NORKART

Databehandleravtale

mellom

Radøy kommune

som den Behandlingsansvarlige
Org: NO 954748634

og

Norkart AS

som databehandler
Org: NO 934 161 181

1. Bakgrunn og formål

1.1 Partene har inngått en eller flere avtaler ("**Hovedavtalen**") hvor Norkart AS ("**Databehandleren**") behandler personopplysninger på vegne av **Radøy kommune**(den "**Behandlingsansvarlige**").

1.2 Denne databehandleravtalen ("**Databehandleravtalen**") regulerer rettighetene og forpliktelsene knyttet til behandlingen av personopplysninger som gjøres i forbindelse med Hovedavtalen. Den har rang foran tidligere avtaler og bestemmelser partene imellom hva gjelder behandling av personopplysninger.

1.3 I tilfelle uoverensstemmelse mellom Hovedavtalen og Databehandleravtalen når det gjelder forhold spesifikt knyttet til personvern, skal Databehandleravtalen gis forrang.

2. Definisjoner

2.1 "**Personvernlovgivning**": De til enhver tid gjeldende lover og regler om behandling av personopplysninger, inkludert personopplysningsloven (med henvisning til GDPR fra 25 Mai 2018).

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

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

2.4 For øvrig skal ord og uttrykk ha samme mening som de er tillagt i gjeldende Personvernlovgivning.

2.5 **Omfang**

2.6 Denne Databehandleravtalen regulerer behandling av personopplysninger som finner sted på vegne av den Behandlingsansvarlige i forbindelse med Hovedavtalen, inkludert (i) personopplysninger overført fra den Behandlingsansvarlige til Databehandler, (ii) personopplysninger som Databehandleren gis tilgang til gjennom den Behandlingsansvarlige, og (iii) personopplysninger som genereres i forbindelse med Databehandlerens utførelse av sine forpliktelser under Hovedavtalen.

2.7 Nærmere informasjon om databehandlingen, herunder behandlingens formål/art og hvilke personopplysninger/registrerte som inngår ("Behandlingsoversikt), fremgår av den Behandlingsansvarliges innloggingsside på Kundesenteret. Behandlingsoversikten angis pr produkt/tjeneste og den Behandlingsansvarlige vil basert på egen oversikt over hvilke tjenester som benyttes kunne identifisere hva slags personopplysninger Databehandleren behandler på den Behandlingsansvarliges vegne.

2.8 Dersom Behandlingsoversikten endres som følge av endringer som Databehandleren initierer, f.eks. i form av endringer i produkt/tjeneste, vil den Behandlingsansvarlige varsles skriftlig uten ugrunnet opphold. Dersom den Behandlingsansvarlige motsetter seg endringen hva gjelder behandling av personopplysninger, og partene ikke finner en løsning, kan den Behandlingsansvarlige si opp relevant produkt/tjeneste med én måneds skriftlig varsel.

3. Alminnelige forpliktelser

3.1 Databehandleren garanterer at den vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysninger oppfyller kravene i Personvernlovgivningen og ivaretar de registrertes rettigheter. Databehandleren skal kun behandle personopplysninger i henhold til dokumenterte instruksjoner fra den Behandlingsansvarlige.

3.2 Dersom Databehandleren er forpliktet under en godkjent adferdsnorm som vist til i GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i GDPR artikkel 42, vil Databehandlerens overholdelse av slik adferdsnorm være tilstrekkelig for å påvise tilstrekkelige garantier som nevnt i punkt 3.1.

4. Bistand til den behandlingsansvarlige

4.1 Databehandleren skal på forespørsel bistå den Behandlingsansvarlige, gjennom egnede tekniske og organisatoriske tiltak, med å oppfylle den Behandlingsansvarliges plikt til å besvare forespørsler fra de registrerte i henhold til GDPR kapittel III.

4.2 Databehandleren skal på forespørsel bistå den Behandlingsansvarlige med å sikre overholdelse av GDPR artikkel 32 – 36, tatt i betraktning behandlingens art og informasjonen som er tilgjengelig for Databehandleren.

4.3 Bistand som nevnt i dette punkt 4.1 og 4.2 vil ytes på de timepriser som er avtalt mellom partene, eller, dersom det ikke er avtalt, på Databehandlerens gjeldende timepriser.

5. Tekniske og organisatoriske sikkerhetstiltak

5.1 Databehandleren skal gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen. Tiltakene skal ha til formål å verne personopplysningene mot tilfeldig eller ulovlig sletting eller tilfeldig tap, endringer eller uautorisert overføring eller tilgang. Databehandleren garanterer imidlertid ikke at sikkerhetsbrudd eller øvrige brudd på personopplysningssikkerheten ikke kan forekomme.

5.2 Databehandleren har angitt sine sikkerhetstiltak i Vedlegg 1. Disse anses generelt egnet for å oppfylle det nødvendige sikkerhetsnivået som nevnt i punkt 5.1.

5.3 Databehandleren skal påse at kun relevant personell har tilgang til personopplysninger og at disse er underlagt avtalefestet eller lovfestet taushetsplikt.

6. Bruk av underleverandører

6.1 Databehandleren kan engasjere andre databehandlere (underdatabehandlere) til å utføre oppgaver under denne Databehandleravtalen. Dette skal i så fall skje gjennom avtaler som pålegger tilsvarende forpliktelser som i denne Databehandleravtalen og som gir tilstrekkelige garantier for at det blir gjennomført tekniske og organisatoriske tiltak hos underdatabehandleren for å ivareta Personvernlovgivningen. Databehandleren har fullt ansvar overfor den Behandlingsansvarlige for at underdatabehandleren oppfyller sine forpliktelser.

6.2 Den Behandlingsansvarlige kan på forespørsel få en oversikt over underdatabehandlerne. På forespørsel kan den Behandlingsansvarlige også kreve fremlagt databehandleravtaler med underdatabehandlerne (forretningsmessig og annet sensitivt materiale kan dog skjules).

6.3 Databehandleren skal underrette den Behandlingsansvarlige om eventuelle planer om å benytte nye underdatabehandlere eller om å skifte ut underdatabehandlere og dermed gi den Behandlingsansvarlige muligheten til å motsette seg slike endringer. Den Behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn og denne grunnen veier tyngre enn Databehandlerens interesse i å gjøre endringen.

7. International Dataoverføring

7.1 Databehandleren kan kun overføre personopplysninger utenfor EU/EØS etter dokumenterte instruksjoner fra den Behandlingsansvarlige.

7.2 Ved slik eventuell instruksjon har Databehandleren fullmakt, på vegne av den Behandlingsansvarlige, til å inngå en databehandleravtale med underdatabehandleren som inneholder EUs standardklausuler i uendret form, dersom dette er nødvendig for å gjøre overføringen lovlig.

8. Brudd på personopplysningssikkerheten

8.1 Databehandleren skal skriftlig underrette den Behandlingsansvarlige om eventuelle brudd på personopplysningssikkerheten. Varselet skal gis senest 48 timer etter at Databehandleren ble oppmerksom på bruddet.

8.2 Den Behandlingsansvarlige har, der det er relevant, ansvaret for å varsle den relevante tilsynsmyndighet og de registrerte om brudd på personvernopplysningssikkerheten.

9. Revisjon

9.1 Databehandleren skal foreta jevnlige revisjoner av sin behandling av personopplysninger. Databehandleren skal dokumentere og på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige informasjon som er nødvendig for å påvise etterlevelse av denne Databehandleravtalen og Personvernlovgivningen.

9.2 På forespørsel kan den Behandlingsansvarlige få oversendt eventuelle revisjonsrapporter om personvern utarbeidet av tredjepart på vegne av Databehandleren. Den Behandlingsansvarlige skal ha rett til å fremlegge slike revisjonsrapporter for sine eksterne revisorer og for tilsynsmyndigheter.

9.3 På forespørsel har den Behandlingsansvarlige, gjennom revisor eller lignende tredjepart som er underlagt konfidensialitet, rett til å gjøre revisjoner av Databehandleren. Forespørselen skal gis med minst 14 dagers varsel. Revisjoner kan ikke gjøres mer enn én gang pr år, med mindre det er påkrevd etter Personvernlovgivningen.

9.4 Revisjoner kan først og fremst innebære gjennomgang av dokumentasjon, rutiner, systemer og relevante tekniske og organisatoriske sikkerhetstiltak. Den Behandlingsansvarlige skal gjøre sitt ytterste for å gjennomføre revisjoner uten at

dette er til hinder for Databehandlerens virksomhet. Den Behandlingsansvarlige skal videre påse at personell som utfører revisjoner er underlagt taushetsplikt.

9.5 Dersom en revisjon avdekker brudd på denne Databehandleravtalen eller Personvernlovgivningen, skal Databehandleren rette slike brudd innen rimelig tid.

9.6 Hver av partene dekker i utgangspunktet sine egne kostnader forbundet med revisjon. Den Behandlingsansvarlige skal også dekke Databehandlerens nødvendige kostnader for revisjoner den Behandlingsansvarlige har initiert (hvor arbeid for Databehandleren dekkes i samsvar med de timepriser som er avtalt mellom partene, eller, dersom det ikke er avtalt, i samsvar med Databehandlerens gjeldende timepriser).

9.7 Databehandleren skal varsle den Behandlingsansvarlige dersom tilsynsmyndighet krever tilgang til eller informasjon om behandlingen av personopplysninger i henhold til denne Databehandleravtalen, med mindre dette er forbudt ved lov eller myndighetspålegg.

10. Ansvarsbegrensning

10.1 Med mindre annet er avtalt i Hovedavtalen, skal Databehandleren være ansvarlig for den Behandlingsansvarliges direkte tap ved Databehandlerens eventuelle mislighold av denne Databehandleravtalen. Indirekte tap dekkes ikke. Indirekte tap omfatter, men er ikke begrenset til, tapt fortjeneste av enhver art, tapte besparelser og krav fra tredjeparter. Erstatningsansvaret i løpet av ett år er oppad begrenset til beløpet betalt av den Behandlingsansvarlige til Databehandleren under Hovedavtalen det året. Ansvarsbegrensningen gjelder ikke der det er utvist grov uaktsomhet eller forsett.

11. Varighet og oppsigelse

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

11.2 Ved Databehandleravtalens opphør skal Databehandleren, dersom den Behandlingsansvarlige ønsker det, returnere alle personopplysninger og alle kopier til den Behandlingsansvarlige eller slette alle personopplysningene og bekrefte overfor den Behandlingsansvarlige at det er gjort, med mindre Databehandleren er forhindret ved lov fra å gjøre det. Dersom det er tilfelle, skal Databehandleren besørge sikker lagring av personopplysningene, men ikke lenger aktivt behandle dem.

11.3 Oppsigelse av denne Databehandleravtalen skal ikke hindre Databehandleren fra å fortsette å behandle anonymiserte opplysninger for analytiske, statistiske og andre formål.

Undertegning

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

Behandlingsansvarlig For Virksomheten: **Radøy kommune**	**Databehandler** For Leverandøren: **Norkart AS**
Dato, sted og underskrift 19. juni 2019	**Dato, sted og underskrift** **Sandvika,** 19. juni 2019
Navn og stilling Sveinung Kvamme, Økonomisjef	**Navn og stilling** Kjell Krüger Næss,

1 VEDLEGG 1: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Norkart har etablert et internkontrollsystem som søker å ivareta kravene til tekniske og organisatoriske sikkerhetstiltak. Systemet omfatter rutiner for utvikling og vedlikehold av våre produkter, samt prosesser for å reagere på uforutsette hendelser.

1.1 Organisatoriske tiltak

Organisatoriske tiltak handler om rutiner og retningslinjer for gjennomføring av arbeid på et overordnet nivå.

1.1.1 Taushetserklæring

Taushetserklæringer i Norkart brukes for å gjøre ansatte oppmerksom på at det forekommer konfidensiell informasjon i Norkart. Rutinen er at de ansatte undertegner en slik erklæring samtidig med ansettelseskontrakten.

1.1.2 Håndtering av kundehenvendelser

Norkart har etablert rutiner for å ivareta kundehenvendelser og sikre at de kommer frem til riktig person, uavhengig av hvor de kommer inn fra. Hver kunde har en egen kundeansvarlig, og hvert produkt har en egen fag/markedsansvarlig. Sammen har disse ansvaret for å inndrive informasjon for å svare på kunders henvendelser, og/eller håndtere andre situasjoner som oppstår.

1.1.3 Årlig intern revisjon

Innholdet i internkontrollsystemet og oversikten over ansvarspersoner skal revideres årlig, for å sikre at informasjonen er oppdatert. Eventuelle svakheter i systemet som har blitt oppdaget skal rettes opp ved revisjonen.

1.1.4 Tilrettelegging for ekstern revisjon

Norkart har etablert rutiner for å håndtere forespørsler om ekstern revisjon, med oversikt over hvem som skal håndtere dette og hvor informasjonen eksterne revisorer skal ha tilgang til ligger.

1.1.5 Vedlikehold av Behandlingsoversikten

Behandlingsoversikten er en viktig del av databehandleravtalen og skal vedlikeholdes løpende av de fag/markedsansvarlige. I tillegg gjennomgås den ved den årlige revisjonen.

1.1.6 Personvernerklæringer

Alle produkter som har behov for personvernerklæringer skal utarbeide disse og gjøre dem tilgjengelige for produktets brukere. Denne inneholder informasjon om hva slags data som behandles og hvordan det behandles.

1.2 Generelle tekniske tiltak

Tekniske tiltak som skal være implementert i alle produkter, og som er et absolutt krav i all nyutvikling.

1.2.1 Forsvarlig utviklingspraksis og videreutdanning av utviklere

Alle utviklere skal ha et bevisst forhold til sikker utviklingspraksis og vil løpende bli lært opp i dette. Sikker utviklingspraksis inkluderer, men er ikke begrenset til, temaer som korrekt bruk av

kildekontrollsystemer, fagfellevurdering av hverandres arbeid og grunnleggende tema innen personvern. Utviklere blir blant annet utstyrt med sjekklister for håndtering av personlig informasjon.

1.2.2 Bruk av kryptering der det er hensiktsmessig

En hovedregel er at personlig informasjon lagret i databaser skal være kryptert, og alle tjenester over internett skal leveres over kryptert kommunikasjon. Alle systemer skal ha unike brukere med sterke passord.

1.2.3 Arkitekturdokumentasjon

Alle produkter må dokumentere hvordan arkitekturen er bygget opp mellom tjenester, front-end, database og så videre. Videre må også prosjektet dokumentere hvordan tjenesten er satt i drift, og rutinene som brukes for testing, staging og produksjonssetting.

1.2.4 Driftsovervåking

I systemer med personlig informasjon vil Norkart logge autorisert bruk og forsøk på uautorisert bruk av informasjonssystemet i henhold til personopplysningsforskriften:

- Autorisert bruk av informasjonssystemet skal registreres (logging av pålogging og avlogging til nettverk og applikasjoner).
- Forsøk på uautorisert bruk av informasjonssystemet skal registreres (logging av mislykte forsøk på pålogging til nettverk og applikasjoner).
- Overvåkingssystemet bør kunne automatisk varsle utviklere ved uvanlig oppførsel.

I tjenester med personlig informasjon skal det føres oversikt over alle ansatte med tilgang til informasjonen.

1.2.5 Risikovurderinger

Ved etablering av nye produkter eller større endringer av eksisterende produkter, skal det gjøres en risikovurdering som fastslår sannsynligheten for et sikkerhetsbrudd og de potensielle konsekvensene av det. Denne drar nytte av informasjon om hvilke data som behandles og teknisk dokumentasjon som for eksempel arkitekturdokumentasjonen. Dersom risikovurderingen avslører en uakseptabel risiko skal dette være førende for den videre utviklingen av produktet slik at risikoen reduseres

1.3 Spesifikke tekniske tiltak

I tillegg til de generelle organisatoriske og tekniske tiltakene, finnes det tekniske tiltak som er særegne for det enkelte produkt. Informasjon om spesifikke tekniske tiltak er listet opp per produkt i behandlingsoversikten som er referert til i punkt 2.7, og det henvises til denne for mer informasjon om produktene omfattet av kundeforhold