

DATABEHANDLERAVTALE

Denne databehandleravtalen (**Avtalen**) er inngått mellom:

- (i) [selskapsnavn og organisasjonsnummer til behandlingsansvarlig] (**Behandlingsansvarlig**), og
- (ii) MuseumsIT AS, org.nr. 897 761 602 (**Databehandler**).

Behandlingsansvarlig og Databehandler omtales hver for seg som **Part** og samlet som **Partene**.

1. Bakgrunn

Formålet med Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig, er kun å levere og administrere tjenester som er inkludert i separate avtaler om leveranse av tjenester.

I forbindelse med ovennevnte tjenester (**Tjenestene**) vil Databehandleren behandle personopplysninger på vegne av Behandlingsansvarlig.

Denne Avtalen regulerer rettigheter og plikter i forbindelse med Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig. Avtalen skal sikre at personopplysningene behandles i samsvar med gjeldende personvernlovgivning (**Personvernregelverket**), herunder Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 (**Personvernforordningen**).

Begreper benyttet i Avtalen skal forstås på samme måte som i Personvernregelverket.

2. Behandlingens formål og rammer

Behandlingens formål er å sikre kontraktsmessig leveranse av Tjenestene (**Formålet**).

Databehandleren skal kun behandle personopplysningene i den grad og så lenge det er nødvendig for å oppfylle Formålet.

Under er eksempler av personopplysninger som Databehandleren kan behandle i forbindelse med levering og administrasjon av tjenestene. Listen er ikke uttømmende.

- **Personopplysninger:** Navn, adresse, telefonnummer, e-postadresse, IP adresser, bilder av personer, fødselsnummer, kontonummer osv.

- **Sensitive personopplysninger:** Medlemskap i fagforeninger, helseforhold, politisk og/eller religiøs overbevisning.

Behandlingsansvarlig har selv ansvar for å beskrive hvilke personopplysninger som finnes i de ulike systemene Databehandler er databehandler for (jfr vedlegg 1).

Databehandleren skal kun behandle personopplysningene i henhold til dokumenterte instruksjoner fra Behandlingsansvarlige og for øvrig i tråd med denne Avtalen. Dersom Databehandleren er rettslig forpliktet til å behandle personopplysningene på annen måte, for eksempel ved at han plikter å utlevere opplysningene til andre, skal Databehandleren varsle Behandlingsansvarlig før slik behandling foretas, med mindre viktige samfunnsinteresser tilsier at slikt varsel ikke kan finne sted.

Databehandleren plikter å overholde adferdsnormer og sertifiseringsordninger etter Personvernforordningens Artikkel 40 og 42, dersom Databehandleren er underlagt slike.

Databehandleren skal føre protokoll over de behandlingsaktiviteter han utfører på vegne av Behandlingsansvarlig i henhold til Personvernforordningens Artikkel 30. Behandlingsansvarlig kan til enhver tid be om kopi av protokollen.

Databehandleren skal straks underrette Behandlingsansvarlig dersom Databehandleren mener en instruks fra Behandlingsansvarlig er i strid med Personvernregelverket.

3. Geografisk område

Databehandleren skal kun behandle personopplysningene innenfor EØS-området og kan ikke overføre opplysningene til andre land, med mindre dette er skriftlig og uttrykkelig avtalt med Behandlingsansvarlig.

4. Vurdering av personvernkonsekvenser

Databehandleren skal bistå Behandlingsansvarlig med å vurdere personvernkonsekvenser av den behandlingen Databehandleren skal foreta, og med eventuelle forhåndsdrøftinger med Datatilsynet, jf. Personvernforordningens Artikkel 35 og 36.

5. Personopplysningssikkerhet

Databehandleren skal gjennomføre slike tekniske og organisatoriske tiltak som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå i tråd med Personvernregelverket, herunder særlig Personvernforordningens Artikkel 32. Databehandleren skal også bistå Behandlingsansvarlig med å gjennomføre slike tiltak.

Databehandleren skal dokumentere sine tiltak, og dokumentasjonen skal være tilgjengelig på Behandlingsansvarliges forespørsel.

Det skal foretas jevnlig sikkerhetsrevisjoner, i henhold til nærmere avtale mellom partene. Revisjonene skal omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

6. Brudd på personopplysningssikkerheten

Dersom Databehandleren får kjennskap til et brudd på personopplysningssikkerheten skal han uten ugrunnet opphold varsle den Behandlingsansvarlige.

Varselet skal overholde de krav som fremgår av Personvernforordningens Artikkel 33 nr. 2 og 3, og skal for øvrig inneholde all relevant informasjon knyttet til bruddet som Databehandler har kjennskap til. Dersom Databehandleren senere blir kjent med ytterligere forhold knyttet til bruddet, skal han uten ugrunnet opphold ettersende informasjon om dette til Behandlingsansvarlig.

Eventuell melding til Datatilsynet og/eller den registrerte skal skje gjennom Behandlingsansvarlig, med mindre annet er spesifikt avtalt mellom Partene.

Databehandleren skal bistå Behandlingsansvarlig med å oppfylle de krav som stilles til Behandlingsansvarliges håndtering av brudd på personvernssikkerheten.

7. Henvendelser fra de registrerte

Databehandleren skal uten ugrunnet opphold varsle Behandlingsansvarlig om eventuelle henvendelser fra de registrerte.

Databehandleren skal bistå Behandlingsansvarlig med å besvare henvendelser vedrørende de registrertes rettigheter etter Personvernforordningens kapittel III. Databehandleren skal ikke selv besvare henvendelser direkte, med mindre dette er spesifikt avtalt med Behandlingsansvarlig.

8. Bruk av underleverandør

Databehandleren kan bare benytte underleverandør/annen databehandler som er skriftlig forhåndsgodkjent av Behandlingsansvarlig.

Databehandleren skal inngå egne skriftlige databehandleravtaler med sine underleverandører som pålegger underleverandøren de samme avtale- og lovmessige forpliktelsene som Databehandleren er underlagt i henhold til denne Avtalen. Behandlingsansvarlig har rett til innsyn i disse avtalene.

Databehandleren er ansvarlig for at underleverandøren oppfyller sine forpliktelser knyttet til behandlingen av Behandlingsansvarliges personopplysninger.

Databehandleren benytter seg av følgende underleverandører:

NAVN PÅ UNDERLEVERANDØRER:	AVTALE:
MICROSOFT ONLINE SERVICES (OFFICE 365)	Vilkår for elektroniske tjenester
AMAZON WEB SERVICES	AWS Data Processing Agreement
LIFTIT	Databehandleravtale
SOPRA STERIA	Databehandleravtale
TIETO NORWAY AS	Databehandleravtale

9. Revisjon

Databehandleren skal gi Behandlingsansvarlig tilgang til slik dokumentasjon og informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene fastsatt i denne Avtalen, og for at Behandlingsansvarlig skal kunne gjennomføre revisjoner. Revisjoner kan blant annet omfatte stedlig inspeksjon og evaluering av systemer, organisering og sikkerhetstiltak, samt bruk av underleverandører. Revisjoner kan utføres av Behandlingsansvarlig selv eller av den han bemyndiger.

Databehandler vil fakturere medgått tid etter gjeldene satser for arbeid knyttet til revisjon.

10. Taushetsplikt

Partene har taushetsplikt om informasjon knyttet til den annen Part som mottas i forbindelse med gjennomføringen av denne Avtalen og levering av Tjenestene, herunder Behandlingsansvarliges personopplysninger. Taushetsplikten gjelder også etter Avtalens opphør.

Partene skal påse at ansatte og underleverandører som er involvert i gjennomføringen av denne Avtalen er underlagt tilsvarende taushetsplikt gjennom avtale eller lov.

11. Erstatningsansvar

Databehandleren er ansvarlig for skade som skyldes at Databehandleren har unnlatt å oppfylle sine forpliktelser etter Avtalen eller Personvernregelverket, eller for øvrig har opptrådt utenfor eller i strid med lovlige instruksjoner fra Behandlingsansvarlig.

Dersom Behandlingsansvarlig har vært direkte involvert i den skadevoldende behandlingen har Databehandleren rett til å kreve tilbake en forholdsmessig andel av en eventuell erstatningsutbetaling, jf. Personvernforordningens Artikkel 82.

12. Avtalens varighet

Denne Avtalen trer i kraft [] og gjelder inntil leveransen av Tjenestene opphører, med mindre Partene er enige om å avslutte Avtalen tidligere. Ved brudd på Avtalen eller Personvernregelverket kan Behandlingsansvarlig pålegge Databehandleren å stoppe den videre behandlingen av personopplysninger med umiddelbar virkning.

Ved Avtalens opphør skal Databehandleren på Behandlingsansvarliges instruks enten tilbakelevere eller slette/destruere alle personopplysninger han har behandlet på vegne av Behandlingsansvarlig, med mindre videre behandling er lovpålagt. Databehandleren skal innen rimelig tid skriftlig dokumentere at eventuell sletting/destruksjon er foretatt i henhold til Behandlingsansvarliges instruks.

Ved Avtalens opphør skal Databehandlerens tilgang til Behandlingsansvarliges systemer stenges. Databehandleren skal i nødvendig omfang bistå Behandlingsansvarlig med gjennomføringen av dette.

Databehandler vil fakturere arbeid med avvikling av tjenester og tilbakelevering av data etter gjeldene satser.

13. Endringer

Partene skal revidere Avtalen ved behov for tilpasninger til preceptorisk lovgivning og tolkninger av Personvernforordningen.

14. Vernetting

Denne Avtalen er underlagt norsk rett og Partene vedtar Databehandlers hjemting som vernetting. Dette gjelder også etter Avtalens opphør.

15. Vedlegg

Vedlegg 1

Beskrivelse av hvilke personopplysninger som finnes i de ulike systemene som Databehandler er databehandler for:

(fylles ut av Behandlingsansvarlig)

* * *

Denne Avtalen er i 2 – to eksemplarer, hvorav Partene har hvert sitt.

[sted og dato]

For Behandlingsansvarlig:

For Databehandler:

Navn:

Navn:

Tittel:

Tittel: