Eksempel på databehandleravtale. Denne skal fylles ut dersom det blir aktuelt.

BILAG T6
DATABEHANDLERAVTALE

MELLOM

NRK, org. no. xxx xxx xxx
«Behandlingsansvarlig»

og

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

INNHOLD

1. BAKGRUNN, FORMÅL OG DEFINISJONER

Partene til denne Databehandleravtalen har inngått en avtale om bistand til karriereveiledning i forbindelse med omstillingsprosesser i NRK (NRK MA3256/19E) av (dato) («**Avtalen**»). 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.

Databehandler vil behandler personopplysninger i den utstrekning det er nødvendig for å oppfylle Avtalen, som spesifisert i Appendix 1. I Appendix 1 spesifiseres:

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

Behandlingsansvarlig fastsetter formål og hjelpemidler for Behandling i henhold til gjeldende lovgivning. Databehandler behandler kun personopplysninger på vegne av og etter instruks fra Behandlingsansvarlig 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. BEHANDLINGSANSVARLIGES PLIKTER

Behandlingsansvarlig bekrefter at Behandlingsansvarlig:

- 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

Behandlingsansvarlig 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 FORPLIKTELSER

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 Behandlingsansvarlig med hensyn til Behandling av Personopplysninger. Databehandler skal umiddelbart gi beskjed til Behandlingsansvarlig dersom Databehandler er av den oppfatning at en instruks fra Behandlingsansvarlig er i strid med gjeldende personvernlovgivning.

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

3.2. RESTRIKSJONER FOR BEHANDLING

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

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

ii) Databehandler må behandle Personopplysninger for å oppfylle sine forpliktelser overfor Behandlingsansvarlig 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 Bilag 2. (Alternativ: En detaljert beskrivelse av tiltak for informasjonssikkerhet og internkontrolldokumentasjon gjøres tilgjengelig for Behandlingsansvarlig på forespørsel.)

3.3.2. Vurdering av tiltak

I vurderingen av hvilke tekniske og organisatoriske tiltak som skal implementeres, skal Databehandler i samråd med Behandlingsansvarlig 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 Behandlingsansvarlig, 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 Behandlingsansvarliges plikt til å svare på spørsmål om utøvelse av den registrertes rettigheter i henhold til GDPR kapittel 3.

3.3.4. Bistand til Behandlingsansvarlig

Databehandler skal gi bistand slik at Behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift, herunder bistå Behandlingsansvarlig 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 Behandlingsansvarlig dersom Databehandler mener at en instruks fra Behandlingsansvarlig er i strid med gjeldende personvernregelverk.

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

3.4. AVVIK OG AVVIKSMELDINGER

Enhver bruk av informasjonssystemene og Personopplysninger i strid med etablerte rutiner, instrukser fra Behandlingsansvarlig eller gjeldende personvernlovgivning, så vel som sikkerhetsbrudd, 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 umiddelbart - senest innen 36 timer - varsle Behandlingsansvarlig om:

i) ethvert brudd på denne Databehandleravtalen
ii) utilsiktet, ulovlig eller uautorisert tilgang, bruk eller utlevering av Personopplysninger, eller
iii) at Personopplysninger kan ha blitt kompromittert eller
iv) brudd på Personopplysningenes integritet.

Databehandler skal gi Behandlingsansvarlig all informasjon nødvendig for å sette Behandlingsansvarlig i stand til å overholde gjeldende lovgivning om behandling av personopplysninger og sette Behandlingsansvarlig i stand til å besvare henvendelser fra datatilsynsmyndigheter. Det er Behandlingsansvarlig 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 foreta sikkerhetsrevisjoner for systemer og lignende som er relevant for Behandlingen av Personopplysninger som omfattes av denne Databehandleravtalen. Behandlingsansvarlig skal ha tilgang til rapporter som dokumenterer sikkerhetsrevisjoner.

Behandlingsansvarlig har rett til å kreve sikkerhetsrevisjon utført av uavhengig tredjepart. Vedkommende tredjepart vil utarbeide en rapport som vil bli overlevert Behandlingsansvarlig på

forespørsel. Behandlingsansvarlig er innforstått med at Databehandler kan beregne seg en særskilt godtgjørelse for gjennomføringen av revisjonen i henhold til gjeldende timepriser.

Behandlingsansvarlig 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 Behandlingsansvarlig før underleverandøren kan behandle personopplysninger. Databehandler har rett til å benytte underleverandører og Behandlingsansvarlig aksepterer underleverandører som angitt i Bilag 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 varsle Behandlingsansvarlig 4 måneder før ny underleverandør starter Behandling av Personopplysninger, og Behandlingsansvarlig kan innen 1 måned varsle om at han motsetter seg endringen. Dersom Behandlingsansvarlig motsetter seg endringen, kan Behandlingsansvarlig si opp avtalen med 3 måneders oppsigelsestid. Dersom Behandlingsansvarlig ikke sier opp avtalen, anses den nye underleverandøren akseptert.

3.8. OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJELAND

Dersom Databehandler benytter underleverandør(er) utenfor EU/EØS («Tredjeland») for behandling av personopplysninger, må Behandlingen skje i henhold til EUs Privacy Shield Framework, EUs standardavtaler for overføring til tredjeland eller annet akseptert og spesifikt angitt grunnlag for overføring til tredjeland. For å unngå tvil, gjelder det samme dersom opplysningene lagres i EU/EØS, men kan aksesseres av personell som er lokalisert utenfor EU/EØS.

Dersom Behandlingsansvarlig godkjenner slik overføring, skal Databehandler samarbeide med Behandlingsansvarlig om å sikre lovligheten av overføringene.

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 Behandlingsansvarlig 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 Behandlingsansvarlig, 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 ovenfor Behandlingsansvarlig.

Samlet erstatning pr. kalenderår etter dette punkt 4.2 er begrenset til et beløp som tilsvarer X ganger Avtalens samlede årlige vederlag ekskl. merverdiavgift.

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 Behandlingsansvarliges 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 Behandlingsansvarlig.

Som alternativ til å returnere Personopplysninger (eller andre data) kan Behandlingsansvarlig, 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 Behandlingsansvarlig 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 Behandlingsansvarlig en skriftlig erklæring, hvoretter Databehandler garanterer at alle Personopplysninger eller data nevnt ovenfor har blitt returnert eller slettet i henhold til Behandlingsansvarliges 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 Behandlingsansvarlig
Sign.	Sign.
_____	_____
Navn: Kjellaug Tørstad	Navn:
Tittel:	Tittel:

APPENDIX 1 – SPESIFISERING AV BEHANDLINGSAKTIVITETER

1. KATEGORIER AV REGISTRERTE PERSONER

Personopplysningene som blir behandlet I henhold til Databehandleravtalen gjelder følgende kategorier av registrerte personer: Behandlingsansvarliges ansatte.

2. OPPLYSNINGSKATEGORIER

Kategoriene av personopplysninger som blir behandlet i henhold til Databehandleravtalen er:

Navn og kontaktinformasjon, samt eventuell informasjon som registreres i forbindelse med karriererådgivning eller økonomisk rådgivning til den enkelte ansatte.

3. SÆRLIGE KATEGORIER (SENSITIVE) PERSONOPPLYSNINGER (OM AKTUELT)

Personopplysningene som blir behandlet I henhold til Databehandleravtalen gjelder følgende særlige (sensitive) kategorier av personopplysninger:

- Rasemessig eller etnisk opprinnelse,
- politisk oppfatning, religion, filosofisk overbevisning eller
- fagforeningsmedlemskap,
- genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller
- opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering

4. FORMÅL MED BEHANDLINGEN

Formålet med behandling av personopplysninger iht. Avtalen er å tilby den Behandlingsansvarliges ansatte:

- Karriererådgivning
- Økonomisk rådgivning

5. BEHANDLINGSAKTIVITETER

Personopplysningene vil være gjenstand for følgende behandlingsaktiviiteter:
Registerering, analyse, bruk som grunnlag for fakturering, arkivering.

6. UNDERLEVERANDØRER LOKALISERT I EU/EEA (OM AKTUELT):

Not applicable

7. UNDERLEVERANDØRER LOKALISERT UTENFOR EU/EEA (SPESIFISÉR LAND OG RETTSLIG GRUNNLAG FOR OVERFØRING (OM AKTUELT):

Not applicable

8. FORMÅL OG BEHANDLINGSAKTIVITER FOR HVER UNDERLEVERANDØR (OM AKTUELT):

Not applicable

APPENDIX 2 – DATABEHANDLERS TEKNISKE OG ORGANISATORISKE TILTAK FOR INFORMASJONSSIKKERHET

(fylles inn av Databehandler)

APPENDIX 3 – APPLICABLE LEGAL BASIS FOR TRANSFER OF PERSONAL DATA TO THIRD COUNTIES

[EU Standard Contractual Clauses to be inserted if applicable]
https://www.datatilsynet.no/globalassets/global/skjema-maler/kontraktsvilkaar_overforing_eng.pdf