

**Databehandleravtale i henhold til Personopplysningsloven 15. juni 2018 nr 38 og EUs
personvernforordning 2016/679 («GDPR»),**

mellom:

Meland Kommune

Behandlingsansvarlig

og

Norsk kulturskoleråd (Kor Arti')

Databehandler

Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Lov av 15. juni 2018 nr 38 om behandling av personopplysninger (personopplysningsloven) og GDPR. Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende og forøvrig sikre at Databehandler behandler personopplysninger i henhold til gjeldende lovkrav.

Avtalen regulerer Databehandlers bruk av personopplysninger på vegne av Behandlingsansvarlig, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med bruk av Kor Arti'.

Behandlingens art og formål

Behandlingen av personopplysninger som Databehandler gjør på vegne av Behandlingsansvarlige, består i å levere og administrere Kor Arti', samt utføre nødvendig drift og vedlikehold av systemet.

Databehandler kan ikke overføre personopplysninger til underleverandører eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. også punkt 4 i denne avtalen.

Registrerte og personopplysninger som behandles

Typen personopplysninger som databehandleren behandler i forbindelse med levering og administrasjon av Kor Arti':

- Organisasjonsnummer (eduPersonOrgDN:norEduOrgNIN)
- Liste med skoler (feideSchoolList)
- Kontaktperson for Kor Arti' brukerkonto med navn, e-post og telefon

Feide-attributter blir brukt ved innlogging for sammenligning mot informasjon som ligger på en eksisterende brukerkonto hos Kor Arti'. Dersom Feide-brukere er knyttet til samme organisasjonsnummer som også ligger på en Kor Arti' brukerkonto, så vil Feide-brukere bli logget inn med den Kor Arti' brukerkontoen.

Informasjon som ligger på en Kor Arti' brukerkonto er oppgitt frivillig gjennom en bestilling av tjenesten og brukes ikke til andre formål enn levering og administrasjon av Kor Arti'.

Databehandlers plikter

Databehandler skal følge de rutiner og instruksjoner for behandling av personopplysninger som behandlingsansvarlig til enhver tid har bestemt skal gjelde. Vilkårene i denne avtalen går foran databehandlerens personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandleren i forbindelse med bruk av Kor Arti'.

Databehandler plikter å bistå behandlingsansvarlig ved ivaretagelse av den registrertes rettigheter.

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon. Databehandleren plikter også å bistå den behandlingsansvarlige slik at denne kan ivareta sitt eget ansvar etter lov og forskrift.

Behandlingsansvarlig har, med mindre annet er avtale eller følger av lov, rett til tilgang til og innsyn i personopplysningene som databehandleren håndterer og de systemene som benyttes til dette formål.

Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør. Taushetsplikten omfatter også ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer som databehandleren anvender for å levere eller administrere tjenesten.

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysningene, kan gis slik tilgang. Databehandleren plikter å dokumentere sine rutiner og retningslinjer for tilgangsstyring på forespørsel fra behandlingsansvarlig.

Databehandler plikter å loggføre all autorisert og forsøk på uautorisert bruk av Kor Arti'. Loggene skal oppbevares av databehandleren i minimum 3 måneder. Behandlingsansvarlig skal på forespørsel gis tilgang til loggene.

Behandlingsansvarlige bekrefter gjennom signering av denne databehandleravtalen at:

- Behandlingsansvarlig skal, i sin bruk av systemet, behandle personopplysninger i samsvar med kravene i gjeldende personvernlovgivning og GDPR
- Behandlingsansvarlig har ansvaret for nøyaktighet, integritet, innhold, pålitelighet og lovlighet rundt personopplysningene som Behandlingsansvarlig har ført inn i systemet og gjort tilgjengelig for Databehandleren, i henhold til personvernlovgivningens krav.
- Behandlingsansvarlig oppfylder lovens plikter til å gi relevant informasjon til de registrerte.
- Den Behandlingsansvarliges plikter etter dette punkt fritar ikke Databehandler fra sine plikter etter personvernlovgivningen og denne avtale.

Databehandleren skal føre protokoll (logg) over behandlingsaktiviteter denne utfører på vegne av den Behandlingsansvarlige, som skal inneholde minimum den informasjon som er pålagt etter personvernforordningen artikkel 30 nr. 2. Bruk av underleverandør

Databehandler har den Behandlingsansvarliges generelle godkjenning til å bruke andre databehandlere. Databehandler må likevel underrette den behandlingsansvarlige ved eventuelle planer om å skifte ut eller bruke nye databehandlere og slik at den Behandlingsansvarlige gis muligheten til å motsette seg slike endringer.

Samtlige som på vegne av Databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med og pålagt å følge samme forpliktelser som Databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse. Dersom underdatabehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger og kravene ellers i denne avtalen, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser.

Databehandler skal etablere egne avtaler med eventuelle underleverandører før behandlingen av personopplysninger starter. I avtalene skal databehandler sørge for at underleverandører er pålagt å ivareta alle plikter som databehandleren selv er forpliktet å ivareta iht. denne avtalen. Databehandler plikter å forelegge alle avtaler med underleverandører for den behandlingsansvarlige.

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

Databehandler kan ikke overføre personopplysninger til underleverandører utenfor EU/EØS-området, med mindre underleverandørene er sertifisert etter Safe Harbour-ordningen eller opplysningene overføres til underleverandører i land godkjent av EU.¹ Denne bestemmelsen gjelder også sikkerhetskopier (back-up) av personopplysninger som databehandleren behandler på vegne av behandlingsansvarlig.

Sikkerhet og avvik

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter GDPR art. 32 og personopplysningsloven. Avviksmelding skal skje ved at Databehandler melder avviket til Behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet og Databehandler skal ikke sende slik melding eller kontakte tilsynsmyndighet uten at den Behandlingsansvarlige har gitt instruks om dette.

¹ Oversikt over land som EU har godkjent overføring av personopplysninger til, er tilgjengelig på http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

I tilfelle sikkerhets- eller personvernbrudd, skal Databehandleren varsle den Behandlingsansvarlige uten ugrunnet opphold. Melding om brudd skal minimum inneholde:

1. 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,
2. navnet på og kontaktopplysningene til personvernrådgiveren eller et annet kontaktpunkt der mer informasjon kan innhentes,
3. beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
4. beskrivelse av de tiltak som er truffet eller foreslår å treffe 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 melding, skal opplysningene gis suksessivt så snart de foreligger.

Sikkerhetsrevisjoner

Databehandler skal gjennomføre sikkerhetsrevisjoner jevnlig for systemer og lignende, som omfattes av denne avtalen, og skal ha rutiner som beskriver frekvens, omfang og gjennomføring av disse. Denne dokumentasjonen skal gjøres tilgjengelig for Behandlingsansvarlig på forespørsel.

Behandlingsansvarlig har rett til å kreve kontroll og revisjon av Databehandlers personopplysningssikkerhet og oppfyllelse av denne Databehandleravtale.

Databehandler skal ved behov stille ressurser og kompetanse til rådighet for gjennomføring av sikkerhetsrevisjoner fra Behandlingsansvarlig.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandleren, skal behandlingsansvarlig informeres om dette og ha tilgang til oppsummeringer av revisjonsrapportene.

Avtalens varighet

Avtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

Ved brudd på denne avtale eller personopplysningslovgivningen kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning. Avtalen følger driftsavtalens bestemmelser om varighet og oppsigelse.

Ved opphør/sletting av data

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige og som omfattes av denne avtalen. Behandlingsansvarlig bestemmer når og hvordan sletting eller tilbakelevering av opplysningene skal skje, herunder hvilket format som skal benyttes.

- Brukerkontoer hos Kor Arti' skal på forespørsel slettes etter **30 dager**.
- Brukerkontoer skal slettes etter **450 dager** med inaktivitet.

Databehandler skal slette eller forsvarlig destruere alle dokumenter, data, disk mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

- Sletting skal skje ved at databehandler skriver over personopplysninger innen **30 dager** etter avtalens opphør.
- Personopplysninger i disk og andre fysiske lagringsmedier skal skrives over innen **30 dager** etter avtalens opphør.

Databehandler skal skriftlig dokumentere at sletting eller destruksjon er foretatt i henhold til avtalen på forespørsel fra behandlingsansvarlig.

Databehandler dekker alle kostnader i forbindelse med tilbakelevering eller sletting av personopplysninger.

Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til den til enhver tid gjeldende kontaktperson hos Behandlingsansvarlig og kundekontakt hos Databehandler, jf. driftsavtale.

ANDRE BESTEMMELSER

Øvrige plikter og rettigheter følger av driftsavtalen som gjelder mellom Databehandleren og Behandlingsansvarlige om tjenestene som nødvendigvis gjør behandling av personopplysninger og denne avtale. De samme kontaktpersoner gjelder for denne avtale som etter driftsavtalen.

Denne avtale skal ikke utvide Behandlingsansvarliges sanksjonsmuligheter, herunder erstatningsansvar for Databehandleren, utover det som følger av driftsavtalen.

Databehandler plikter i henhold til denne avtale ansees kompensert for gjennom priser og betingelser som er fastsatt i driftsavtalen og Databehandler skal ikke kunne kreve ekstra betalt for å ivareta de krav og betingelser som følger av denne avtale.

Ved eventuell overdragelse av driftsavtalen til andre parter, skal denne avtale overdras tilsvarende

Lovvalg og verneting

Avtalen er underlagt norsk rett med Sør-Trøndelag tingrett som verneting, også etter opphør av avtalen. Avtalen finnes i 2 - to - eksemplarer, hvorav partene har hvert sitt.

Trondheim, 12/11-2019

For Behandlingsansvarlig


.....

underskrift

For Databehandler


.....

underskrift

Vedlegg til databehandleravtale

Oversikt over underleverandører

Underleverandør - org nr.:	Formål:
Digitalbyrået Arego AS – 994 877 968	Drift av korarti.no
Referanser til avtaler mellom databehandler og underleverandører	Tilbud nettsted Kor Arti' digitalt. Avtale signert 3. mars 2016