Avtale.

Partene skal varsle hverandre uten ugrunnet opphold dersom vedkommende Part ikke er eller vil være i stand til å overholde sine forpliktelser i henhold til denne Databehandleravtalen.

Ved varsel som nevnt ovenfor eller ved brudd på Avtalen, Databehandleravtalen eller gjeldende regelverk kan den Behandlingsansvarlige pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Brudd på Databehandleravtalen vil være å misligholde leveranseforpliktelsene i henhold til gjeldende Avtale.

Ved endringer av formålet med behandling av personopplysninger etter Avtalen skal Databehandleravtalen sies opp og ny Databehandleravtale inngås.

12. Endringer

Alle endringer av denne Databehandleravtalen skal gjøres skriftlig.

13. Ved opphør

Databehandler skal slette personopplysninger (inkludert kopier) 30 dager etter at tjenesten knyttet til behandlingen er avsluttet, med mindre det er avtalt at opplysningene skal lagres eller tilbakeleveres. Personopplysninger som har vært en del av Databehandleravtalen, men som i løpet av Databehandleravtalens varighet har blitt anonymiserte, skal slettes på samme måte.

Dersom det ikke er avtalt at databehandler skal lagre personopplysninger, plikter Databehandler å avslutte behandlingen av alle personopplysninger, tilbakelevere eller irreversibelt slette alle personopplysninger som er mottatt og/eller behandlet på vegne av den Behandlingsansvarlige. Databehandler skal destruere alle dokumenter, data, cd-er eller annet lagringsmedium som inneholder slike opplysninger på forsvarlig måte. Dette gjelder også for eventuelle sikkerhetskopier og personopplysninger som har blitt anonymisert i løpet av Databehandleravtalens varighet.

Tilbakelevering av personopplysninger gjøres etter nærmere avtale, se ellers bestemmelser i Avtalen som danner grunnlag for avslutning av tjenesten.

Databehandler skal skriftlig bekrefte eller dokumentere at sletting og/eller destruksjon er foretatt i henhold til nærmere avtalt tidspunkt etter Databehandleravtalens opphør og garantere for at Databehandleren ikke har beholdt kopi, utskrifter eller andre former for personopplysninger i noen form, med mindre lovgivning forhindrer sletting eller overlevering. I slike tilfeller skal Databehandleren garantere at man ikke lenger vil behandle personopplysningene.

14. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til:

Behandlingsansvarlig:	Databehandler: Digidrift as
Att: e-post: Tlf.:	Att: Erling Rønnekleiv e-post: post@ordeniegethus.no Tlf.: +47 99166419

15. Lovvalg og verneting

Databehandleravtalen er underlagt norsk rett og partene vedtar Nedre Telemark tingrett som verneting. Dette gjelder også etter opphør av Databehandleravtalen.

***

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

Sted og dato

Behandlingsansvarlig

.....

Databehandler

.....