DATABEHANDLERAVTALE

MELLOM

NRK, org. no. 976 390 512
«Behandlingsansvarlig»

og

Leverandør, org. no. xxx xxx xxx
«Databehandler»

INNHOLD

1. BAKGRUNN, FORMÅL OG DEFINISJONER

Partene til denne Databehandleravtalen har inngått en avtale av (dato) («**Avtalen**») på bakgrunn av (bakgrunn/tema for hovedavtalen). Denne Databehandleravtalen regulerer partenes rettigheter og forpliktelser for å sikre at all Behandling av Personopplysninger skjer i henhold til gjeldende lovgivning om behandling av personopplysninger, herunder EUs personvernforordning 2016/679 («GDPR») og i gjeldende personvernlovgivning som gjennomfører denne.

Leverandør/databehandler/data importør vil behandle personopplysninger i den utstrekning det er nødvendig for å oppfylle Avtalen, som spesifisert i Vedlegg 1. I Vedlegg 1 spesifiseres:

- Bakgrunnen for, karakteren av, og formålet med behandlingen,
- kategorier av personopplysninger og kategorier av registrerte personer

NRK/behandlingsansvarlig/data eksportør fastsetter formål og hjelpemidler for Behandling i henhold til gjeldende lovgivning. Databehandler behandler kun personopplysninger på vegne av NRK og ikke til Databehandlers egne formål.

Begrepene «personopplysning», «sensitive personopplysninger», «behandling», «Behandlingsansvarlig», «Databehandler», «Den registrerte», etc. brukt i denne Databehandleravtalen skal ha samme betydning som etter GDPR og gjeldende personvernlovgivning.

2. NRKS PLIKTER

NRK bekrefter at NRK:

- har tilstrekkelig hjemmelsgrunnlag for Behandling av Personopplysninger,
- har rett til å la Databehandler behandle Personopplysningene,
- har ansvaret for nøyaktigheten, integriteten, innholdet, pålitelighet og lovligheten av Personopplysningene,
- skal implementere tilstrekkelige tekniske og organisatoriske tiltak for å sikre og dokumentere overholdelse av gjeldende lovgivning,
- informerer de registrerte i tråd med gjeldende lovgivning

NRK skal:

- varsle aktuelle tilsynsmyndigheter og/eller de registrerte iht. gjeldende personvernlovgivning i tilfelle avvik;
- svare på henvendelser fra de registrerte om Behandling av Personopplysninger i henhold til denne Databehandleravtalen,
- vurdere nødvendigheten av spesifikke tiltak som angitt i denne Databehandleravtalens pkt. 3.3.2 og 3.3.4, og bestille slike tiltak fra Databehandler.

3. DATABEHANDLERS PLIKTER

3.1 OVERHOLDELSE AV GJELDENDE RETT

Databehandler skal overholde alle bestemmelser for beskyttelse av Personopplysninger fastsatt i denne Databehandleravtalen og i gjeldende personvernlovgivning.

Databehandler skal overholde instrukser og rutiner gitt av NRK med hensyn til Behandling av Personopplysninger. Databehandler skal umiddelbart gi beskjed til NRK dersom Databehandler er av den oppfatning at en instruks fra NRK er i strid med gjeldende personvernlovgivning.

Databehandler skal bistå NRK i å sikre og dokumentere at NRK overholder sine forpliktelser under gjeldende personvernlovgivning.

3.2 RESTRIKSJONER FOR BEHANDLING

Databehandler skal bare behandle Personopplysninger på og i samsvar med instruks fra NRK, unntatt når:

i) Databehandler er forpliktet til å behandle Personopplysninger i henhold til preseptorisk lovgivning. I så fall skal Databehandler varsle NRK før behandlingen begynner, med mindre slik varsling er forbudt.

ii) Databehandler må behandle Personopplysninger for å oppfylle sine forpliktelser overfor NRK etter Avtalens opphør. I så fall skal denne Databehandleravtalen gjelde inntil behandlingen opphører.

3.3 INFORMASJONSSIKKERHET

3.3.1 Plikt til å sikre informasjonssikkerhet

Databehandler skal ved planlagte, systematiske, organisatoriske og tekniske tiltak sikre tilstrekkelig informasjonssikkerhet med hensyn til konfidensialitet, integritet, og tilgjengelighet i forbindelse med Behandling av Personopplysninger i samsvar med bestemmelser om informasjonssikkerhet i gjeldende lovgivning om Behandling av Personopplysninger.

En detaljert beskrivelse av tiltak for informasjonssikkerhet skal fastsettes i vedlegg 2.

3.3.2 Vurdering av tiltak

I vurderingen av hvilke tekniske og organisatoriske tiltak som skal implementeres, skal Databehandler i samråd med NRK ta i betraktning:

- beste praksis,
- kostnaden ved implementering,
- karakteren og omfanget av behandlingen,
- konteksten og formålet med behandlingen,
- alvorlighet av den risiko Behandlingen av Personopplysninger medfører for den registrertes rettigheter.

Databehandler skal, i samråd med NRK, vurdere:

- Implementering av pseudonymisering og kryptering av Personopplysninger
- Evnen til å sikre løpende konfidensialitet, integritet, tilgjengelighet og robustheten til systemer for behandling og tjenester
- Evnen til å gjenopprette tilgjengelighet og tilgang til personopplysninger til rett tid i tilfelle fysiske eller tekniske hendelser
- En prosess for jevnlig testing, vurdering og evaluering av effektiviteten til tekniske og organisatoriske tiltak for sikkerheten til Behandlingen

3.3.3 Forespørsler fra den registrerte

Tatt i betraktning arten av behandlingen, skal Databehandler implementere tilstrekkelige tekniske og organisatoriske tiltak for å støtte NRKs plikt til å svare på spørsmål om utøvelse av den registrertes rettigheter i henhold til GDPR kapittel 3.

3.3.4 Bistand til NRK

Databehandler skal gi bistand slik at NRK kan ivareta sitt eget ansvar etter lov og forskrift, herunder bistå NRK med å:

- Implementere tekniske og organisatoriske tiltak som nevnt over,
- overholde varslingsplikt til tilsynsmyndigheter og registrerte personer som følge av avvik,
- utføre vurdering av personvernkonsekvenser («data privacy impact assessments»),
- utføre forutgående drøftelser med tilsynsmyndigheter når en vurdering av personvernkonsekvenser gjør det nødvendig
- varsle NRK dersom Databehandler mener at en instruks fra NRK er i strid med gjeldende personvernregelverk.

Bistand som nevnt over, skal utføres i den utstrekning det er nødvendig ut fra NRK sitt behov, karakteren av behandlingen og informasjonen tilgjengelig for Databehandler.

3.4 PERSONOPPLYSNINGSSIKKERHETSBRUDD (AVVIK) OG AVVIKSMELDINGER

Enhver bruk av informasjonssystemene og Personopplysninger i strid med etablerte rutiner, instrukser fra NRK eller gjeldende personvernlovgivning skal behandles som avvik.

Databehandler skal ha rutiner og systematiske prosesser for å følge opp avvik, som skal inkludere reetablering av normaltilstanden, eliminasjon av årsaken til avviket, og hindre gjentagelse.

Databehandler skal uten ugrunnet opphold varsle NRK om:

i) personopplysningssikkerhetsbrudd som innebærer
   a. en utilsiktet, ulovlig eller uautorisert tilgang, bruk eller utlevering av Personopplysninger
   b. at Personopplysninger kan ha blitt kompromittert eller
   c. brudd på Personopplysningenes integritet.

ii) ethvert annet avvik fra denne Databehandleravtalen

Databehandler skal varsle avvik til personvern@nrk.no og til NRKs kontaktperson for Avtalen.

Databehandler skal gi NRK all informasjon nødvendig for å sette NRK i stand til å overholde gjeldende lovgivning om behandling av personopplysninger og sette NRK i stand til å besvare henvendelser fra datatilsynsmyndigheter. Det er NRK sitt ansvar å melde avvik til Datatilsynet i henhold til gjeldende lovgivning.

3.5 KONFIDENSIALITET

Databehandler har taushetsplikt om personopplysninger og annen konfidensiell informasjon, herunder men ikke begrenset til, forretningshemmeligheter. Databehandler skal sikre at alle som utfører arbeid for Databehandler, enten ansatte eller innleide, som har tilgang til eller er involvert i Behandling av personopplysninger etter Avtalen (i) er underlagt taushetsplikt og (ii) er informert om og overholder forpliktelsene etter denne Databehandleravtalen. Taushetsplikten gjelder også etter opphør av Avtalen eller Databehandleravtalen.

3.6 SIKKERHETSREVISJONER

Databehandler vil jevnlig, enten selv eller ved hjelp av tredjepart, foreta sikkerhetsrevisjoner for systemer og lignende som er relevant for Behandlingen av Personopplysninger som omfattes av denne Databehandleravtalen. NRK skal ha tilgang til rapporter som dokumenterer sikkerhetsrevisjoner.

NRK har rett til å kreve sikkerhetsrevisjon utført av uavhengig tredjepart. Vedkommende tredjepart vil utarbeide en rapport som vil bli overlevert NRK på forespørsel. NRK er innforstått med at Databehandler kan beregne kompensasjon for gjennomføringen av revisjonen.

NRK kan vise slik rapport til tilsynsmyndigheter og andre som har krav på å kjenne innholdet.

3.7 BRUK AV UNDERLEVERANDØRER

Enhver underleverandør skal godkjennes skriftlig av NRK før underleverandøren kan behandle personopplysninger. Databehandler har rett til å benytte underleverandører og NRK aksepterer underleverandører som angitt i Vedlegg 1. Databehandler skal, i skriftlig avtale med enhver underleverandør, sikre at Behandling av Personopplysninger utført av underleverandører skal være underlagt de samme forpliktelser og begrensninger som de pålagt Databehandler i henhold til denne Databehandleravtalen.

Dersom Databehandler planlegger å skifte ut eller benytte ny underleverandør, skal Databehandler skriftlig innhente godkjenning fra NRK senest innen ny underleverandør starter Behandling av Personopplysninger. Dersom NRK motsetter seg endringen, kan NRK si opp avtalen med 3 måneders oppsigelsestid. Dersom NRK ikke sier opp avtalen, anses den nye underleverandøren akseptert. Partene skal til enhver tid holde listen over godkjente underleverandører i vedlegg 2 oppdatert.

3.8 OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJELAND

Databehandleren skal ikke overføre Personopplysninger utenfor Det europeiske økonomiske samarbeidsområde (EØS), eller gi noen utenfor EØS (herunder underleverandører) tilgang til Personopplysninger som behandles på vegne av NRK, uten skriftlig forhåndssamtykke fra NRK. For å unngå enhver tvil, gjelder det samme dersom opplysningene lagres i EØS, men kan aksesseres av personell som er lokalisert utenfor EØS.

Dersom NRK har gitt sitt skriftlige samtykke til overføring av Personopplysninger til et land utenfor EØS som ikke er ansett å sikre et tilstrekkelig beskyttelsesnivå i henhold til GDPR («Tredjeland») skal Databehandler samarbeide med NRK om å sikre lovligheten av overføringene. Databehandler forplikter seg herunder, på forespørsel fra NRK, til å inngå EUs standardavtale for overføring av personopplysninger til databehandlere i tredjeland (2010/87/EC) eller andre bestemmelser som erstatter disse vilkårene, i NRK navn og på den NRKs vegne. Databehandler påtar seg å sende en kopi av den signerte EU standardavtalen til NRK. Databehandler skal videre bistå med å sikre at det, når det er nødvendig, etableres tilleggstiltak for å sikre et forsvarlig vernenivå i Tredjelandet.

4. ANSVAR, BRUDD

4.1 Prosedyre

I tilfelle brudd på denne Databehandleravtalen, eller forpliktelser etter gjeldende lovgivning om Behandling av Personopplysninger, skal de relevante bestemmelser i Avtalen om prosedyre for håndtering av brudd/mislighold komme til anvendelse.

Databehandler skal varsle NRK uten ugrunnet opphold dersom Databehandler ikke vil være, eller har grunn til å tro at den ikke vil være, i stand til å overholde sine forpliktelser etter denne Databehandleravtalen.

4.2 Ansvar og ansvarsbegrensning

Databehandler er erstatningsansvarlig for direkte økonomisk tap, herunder bot og lignende administrative sanksjoner og gebyrer, erstatningskrav som rettes mot NRK, som stammer fra Databehandlers brudd på noen av sine forpliktelser i henhold til denne Databehandleravtalen. I den grad Databehandlerens underleverandører bryter noen av forpliktelsene ihht. denne Databehandleravtalen er Databehandler på samme måte erstatningsansvarlig overfor NRK.

Hvis én av eller begge Parter blir ilagt overtredelsesgebyr etter GDPR artikkel 83, skal den parten som vedtaket retter seg mot, betale gebyret. Hvis NRK er ilagt overtredelsesgebyr som følge av at Databehandler har misligholdt Avtalen, har NRK krav på erstatning tilsvarende overtredelsesgebyrets størrelse. Hvis overtredelsesgebyret også skyldes NRK sitt forhold, reduseres Databehandlers ansvar tilsvarende. Eventuell ansvarsbegrensning fastsatt i Avtalen gjelder ikke i disse tilfeller.

Har Databehandler eller noen denne svarer for utvist grov uaktsomhet eller forsett, gjelder ikke de nevnte erstatningsbegrensningene.

5. VARIGHET, AVSLUTNING AV DATABEHANDLERAVTALEN, ENDRINGER

Denne Databehandleravtalen skal gjelde fra den dato den er signert av begge parter og inntil Avtalen utløper, eller inntil Databehandlers plikt til ytelse av tjenester i henhold til Avtalen opphører av annen grunn, med unntak av de bestemmelser i Avtalen og Databehandleravtalen som fortsetter å løpe etter avslutning.

Ved avslutning av denne Databehandleravtalen skal Personopplysninger og annen data returneres i standardisert format og medium sammen med nødvendige instruksjoner for å legge til rette for NRKs videre bruk av Personopplysningene og annen data. Databehandler skal først returnere og deretter slette alle Personopplysninger og annen data. Databehandler og dennes underleverandører skal umiddelbart stanse behandling av personopplysningene fra dagen fastsatt av NRK.

Som alternativ til å returnere Personopplysninger (eller andre data) kan NRK, etter egen vurdering, skriftlig instruere Databehandler om at alt eller deler av Personopplysningene (eller andre data) skal slettes av Databehandler, med mindre preseptorisk lovgivning forhindrer Databehandler fra slik sletting.

Databehandler har ikke rett til å beholde kopi av Personopplysninger eller annen data gitt av NRK i forbindelse med Avtalen eller denne Databehandleravtalen i noe format, og all fysisk og logisk tilgang til slike Personopplysninger eller data skal slettes.

Databehandler skal gi NRK en skriftlig erklæring, hvoretter Databehandler garanterer at alle Personopplysninger eller data nevnt ovenfor har blitt returnert eller slettet i henhold til NRKs instrukser, og at Databehandler ikke har beholdt noen kopi, utskrift eller beholdt dataene i annet medium.

Forpliktelsene etter pkt. 3.5 og 4 skal fortsette å gjelde etter avslutning. Videre skal bestemmelsene i Databehandleravtalen gjelde fullt ut for eventuelle Personopplysninger beholdt av Databehandler i strid med dette pkt. 5.

Partene skal revidere denne Databehandleravtalen i tilfelle relevante endringer i gjeldende lovgivning.

6. TVISTER OG JURISDIKSJON

Denne Databehandleravtalen skal være underlagt og tolkes i samsvar med norsk rett. Verneting skal være Oslo tingrett.

7. SIGNATURER

Denne Databehandleravtalen er signert i to – 2 – eksemplar, en til hver av partene.

Dato:	Dato:
For Databehandler	For NRK
_____	_____
Navn:	Navn:
Tittel:	Tittel:

VEDLEGG 1 TIL DATABEHANDLERAVTALEN

Dette Vedlegg utgjør NRKs videre instrukser til Databehandleren i forbindelse med Databehandlers Behandling på vegne av NRK, og er en integrert del av denne Avtalen.

1. BEHANDLINGSAKTIVITETENES FORMÅL OG ART

[For eksempel: Databehandleren skal sende ut spørreundersøkelse på vegne av NRK, eks. Rambøll. I denne forbindelse vil Databehandleren bli gitt informasjon om mottakerne, eks. e-postadressen til NRKs medarbeidere for å kunne sende ut medarbeiderundersøkelse.]

2. KATEGORIER AV REGISTRERTE

Databehandleren skal Behandle Personopplysninger om følgende kategorier av Registrerte på vegne av NRK [sett inn videre beskrivelser av kategorier av Registrerte, om nødvendig]

a) [NRKs medarbeidere]

b)

3. KATEGORIER AV PERSONOPPLYSNINGER

[Sett inn en beskrivelse av kategoriene av opplysninger for hver kategori av registrerte som opplistet i pkt. 2 over]

Re a): [e-postadresse og navn]

Re b):

Re c):

4. SÆRLIGE KATEGORIER AV OPPLYSNINGER

[Sett inn beskrivelse av de særlige kategorier av opplysninger for hver kategori av registrerte. Særlige kategorier av opplysninger omfatter opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, genetiske opplysninger, biometriske opplysninger som behandles for å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, og personopplysninger om straffedommer og lovovertredelser.]

Re a):

Re b):

Re c):

5. LISTE OVER GODKJENTE UNDERLEVERANDØRER HERUNDER LOKASJON(ER), HERUNDER NAVN PÅ LAND FOR BEHANDLING

Navn	Org.nr.	Oppgave knyttet til behandlingen	Lokasjon for behandlingen (navn på land)

VEDLEGG 2

1. INNLEDNING

Det forventes at leverandører kan oppfylle minimumskravene til informasjonssikkerhet. Dette dokumentet er basert på ISO 27001 Controls og EBU R143 *Cybersecurity Recommendation for Media Vendors' Systems, Software & Services*.

2. ORGANISATORISKE TILTAK

Vennligst besvar følgende utsagn (J=JA, N=NEI eller N/A=Ikke relevant).

#	Beskrivelse	J	N	N/A	Kommentar
1	**Sikkerhetsstyring** Leverandøren har en sikkerhets-policy som regelmessig evalueres og holdes oppdatert.				
2	**Risikostyring** Leverandøren identifiser risiko knyttet til tjenesten og sørger for risikoreduserende tiltak.				
3	**Dataoverføring** NRKs data lagres og behandles kun i EU/EØS.				
4	**Personellsikkerhet** Bakgrunnssjekk foretas av alle medarbeidere som er involvert i oppdraget, f.eks. ID og CV-sjekk.				
5	**Leverandørkjeden** Leverandøren tar ansvar for sikkerheten i sin leverandørkjede.				

3. Tekniske tiltak

Vennligst besvar følgende utsagn (J=JA, N=NEI eller N/A=Ikke relevant).

#	Beskrivelse	J	N	N/A	Kommentar
6	**Sårbarhetshåndtering** Leverandøren har prosedyrer for å for å identifisere og patche sårbarheter.				
7	**Sikkerhetstesting** Leverandøren gjennomfører regelmessig sikkerhetsanalyser, som penetrasjonstest eller sårbarhetsskanning.				
8	**Hendelseshåndtering** Leverandøren har implementert prosedyrer for hendelseshåndtering.				
9	**Varsling** Leverandøren har rutiner for å varsle kunder om datalekkasje eller alvorlige hendelser.				
10	**Datagjenoppretting** Leverandøren har innført og testet rutiner for sikkerhetskopi og planer for gjenoppretting.				
11	**Tilgangsstyring** Leverandøren forsikrer at tjenesten støtter rollebasert tilgangskontroll og Azure AD SSO.				
12	**Kryptering av data** Leverandøren muliggjør kryptering av sensitive data, for både data i ro og i transitt.				
13	**Sikker utvikling** Leverandøren forsikrer at endringer i tjenesten skjer kontrollert gjennom en formell dokumentert prosess.				
14	**Skille mellom miljøer** Leverandøren holder miljøene for drift og test adskilt.				
15	**Segregering av kundedata** Leverandøren sørger for segregering av kundedata ved lagring i delte miljøer.				
16	**Fysisk sikkerhet** Leverandøren har adgangskontroll og fysisk sikring av sine lokaler.				

VEDLEGG 3 – RETTSLIG GRUNNLAG FOR OVERFØRING TIL TREDJELAND (LAND UTENFOR EU/EØS)

[EU-kommisjonens standard personvernbestemmelser (Standard Contractual Clauses eller SCCs) skal inntas her hvis aktuelt]
Overføring av personopplysninger ut av EØS | Datatilsynet