

# Databehandleravtale

Mellom

Norconsult Norge AS

og

Krødsherad kommune

## 1 PARTSFORHOLD

Denne avtalen er inngått mellom Norconsult (heretter kalt **databehandler**) som databehandler og Krødsherad kommune (heretter kalt **behandlingsansvarlig**) som behandlingsansvarlig.

## 2 AVTALENS HENSIKT

Avtalens hensikt er å regulere rettigheter og plikter etter personopplysningsloven som gjennomfører EUs General Data Privacy Regulation (personvernforordningen), og annet regelverk som senere erstatter eller supplerer disse reglene. Avtalen skal sikre at personopplysninger som databehandler behandler på vegne av behandlingsansvarlig ikke brukes urettmessig eller kommer uberettigede i hende.

## 3 FORMÅLET MED BEHANDLINGEN OG ROLLER

Avtalen regulerer databehandlers bruk og annen behandling av personopplysninger på vegne av behandlingsansvarlig i forbindelse med at databehandler leverer en ArcGIS innspillsløsning for å innhente innspill til KDP for friluftslivets ferdselsårer i Krødsherad kommune i overensstemmelse med det som fremgår av Oppdragsavtalen, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse. Denne databehandleravtalen er en del av Oppdragsavtalen mellom partene og utfylles med bestemmelser i denne.

Databehandler skal på denne bakgrunn være behandlingsansvarliges databehandler i forbindelse med levering av ArcGIS innspillsløsning til behandlingsansvarlig.

Behandlingsansvarlig er behandlingsansvarlig for personopplysninger som behandles i databehandlers eller tredjeparters systemer i forbindelse med levering av ArcGIS innspillsløsning til behandlingsansvarlig.

Behandlingsansvarlig innestår for å ha rettslig grunnlag etter gjeldende regelverk for bruken av disse personopplysningene. Behandlingsansvarlig skal ivareta lovbestemte plikter.

## 4 VEDLEGG

Som vedlegg til denne avtalen skal det utarbeides og ajourholdes en oversikt over de personopplysninger databehandler behandler på vegne av behandlingsansvarlig, samt eventuelle særlige krav til behandlingen som behandlingsansvarlig har satt.

Behandlingsansvarlig kan som behandlingsansvarlig sette særlige krav til databehandlers behandling av personopplysningene og skal følge opp at det kan dokumenteres at disse krav oppfylles.

Behandlingsansvarlig skal utarbeide og vedlikeholde vedlegget til databehandleravtalen. Databehandler plikter å bistå behandlingsansvarlig med å utarbeide og vedlikeholde dette vedlegget. Vedlegget er et dynamisk dokument som oppdateres når det skjer endringer, og signeres av de hos databehandler og behandlingsansvarlig som har det operative ansvaret etter Oppdragsavtalen.

## 5 BRUK AV UNDERLEVERANDØRER

Dersom databehandler i sin rolle som behandlingsansvarliges databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal dette avtales skriftlig med behandlingsansvarlig før behandlingen av personopplysninger med bistand av slike underleverandører starter.

Alle som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med [databehandlers avtalemessige og lovmessige forpliktelser og skal ved skriftlig databehandleravtale være pålagt å oppfylle vilkårene etter disse. Databehandler er overfor behandlingsansvarlig ansvarlig for at underleverandører utfører sine oppgaver i overensstemmelse med denne avtalen og gjeldende norsk rett til enhver tid, jf. blant annet de krav som gjelder etter personvernforordningen Artikkel 28, og de krav behandlingsansvarlig har satt for de aktuelle tjenestene.

## 6 KRAV TIL INFORMASJONSSIKKERHET

Databehandler er forpliktet til å ivareta det ansvar for informasjonssikkerhet som tilligger databehandler etter gjeldende norsk rett til enhver tid, herunder krav som gjelder i medhold av personvernforordningen Artikkel 32. Informasjonssikkerhet omfatter blant annet:

- Sikring av konfidensialitet; beskyttelse mot at uvedkommende får innsyn i opplysningene
- Sikring av integritet; beskyttelse mot utilsiktet endring av opplysningene
- Sikring av tilgjengelighet; sørge for at tilstrekkelige og relevante opplysninger er til stede
- Sikring av robusthet; sørge for at tilstrekkelige tiltak er på plass for å sikre tilstrekkelig tilgjengelighet og for å minske effekten av feil som kan oppstå.

Databehandler skal følge de rutiner og instruksjoner for behandlingen som behandlingsansvarlig til enhver tid har bestemt skal gjelde for databehandlers behandling av personopplysninger på behandlingsansvarliges vegne, og skal ikke behandle personopplysninger på annen måte enn det som fremgår av denne databehandleravtalen. Databehandler plikter for øvrig å etterkomme krav til databehandlingen, herunder informasjonssikkerhet, som ellers følger av relevante lover og forskrifter. Databehandlingen vil i tillegg utføres i henhold til gjeldende systemdokumentasjon og øvrige rutinebeskrivelser for tjenestene.

Databehandler kan ikke gjøre vesentlige endringer i sine informasjonssikkerhetstiltak uten at behandlingsansvarlig er informert og har godkjent endringen. Hvis de aktuelle tjenestene nødvendiggjør tilleggskrav til sikkerhet, skal det før tjenestene besluttet lagt inn, avklares mellom databehandler og behandlingsansvarlig om ytterligere sikkerhetstiltak som tilfredsstillende disse kravene kan dekkes.

Databehandler skal ha definert sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisering og ansvar i samsvar med de rettslige krav som nevnt ovenfor, samt påse at dette følges opp med internkontroll. Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjon for databehandlers oppfyllelse av sine forpliktelser etter dette punktet skal på forespørsel være tilgjengelig for behandlingsansvarlig, Personvernemnda, Datatilsynet og andre relevante tilsynsmyndigheter.

Databehandler har taushetsplikt om personopplysninger som databehandler får tilgang til i henhold til Oppdragsavtalen og denne avtalen. Databehandler skal påse at alle involverte er orientert om taushetsplikten og iverksette slike tiltak som følger av personvernforordningen Artikkel 5 nr. 1 bokstav f og tilsvarende regler som senere erstatter eller supplerer disse bestemmelsene, og avtalen for øvrig. Taushetsplikten gjelder også etter avtalens opphør.

Databehandler skal sikre at all behandling av personopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabelt risikonivå definert av behandlingsansvarlig. Som en del av dette skal databehandler legge fram risikovurderinger av egen og eventuelle underleverandørers sikkerhet.

Databehandler skal bistå behandlingsansvarlig i å utrede eventuelle personvernkonsekvenser (konsekvensanalyse) og å gjennomføre en konsekvensanalyse i henhold til gjeldende norsk rett.

Databehandler kan ikke overføre personopplysninger til land utenfor EØS-området eller til internasjonale organisasjoner uten at dette er avtalt skriftlig med behandlingsansvarlig på forhånd.

## **7 SIKKERHETSBRUDD OG AVVIKSHÅNDTERING**

Databehandler skal ha klare rutiner for logging av sikkerhetsbrudd og avvik i systemer som brukes til å behandle personopplysninger, og som er omfattet av denne avtalen. Dersom det avdekkes feil eller avvik, skal databehandler uten ugrunnet opphold varsle behandlingsansvarlig om dette. Databehandler skal i slike tilfeller straks igangsette tiltak for å minimere mulig skade for behandlingsansvarlig, samt tiltak for å unngå at liknende hendelser kan inntreffe på nytt.

Databehandler plikter å melde avvik, jf. personvernforordningen Artikkel 33 og 34 og tilsvarende regler som senere erstatter eller supplerer disse bestemmelsene til behandlingsansvarlig. Avviksmelding skal som minimum: (a) beskrive sikkerhetsbruddet, herunder, hvis mulig, kategoriene og det omtrentlige antall berørte registrerte, samt kategoriene og det omtrentlige antall personopplysninger som er berørt av avviket; (b) angi navn på og kontaktopplysninger for personvernombud eller andre kontaktpunkt hvor ytterligere opplysninger kan innhentes; (c) beskrive de sannsynlige konsekvenser av bruddet på informasjonssikkerhet; (d) beskrive de tiltak som er truffet eller som er foreslått truffet for å håndtere bruddet på informasjonssikkerhet, herunder eventuelle tiltak for å begrense de mulige skadevirkningene.

Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet.

## **8 KRAV FRA ENKELTPERSONER**

Databehandler skal gjennom passende tekniske og organisatoriske tiltak bistå behandlingsansvarlig med å etterkomme krav fra enkeltpersoner, herunder de registrerte (de personer som personopplysningene gjelder). Dette gjelder også krav om innsyn, retting og sletting av personopplysninger.

## **9 INNSYN OG SIKKERHETSREVISJONER**

Behandlingsansvarlig kan til enhver tid kreve innsyn i databehandlers behandling av personopplysninger. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten i tjenesten som leveres.

Det skal gjennomføres årlig sikkerhetsrevisjoner av løsningene. Behandlingsansvarlig kan be om utlevering av de sikkerhetsrevisjoner som viser hvordan løsningene håndterer behandlingsansvarliges data.

Dokumentasjon for databehandlers oppfyllelse av sine forpliktelser etter personvernforordningen Artikkel 28, skal gjøres tilgjengelig for behandlingsansvarlig, Datatilsynet og Personvernemnda.

## **10 AVTALENS VARIGHET**

Denne avtalen trer i kraft samtidig med Oppdragsavtalen. Avtalen varer så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig i henhold til Oppdragsavtalen.

Ved brudd på denne avtalen eller gjeldende personvernlovgivning kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

## 11 OPPHØR

Ved opphør av denne avtalen plikter databehandleren å slette eller tilbakelevere alle personopplysninger som er mottatt på vegne av behandlingsansvarlig og som omfattes av denne avtalen. Behandlingsansvarlig gis rett til å velge om det skal foretas sletting eller tilbakelevering.

I den utstrekning behandlingsansvarlig velger at sletting skal skje, skal databehandler slette eller forsvarlig destruere alle elektronisk og ikke-elektronisk lagrede personopplysninger som omfattes av avtalen. Eventuelle sikkerhetskopier skal også slettes. Dette gjelder med mindre annet følger av annen ufravikelig lovgivning.

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

## 12 MEDDELELSER

Meddelelser skal sendes skriftlig til partenes utpekte kontaktpersoner etter Oppdragsavtalen.

\* \* \*

Avtalen er utstedt i 2 eksemplarer, hvor partene har mottatt hvert sitt.

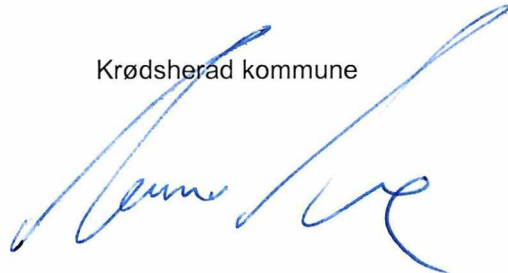
[Foretaksnavn databehandler]

Norconsult Norge AS



[Foretaksnavn behandlingsansvarlig]

Krødsherad kommune



## Vedlegg

Oversikt over personopplysninger databehandler behandler på vegne av behandlingsansvarlig.

## Vedlegg

I forbindelse med utarbeidelse av KDP for friluftslivets ferdselsårer i Krødsherad kommune har Norconsult Norge AS utarbeidet en innspillsløsning i ArcGIS. Målet med innspillsløsningen er å samle inn innspill i forbindelse med kartleggingsfasen i prosjektet.

### Hvem

Alle som ønsker å komme med innspill til KDP Friluftslivets ferdselsårer i Krødsherad kommune kan legge inn innspill i innspillsportalen. Det forventes at det i all hovedsak vil være aktuelt for innbyggere, besøkende og hytteeiere i kommunen.

### Hva

Det er mulig å velge om man vil være anonym eller ikke når man legger inn innspill. Velger du å ikke være anonym legger du igjen navn (fornavn og etternavn) og E-postadresse. Innspillsdata: fritekst, kartfestede posisjoner (GPS-koordinater) og eventuelle vedlegg knyttet til det enkelte innspill. Tekniske data: tidsstempel for innsending, IP-adresse og enhetsinformasjon som automatisk registreres av Survey123 og ArcGIS Online.

### Hvordan

I selve innspillsløsningen er det et eget punkt hvor man skriver inn navn og E-post (frivillig), samt at det registreres fritekst og kartfestede posisjoner. Behandlingsansvarlig behandler personopplysninger med følgende rettslige grunnlag i henhold til personvernforordningen artikkel 6 nr. 1:

For innsamling og behandling av innspill knyttet til KDP Friluftslivets ferdselsårer: bokstav e — behandlingen er nødvendig for utførelse av en oppgave i allmennhetens interesse, jf. plan- og bygningsloven. For frivillig avgivelse av navn og e-postadresse: bokstav a — den registrertes samtykke, gitt ved aktiv handling i innspillsløsningen.

Personopplysninger innsamlet gjennom innspillsløsningen skal slettes fra ArcGIS Online innen 30 dager etter at innspillsperioden for KDP Friluftslivets ferdselsårer er avsluttet. Før sletting skal databehandler overlevere en fullstendig kopi av innsamlede data til behandlingsansvarlig i et maskinlesbart format. Slettingen skal omfatte alle innspill, vedlegg, eksporterte kopier og eventuelle sikkerhetskopier. Databehandler skal skriftlig bekrefte gjennomført sletting til behandlingsansvarlig innen 14 dager etter at sletting er utført.

### Hvorfor

Målet med å samle inn navn og E-post er at Krødsherad kommune kan ta kontakt med innspiller hvis innspillet er relevant for kommunen å følge opp direkte videre.

### Brudd på sikkerhet

Dersom det avdekkes brudd på sikkerheten som berører personopplysninger omfattet av denne avtalen, skal databehandler varsle behandlingsansvarlig så raskt som mulig og senest innen 24 timer etter at bruddet ble oppdaget. Varselet skal inneholde den informasjon som er tilgjengelig på varslings tidspunktet, og suppleres fortløpende etter hvert som ytterligere informasjon foreligger. Tidsfristen på 24 timer skal sikre at behandlingsansvarlig kan oppfylle sin varslingsplikt overfor Datatilsynet innen 72 timer i henhold til personvernforordningen artikkel 33.

### Underleverandør

Databehandler benytter følgende godkjente underdatabehandler for levering av ArcGIS innspillsløsning:

Environmental Systems Research Institute, Inc. (Esri), 380 New York Street, Redlands, California 92373, USA. Esri leverer ArcGIS Online som skytjeneste, herunder lagring og prosessering av data innsamlet gjennom Survey123. Forholdet mellom databehandler og Esri er regulert av Esris Data Processing Addendum (G666), som inneholder Standard Contractual Clauses i henhold til EU-kommisjonens gjennomføringsbeslutning 2021/914 samt supplerende tiltak. Databehandler skal på forespørsel fremlegge kopi av gjeldende DPA for behandlingsansvarlig.

Databehandler skal varsle behandlingsansvarlig skriftlig før eventuell endring av underdatabehandlere, herunder tillegg av nye eller erstatning av eksisterende, i henhold til personvernforordningen artikkel 28 nr. 2. Behandlingsansvarlig har rett til å motsette seg slike endringer innen 30 dager etter mottak av varsel.