

Databehandleravtale til avtale om Kjøp av IKT – verktøy for FDV - arbeid

**Avtalen omhandler også håndtering av taushetsbelagt informasjon
og data.**

Mellom

Trøndelag fylkeskommune

Org.nr: 817 920 632

som Behandlingsansvarlig

og

X

Org.nr: xxx xxx xxx

som Databehandler

Behandlingsansvarlig og Databehandler benevnes i fellesskap «Partene».

Avtalen signeres i to eksemplarer, ett til hver av partene.

Denne databehandleravtalen (heretter «DBA») er knyttet til Avtale om kjøp av IKT – verktøy for FDV - arbeid med tilhørende vedlegg datert XX.XX.XX mellom partene, senere kalt «Leveranseavtalen».

DBA er avtale om behandling av personopplysninger som Databehandler skal foreta for Behandlingsansvarlig som følge av avtale inngått mellom partene, «Leveranseavtalen».

Databehandler er X og er den som behandler personopplysninger på vegne av Behandlingsansvarlig, Trøndelag fylkeskommune.

1. DATABASEHANDLERAVTALENS FORMÅL

Formålet med og gjenstand for behandlingen er å gjøre det mulig for Databehandler å behandle personopplysninger som kreves for levering av tjenestene, som angitt i Leveranseavtalen, på vegne av og til fordel for Behandlingsansvarlig. Behandlingen begynner og slutter med levering av tjenestene til Behandlingsansvarlig, som angitt i Leveranseavtalen.

Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig på den bakgrunn som følger ovenfor. Databehandler er ansvarlig for all behandling av personopplysninger som er nødvendig for gjennomføring av tjenesten som angitt i Leveranseavtalen og som Databehandler er forpliktet til å levere.

Formålet med behandlingen, varigheten av behandlingen, behandlingens art, de typer personopplysninger som skal behandles og kategorier av registrerte er nærmere definert i vedlegg til DBA.

Avtalen skal sikre at personopplysninger behandles i samsvar med de til enhver gjeldende kravene til behandling av personopplysninger, herunder bl.a. Europaparlaments- og rådsforordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger og om oppheving av direktiv 95/46/EF (personvernforordningen) som besluttet 27. april 2016, og norsk lov med tilhørende forskrifter som innføres som en følge av personvernforordningen som personopplysningsloven. I det følgende vil dette betegnes som «Rettsgrunnlaget».

Begreper og definisjoner benyttet i DBA skal forstås på samme måte som i Rettsgrunnlaget.

DBA fritar ikke Databehandleren for forpliktelser som etter Rettsgrunnlaget eller enhver annen lovgivning direkte er pålagt Databehandleren.

Databehandler skal behandle personopplysningene på den måten som er beskrevet i DBA, samt på annen måte dersom dette er skriftlig avtalt mellom Databehandleren og Behandlingsansvarlig. Databehandler skal kun behandle personopplysninger basert på dokumenterte instruksjoner fra Behandlingsansvarlig og i samsvar med formålet til DBA.

DBA regulerer også partenes rettigheter og plikter ved behandling av data og informasjon som er underlagt taushetsplikt i medhold av annen lov eller avtale.

Avtalen skal sikre at personopplysninger eller annen taushetsbelagt informasjon, ikke brukes urettmessig eller kommer uberettigede i hende.

2. RANGORDNING

Ved motstrid skal følgende tolkningsprinsipper legges til grunn:

1. DBA har forrang ved eventuell motstrid med Leveranseavtalens bestemmelser når det gjelder behandling av personopplysninger.
2. Den generelle avtaleteksten i DBA går foran vedleggene.

DBA bestemmelser har rang foran Databehandlers eventuelle egne personvernvilkår, eller eventuelle andre vilkår som måtte inngå i eller påvirke avtaleforholdet i denne DBA og/eller Leveranseavtalen, herunder avtaler mellom Databehandler og dennes underleverandører eller tredjeparter og eventuelle personvernvilkår disse måtte ha.

Dersom Databehandler eller underleverandør/tredjeparter har vilkår som ikke er regulert i databehandleravtalen og som strider mot personopplysningsloven skal «Rettsgrunnlaget» gå foran.

3. OVERFØRING AV PERSONOPPLYSNINGER TIL LAND UTENFOR EU/EØS(TREDJELAND)

Overføring av personopplysninger til tredjeland forutsetter at overføringen er i samsvar med Rettsgrunnlaget, herunder skal Databehandler sikre at overføringen er i samsvar med kapittel V i personvernforordningen.

Ved overføring av personopplysninger til tredjeland eller en internasjonal organisasjon skal Databehandler behandle personopplysninger kun på dokumentert instruks fra Behandlingsansvarlig. Databehandleren skal altså ikke overføre eller la personer i tredjeland på noen måte få tilgang til personopplysninger uten at Behandlingsansvarlig har eksplisitt godkjent dette skriftlig og gitt instruks om overføring eller tilgang på forhånd. Samtykke og instruks må dekke hvilke land opplysningene skal overføres til. Overføring til tredjeland forutsetter, selv med samtykke og instruks, at de krav til sikkerhet og vern av de registrertes rettigheter som følger av personopplysningsloven og annet regelverk er ivarettatt.

Overføring av personopplysninger til tredjeland forutsetter at overføringen er i samsvar «Rettsgrunnlaget» i hele avtaleperioden.

For å overholde kravene i Rettsgrunnlaget for overføring av personopplysninger til databehandlere etablert i tredjeland, skal EUs standardkontrakter, (Standard Contractual Clauses) for overføring av personopplysninger til databehandlere etablert i tredjeland vedtatt av EU-kommisjonen, benyttes. Det skal i tillegg inngås en databehandleravtale.

Overføring til tredjeland forutsetter i tillegg til ovennevnte at de krav til sikkerhet og vern av de registrertes rettigheter som følger av Rettsgrunnlaget og annet regelverk ivaretas.

4. BEHANDLINGSANSVARLIGES RETTIGHETER OG PLIKTER. DATABASEHANDLERS PLIKTER

Databehandler forplikter å behandle personopplysninger kun i samsvar med Rettsgrunnlaget, denne DBA, som angitt i Leveranseavtalen og Behandlingsansvarlig sine dokumenterte instruksjer. Databehandler skal følge alle rutiner og instruksjer for behandlingen som Behandlingsansvarlig til enhver tid har bestemt skal gjelde.

Databehandler bekrefter at denne vil gjennomføres egnede tekniske og organisatoriske tiltak som sikrer at all behandling av personopplysninger under denne DBA oppfyller kravene i Rettsgrunnlaget og vern av den registrertes rettigheter, herunder innfrir alle kravene etter personvernforordningens art. 28. Se ytterlige plikter i pkt. 5 til 8.

Den Behandlingsansvarlige er ansvarlig for at personopplysninger blir behandlet i samsvar med Rettsgrunnlaget, jfr. artikkel 24. Behandlingsansvarlig har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som skal brukes i behandlingen. Den Behandlingsansvarlige skal til enhver tid ha full rettslig rådighet over personopplysningene. Den Behandlingsansvarlige har rett til å heve avtalen dersom Databehandleren ikke lenger oppfyller lovens krav etter artikkel 28 nr. 1.

Databehandleren skal kun behandle personopplysningene basert på dokumenterte instruksjer fra den Behandlingsansvarlige. Dokumenterte instruksjer for hvordan personopplysninger skal behandles kan være en del av avtalen eller lagt ved som et vedlegg til avtalen. Databehandleren skal til enhver tid kunne dokumentere slike instruksjer. Databehandler skal ikke behandle personopplysninger Databehandleren får tilgang til på annen måte enn det som er nødvendig for å utføre de oppdrag som Databehandler har for den Behandlingsansvarlige.

Databehandler skal gjøre tilgjengelig for den Behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i artikkel 28 er oppfylt, samt muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av den Behandlingsansvarlige eller en annen revisor på fullmakt fra den Behandlingsansvarlige. Den Behandlingsansvarlige har selv det direkte ansvaret for kontakt og kommunikasjon med aktuelle tilsynsmyndigheter, herunder Datatilsynet.

Databehandler skal også omgående underrette den Behandlingsansvarlige dersom vedkommende mener at en instruks er i strid med Rettsgrunnlaget eller andre bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett.

Databehandler skal, idet det tas hensyn til behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak, den Behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.

Foreligger det godkjente adferdsnormer etter personvernforordningens artikkel 40 eller godkjent sertifiseringsordning etter artikkel 42, som Databehandleren har påtatt seg å overholde eller være sertifisert etter, plikter Databehandleren å etterkomme slike

adferdsnormer eller sertifiseringskrav.

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.

Databehandleren har taushetsplikt om personopplysninger som vedkommende får tilgang til som en følge av DBA og behandling av personopplysningene, og skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. Plikten til *konfidensialitet* gjelder også etter at databehandleroppdraget er fullført.

Databehandleren skal sikre at kun autoriserte personer har tilgang til opplysningene, og at Databehandleren fratar tilgangen dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder for personen.

Databehandleren skal kun autorisere personer som av nødvendige grunner må ha tilgang til personopplysningene.

Underdatabehandler (e) som på vegne av Databehandler utfører oppdrag der bruk av/ tilgang til personopplysningene inngår, skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser ovenfor Behandlingsansvarlig og påta seg å etterleve disse.

Databehandleren skal, etter anmodning fra den Behandlingsansvarlige, kunne påvise at de autoriserte personene er underlagt fortrolighet eller taushetsplikt - ved å fremlegge dokumentasjon.

Databehandler skal beskrive i eget vedlegg hvordan forpliktelsene etter dette punkt 4 blir ivaretatt, som vedlegg 2 til denne DBA.

4.1. Tekniske, organisatoriske og sikkerhetsmessige tiltak

Databehandler skal oppfylle de krav til sikkerhetstiltak (personopplysningssikkerhet) som stilles i Rettsgrunnlaget. Databehandler skal bekrefte at den vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne DBA oppfyller kravene i Rettsgrunnlaget, herunder innfrir alle krav i personvernforordningen art. 32. Eventuelle minimumskrav til sikkerhetstiltak beskrives i et eget vedlegg til DBA. Hvilke tekniske og organisatoriske tiltak som Databehandler har gjennomført/vil gjennomføre, skal fremgå i eget vedlegg til DBA.

Databehandler skal bistå den Behandlingsansvarlige med å sikre overholdelse av forpliktelsene i henhold til artikkel 32-36, herunder personopplysningssikkerhet (art.32), melding av brudd på personopplysningssikkerheten (art. 33), underretning av den registrerte (art. 34), vurdering av personvernkonsekvenser (art.35) og forhåndsdrøftinger (art. 36), idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren.

Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

5. BRUK AV UNDERLEVERANDØRER/UNDERDATABEHANDLER

Databehandleren skal kun benytte underleverandører til behandling av personopplysninger (underdatabehandler) som er skriftlig godkjent av den Behandlingsansvarlige og som har bekreftet å gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne DBA oppfyller kravene i Rettsgrunnlaget og vern av den registrertes rettigheter.

Godkjente underdatabehandlere ved Avtalens inngåelse skal spesifiseres i vedlegg til DBA eller Leveranseavtalen.

Underdatabehandler skal pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i DBA i bindende avtale hvor underdatabehandler skal gi tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i Rettsgrunnlaget. Dersom underdatabehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger og kravene i DBA, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser.

Databehandler skal garantere for at underdatabehandler(e) har bekreftet å gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne DBA oppfyller kravene i Rettsgrunnlaget.

Det skal inngås en databehandleravtale mellom Databehandler og underdatabehandler.

6. SIKKERTHET OG AVVIK

Databehandleren skal oppfylle de krav til sikkerhetstiltak som stilles etter Rettsgrunnlaget. Databehandleren skal kunne dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på den Behandlingsansvarliges forespørsel.

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.

Den Behandlingsansvarlige har ansvaret for å sende melding til tilsynsmyndighet, og Databehandler skal ikke sende slik melding eller kontakte tilsynsmyndighet uten at den Behandlingsansvarlige har gitt instruks om dette.

7. AVTALENS VARIGHET, PÅLEGG OM STANS, PLIKTER VED OPPHØR/OPPSIGELSE

Avtalen gjelder så lenge Databehandleren behandler eller har tilgang til personopplysninger på vegne av Behandlingsansvarlige etter Leveranseavtalen.

Ved brudd på denne DBA, personopplysningsloven eller annet relevant regelverk, kan Behandlingsansvarlig pålegge Databehandleren å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandleren skal, etter den Behandlingsansvarliges instruksjon, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og sletter eksisterende kopier, med mindre det er et lovmessig krav om at personopplysningene skal fortsatt lagres. Dette gjelder også for eventuelle sikkerhetskopier, men hvor det er tilstrekkelig med å overskrive etter de etablerte rutiner for sikkerhetskopiering.

Den Behandlingsansvarlige skal motta en skriftlig bekreftelse fra Databehandleren på at alle personopplysninger er returnert eller slettet i henhold til den Behandlingsansvarliges instruksjoner og at Databehandleren ikke har beholdt kopi, utskrifter eller andre former for personopplysninger i noen form.

8. MEDDELELSER

Meddelelser, underretning, instruks, varsel eller annen kommunikasjon mellom Partene etter denne Databehandleravtalen skal sendes skriftlig til kontaktperson for Leveranseavtalen.

Dersom Databehandler mottar henvendelser fra tredjeparter, herunder registrerte og tilsynsmyndigheter, skal Databehandler videreformidle henvendelsen til Behandlingsansvarlig snarest. Med mindre annet er skriftlig avtalt, og så langt det er mulig, skal Behandlingsansvarlig selv ha kontakten med tredjeparter.

Kontaktopplysninger for å melde brudd på personopplysningssikkerheten:

personvernombudet@trondelagfylke.no

9. BESTEMMELSER OM VEDERLAG OG DEKNING AV KOSTNADER

Partenes eventuelle regulering/avtale om vederlag eller lignende i forbindelse med Databehandlerens bistand til Behandlingsansvarlig, fremgår av Leveranseavtalen.

10. ØVRIGE PLIKTER OG RETTIGHETER

Øvrige plikter og rettigheter følger av Leveranseavtalen som gjelder mellom

Databehandleren og Behandlingsansvarlige om tjenestene som nødvendiggjør behandling av personopplysninger og denne DBA. De samme kontaktpersoner gjelder for DBA som etter Leveranseavtalen.

Dersom Databehandler misligholder sine forpliktelser etter denne DBA, skal anvendbare bestemmelser i Leveranseavtalen om mislighold og sanksjoner benyttes. Denne DBA skal ikke utvide Behandlingsansvarliges sanksjonsmuligheter, herunder erstatningsansvar for Databehandleren, utover det som følger av Leveranseavtalen.

Ved eventuell overdragelse av Leveranseavtalen til andre parter, skal denne DBA overdras tilsvarende.

11. TVISTER

Partenes rettigheter og plikter etter denne DBA bestemmes i sin helhet av norsk rett.

Leveranseavtalens bestemmelser om tvisteløsning og vernetting gjelder også for denne DBA. Dersom Leveranseavtalen ikke har bestemmelser om tvisteløsning og vernetting, gjelder pkt. 11.1. og 11.2 nedenfor.

11.1. TVISTELØSNING

Dersom det oppstår uenighet mellom partene om tolkning eller rettsvirkninger av DBA, skal partene først forsøke å bli enige gjennom forhandlinger og/eller mekling.

11.2. VERNETING

Dersom en tvist ikke blir løst ved forhandlinger eller mekling, kan hver av partene forlange tvisten avgjort med endelig virkning ved norske domstoler.

Partene vedtar ved denne DBA Sør-Trøndelag tingrett som vernetting ved uoverensstemmelser rundt praktiseringen og gjennomføringen av denne DBA.

Trondheim_____._____2019

Databehandler

Behandlingsansvarlig

NAVN

NAVN

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

Vedlegg 1

Formålet med behandlingen

[Ta inn hva som er formålet eller hensikten med behandlingen. Her kan det bare tas inn en enkel beskrivelse på hvorfor personopplysninger samles inn og behandles, f.eks: "For å levere de tjenester som følger av Hovedavtalen."].

Varigheten av behandlingen

[Det skal inntas hvor lang varighet behandlingen skal ta. Dersom varigheten følger av en avtale mellom partene, så kan varigheten inntas som «Behandlingen skal vare å lenge Databehandleren yter tjenestene etter Hovedavtalen til Behandlingsansvarlig».]

Behandlingens art

[Her skal det angis hva behandlingen går ut på, som kan f.eks. være «Lagring av personopplysninger eller det som nødvendiggjør behandlingen under Hovedavtalen.»]

Typer personopplysninger som skal behandles

Følgende personopplysninger skal behandles under Avtalen:

[Det skal tas inn typen personopplysninger f.eks. personnavn, epostadresse, telefonnummer mv. Det er ikke nødvendig å være detaljert i hvilke opplysninger som skal behandles, men kun *typen* opplysninger.]

Kategorier av registrerte

[Kategorier av registrerte skal angis, som f.eks. ansatte, kunder, mv.]

Underdatabehandlere ved inngåelse av Avtalen

[Ta inn underdatabehandlere og land dataene vil bli behandlet. Dette vil som regel databehandler vite om.]

