

Databehandleravtale

Leverandøren trenger ikke å fylle ut malen for databehandleravtale som en del av sitt tilbud. Leverandøren som tildeles kontrakt i konkurransen skal fylle ut/komplettere malen for databehandleravtale før kontraktsignering (se rød tekst).

Generell avtaletekst

1. DEFINISJONER

Leverandøren: Med Leverandøren menes den juridiske enheten som leverer ytelser til Kunden hvor Leverandøren på en eller annen måte behandler personopplysninger på vegne av Kunden. Leverandøren er avtalepart med Kunden i Hovedavtalen.

Databehandler: Leverandøren.

Kunden: Med Kunden menes den juridiske enheten som kjøper ytelser fra Leverandøren hvor Leverandøren på en eller annen måte behandler personopplysninger på vegne av Kunden. Kunden er avtalepart med Leverandøren i Hovedavtalen.

Behandlingsansvarlig: Kunden (det selskap som mottar ytelser fra Leverandøren som omfatter behandling av personopplysninger).

Part: Kunden eller Leverandøren.

Partene: Kunden og Leverandøren. Nærmere informasjon om Partene fremgår av Vedlegg 1 pkt. 1.

Hovedavtalen: Gjeldende avtale mellom Kunden og Leverandøren som angir hva Leverandøren skal levere til Kunden og kommersielle betingelser. Denne Databehandleravtalen regnes som et vedlegg til Hovedavtalen og medfører ingen endringer av de kommersielle betingelsene som følger av Hovedavtalen.

Databehandleravtalen: Disse vilkårene med bilag og eventuelle endringer og oppdateringer som er skriftlig avtalt mellom Partene (elektronisk likestilles med skriftlig). Bestemmelsene i denne Databehandleravtalen har forrang i forhold til eventuelle tilsvarende bestemmelser i andre avtaler mellom Partene Databehandleravtalen er utarbeidet i henhold til

personopplysningsloven, veileder fra Datatilsynet og GDPR. Databehandleravtalen gjelder mellom Kunden som behandlingsansvarlig og Leverandøren som databehandler i personopplysningslovens forstand. Databehandleravtalen skal være skriftlig, herunder elektronisk.

GDPR: EUs generelle personvernforordning General Data Protection Regulations (Europaparlaments- og Rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF) som gjelder som norsk lov fra 20. juli 2018.

2. DATABEHANDLERAVTALENS HENSIKT

Databehandleravtalens hensikt er å regulere rettigheter og plikter etter gjeldende personopplysningslov i Norge med tilhørende regelverk. Databehandleravtalens oppfyller minstekrav i personopplysningsloven og GDPR.

Databehandleravtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende. Databehandleravtalen regulerer Databehandlers bruk av personopplysninger på vegne av den Behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

3. DATABEHANDLERAVTALENS FORMÅL

Formålet med Databehandleravtalen er å presisere at Leverandøren som Kundens databehandler også kan behandle personopplysninger innenfor det som er avtalt med Kunden, herunder foreta de behandlinger som følger av Hovedavtalen, for å foreta de behandlinger som Kunden ber Leverandøren bistå Kunden med eller for å fullføre Leverandørens avtaleforhold med Kunden slik det er til enhver tid. Partene er enige om at nye formål/behandlinger må

dokumenteres (skriftlig på en eller annen måte – elektronisk aksepteres som skriftlig).

Databehandleren og enhver person som handler for Databehandleren som har tilgang til personopplysninger, skal behandle nevnte opplysninger bare på dokumenterte **instrukser** fra Behandlingsansvarlig. Partene er enige i at det som angis i denne Databehandleravtalen, skal anses som slike instrukser fra Behandlingsansvarlig.

Hvilke **personopplysninger** som skal behandles: Alle personopplysninger som Leverandøren gir tilgang til av Kunden eller på annen måte behandler gjennom avtaleforholdet med Kunden. Hvilke personopplysninger som behandles i henhold til denne Databehandleravtalen, er nærmere spesifisert i Vedlegg 1.

Kategorier av **registrerte**: Kundens egne ansatte, Kundens innleide personer, Kundens eiere og ledelse, kontaktpersoner tilknyttet Kundens leverandører eller kunder, Kundens øvrige kontraktparter som benytter løsningen fra Leverandøren etter Hovedavtalen samt andre sluttbrukere Kunden tilknytter Leverandørens tilbudte produkter eller tjenester. Kategorier av registrerte er nærmere beskrevet i Vedlegg 1 pkt. 3 til denne Databehandleravtalen.

Hvilke **behandlinger** som omfattes av Databehandleravtalen: De behandlinger som er nødvendige for at Leverandøren kan oppfylle sine forpliktelser som Leverandør til Kunden og som databehandler etter gjeldende regelverk samt den behandling som følger av Hovedavtalen og det løpende avtaleforholdet mellom Partene. Databehandler skal også ha rett til å behandle personopplysningene i den grad slik behandling er nødvendig som følge av det løpende avtaleforholdet mellom Partene etter Hovedavtalen, herunder for å kunne gi råd til Behandlingsansvarlig vedrørende forhold som kan forbedre ytelsene som leveres etter Hovedavtalen. Behandlinger som omfattes av denne Databehandleravtalen, er nærmere beskrevet i Vedlegg 1 pkt. 3.

Hva som er **rammene** for Databehandlers håndtering av personopplysninger: Leverandøren kan håndtere personopplysninger i henhold til rammene gitt av Kunden i Hovedavtalen og i det løpende avtaleforhold mellom Partene til enhver tid og for å oppfylle Leverandørens ansvar som Databehandler etter gjeldende regelverk.

4. DATABEHANDLERS PLIKTER

Databehandler skal følge de rutiner og instrukser for behandlingen som Behandlingsansvarlig til enhver tid har bestemt skal gjelde. Databehandleren plikter å gi Behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå slik at Behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandleren plikter å gi nødvendig bistand til dette.

Databehandleren har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne Databehandleravtalen. Denne bestemmelsen gjelder også etter Databehandleravtalens opphør. Databehandleren skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene konfidensielt ved taushetserklæring i ansettelsesavtale eller annen avtale med Databehandler dersom slik person ikke er underlagt en egnet lovfestet taushetsplikt. I tillegg skal kun personer som har saklig behov for tilgang til opplysningene gis tilgang. Listen over personer som har fått tilgang til personopplysningene skal gjennomgås løpende. På bakgrunn av denne gjennomgangen skal tilgangen til personopplysningene fjernes hvis tilgangen ikke lenger er nødvendig, og da skal personopplysningene ikke lenger gjøres tilgjengelig for disse personene.

Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen med behandlingen av personopplysningene samt for å sikre at behandlingen oppfyller kravene i gjeldende personvernlovgivning, herunder kravene som følger av GDPR, og vern av den registrertes rettigheter.

Databehandler skal, idet det tas hensyn til behandlingens art og i den grad det er mulig, bistå ved hjelp av egnede tekniske og organisatoriske tiltak. Databehandler skal bistå Behandlingsansvarlig med å oppfylle Behandlingsansvarliges plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter som den registrerte etter GDPR kapittel III. Databehandler skal, hensyntatt behandlingens art og den informasjonen som er tilgjengelig for Databehandleren, bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelsene den Behandlingsansvarlig har etter GDPR artikkel 32-36.

Databehandleren skal omgående underrette Behandlingsansvarlige dersom Databehandleren mener at en instruks fra Behandlingsansvarlig er i strid med GDPR eller andre lovbestemmelser om vern av personopplysninger. Databehandler skal føre en protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av Behandlingsansvarlig i henhold til GDPR art. 30 nr. 2.

5. BRUK AV UNDERLEVERANDØR

Dersom Databehandler benytter seg av underleverandører eller personer som ikke normalt er ansatt hos Databehandleren, skal dette avtales skriftlig med Behandlingsansvarlige før behandlingen av personopplysninger starter.

Leverandøren skal ikke engasjere en annen databehandler uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra Kunden siden Kunden er behandlingsansvarlig for personopplysningene. Dersom det er innhentet en generell skriftlig tillatelse, skal Leverandøren underrette Kunden om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi Kunden muligheten til å motsette seg slike endringer.

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

Dersom Databehandler engasjerer en annen databehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal nevnte andre databehandler pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne Databehandleravtalen. Dersom nevnte andre databehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar for at nevnte andre databehandler oppfyller sine forpliktelser.

En oversikt over godkjente underleverandører fremgår av Vedlegg 1 pkt. 4 til denne Databehandleravtalen. Vedlegg 1 pkt. 4 skal oppdateres dersom det gjøres endringer i bruk av underleverandører.

6. BEHANDLINGSANSVARLIGES RETTIGHETER OG PLIKTER

Behandlingsansvarlig har rettigheter og plikter som gjeldende lov til enhver tid gir den behandlingsansvarlige for behandling av personopplysninger.

Behandlingsansvarlig har ansvaret for å sikre at behandlingen av personopplysninger skjer i overensstemmelse med GDPR og personopplysningsloven.

Behandlingsansvarlig har rett og plikt til å treffe beslutninger om formålene med og midlene for behandlingen av personopplysninger.

Behandlingsansvarlig har ansvaret for å sikre at det er behandlingsgrunnlag for behandlingen av personopplysninger som databehandleren instrueres om å foreta.

Ved brudd på denne Databehandleravtalen eller personopplysningsloven kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandleren kan ikke kreve betalt for utførelsen av Databehandlerens plikter fastsatt i denne Databehandleravtalen som også følger av ufravikelig lov, herunder GDPR, særlig artikkel 28 - 36. Hvis en instruks fra Behandlingsansvarlig medfører at Databehandleren må gjøre mer enn det som følger som plikt etter lov, herunder GDPR, kan Databehandler ta betalt for slikt arbeid etter samme timesatser som angitt i Hovedavtalen.

7. SIKKERHET

Databehandleren skal oppfylle de krav til sikkerhetstiltak ved behandlingen som stilles etter gjeldende personopplysningslovgivning (GDPR artikkel 32). Databehandleren skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på forespørsel fra den Behandlingsansvarlige.

Både Behandlingsansvarlig og Databehandler skal begge vurdere risikoen for fysiske personers rettigheter og friheter som behandlingen utgjør og implementere tiltak for å imøtegå risikoen. Behandlingsansvarlig skal gi Databehandler all nødvendig informasjon for å identifisere og vurdere risikoen.

En oversikt over Databehandlerens tekniske og organisatoriske sikkerhetstiltak følger av Vedlegg 2 til denne Databehandleravtalen. De tekniske og organisatoriske sikkerhetstiltak kan forbedres og videreutvikles i samsvar med den teknologiske

utviklingen. I slike tilfeller har Databehandleren adgang til å implementere oppdaterte tekniske og organisatoriske sikkerhetstiltak, så lenge sikkerhetsnivået for de aktuelle sikkerhetstiltak forblir uendret eller endres til et høyere sikkerhetsnivå. Dersom det etter Behandlingsansvarliges vurdering er behov for ytterligere tiltak enn de tiltakene Databehandleren allerede har gjennomført for å imøtegå den identifiserte risikoen, skal Behandlingsansvarlig angi de ytterligere tiltakene som skal gjennomføres i Vedlegg 2.

Avviksmelding skal skje ved at Databehandleren melder avviket til Behandlingsansvarlig uten ugrunnet opphold. Dersom det er mulig, skal Databehandleren underrette Behandlingsansvarlig om avviket senest innen 48 timer. Behandlingsansvarlig har ansvaret for at avviksmelding sendes til Datatilsynet.

Databehandleren skal bistå Behandlingsansvarlig med å samle informasjonen listet nedenfor som også skal følge av Behandlingsansvarliges avviksmelding til Datatilsynet, jf. GDPR artikkel 33 (3):

- a) arten av bruddet på personopplysnings-sikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
- b) de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
- c) tiltakene som den Behandlingsansvarlige og Databehandleren har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følger av bruddet.

8. SIKKERHETSREVISJONER

Behandlingsansvarlig skal avtale med Databehandler at det gjennomføres sikkerhetsrevisjoner jevnlig for systemer og lignende som omfattes av denne Databehandleravtalen. Databehandler skal på forespørsel muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av Behandlingsansvarlig eller en annen revisor på fullmakt fra den Behandlingsansvarlige.

Databehandler skal på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i Databehandleravtalen er oppfylt.

Databehandlerens dokumenterte kostnader grunnet Behandlingsansvarliges inspeksjoner eller revisjon kan viderefaktureres som utlegg til Behandlingsansvarlig i neste faktura fra Databehandleren.

9. AVTALENS VARIGHET

Med mindre noe annet følger av Databehandleravtalen for konkrete bestemmelser i denne Databehandleravtalen, gjelder Databehandleravtalen så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig, og Databehandleravtalen følger samme regler for opphør som følger av Hovedavtalen.

10. VED OPPHØR

Etter den Behandlingsansvarliges valg, skal Databehandler slette eller tilbakelevere til Behandlingsansvarlig alle personopplysninger mottatt på vegne av Behandlingsansvarlig etter at tjenestene knyttet til behandlingen er levert (ved opphør av denne Databehandleravtalen).

Det kan ved opphør av Databehandleravtalen avtales at Databehandler skal slette eller forsvarlig destruere alle dokumenter, data, mv., som inneholder opplysninger som omfattes av Databehandleravtalen. Dette gjelder også for eventuelle sikkerhetskopier. Databehandler skal slette eksisterende kopier av slike personopplysninger, dokumenter og data, med mindre lovgivning krever at personopplysningene eller slike dokumenter/data lagres.

Databehandleren skal skriftlig dokumentere at sletting og/eller destruksjon er foretatt i henhold til Databehandleravtalen innen rimelig tid etter Databehandleravtalens opphør.

11. MEDDELELSER

Meddelelser etter denne Databehandleravtalen skal sendes skriftlig til Partenes oppgitte kontaktpersoner som angitt i Hovedavtalen mellom Partene. I Vedlegg 1 pkt. 2 kan andre kontaktpersoner fremgå, og da skal meddelelser etter denne Databehandleravtalen rettes til de i Vedlegg 1 pkt. 2 oppgitte kontaktpersoner.

12. ANSVAR

Partenes erstatningsansvar for skade som rammer den registrerte eller andre fysiske personer og som skyldes overtredelse av GDPR, personopplysningsloven med forskrifter eller annet regelverk som gjennomfører GDPR, følger av bestemmelsene i GDPR artikkel 82. Erstatningsbegrensningen i Hovedavtalen kommer ikke til anvendelse for ansvar som følger av GDPR artikkel 82. Partene er hver for seg ansvarlige for overtredelsesgebyr ilagt i henhold til GDPR art. 83.

13. TVISTELØSNING

Databehandleravtalen skal tolkes og reguleres i henhold til norsk rett. Eventuelle tvister mellom Kunden og Leverandøren knyttet til Databehandleravtalen skal avgjøres ved alminnelige norske domstoler. Søksmål skal i slike tvister reises for **[Sett inn gjeldende domstol]** som Partene vedtar som rett verneeting. Dette gjelder også etter opphør av Databehandleravtalen.

Vedlegg 1: Spesifikasjon av Leverandørens tjenester og behandling av personopplysninger som omfattes av Databehandleravtalen

1. PARTENE

Leverandøren (Databehandler): [Leverandøren] med org.nr. [Nr] og registrert forretningsadresse: [Adresse].

Kunden (Behandlingsansvarlig): [Kunden] med org.nr. [Nr] og registrert forretningsadresse: [Adresse].

2. KONTAKTPERSONER FOR MEDDELELSER

| | | |
|-------------------------------------|--------|------------------------------------|
| Leverandørens kontaktperson: | [Navn] | [E-postadresse] [Telefonnummer] |
| Kundens kontaktperson: | [Navn] | [E-postadresse] [Telefonnummer] |

Hovedavtalen gjelder for kontaktpersoner og varsling dersom tabellen ikke er utfylt.

3. NÆRMERE ANGIVELSE AV HVA DATABEHANDLERAVTALEN OMFATTER

Databehandleren skal i henhold til Hovedavtalen levere:

Hovedavtalen er kontrakten mellom Kunden og Leverandøren om levering av Rammeavtale IT forvaltning og vedlikehold og IT konsulentttjenester datert [...] (SSA-R med tilhørende bilag, avropsavtaler og senere endringsavtaler), hvor Databehandleren skal levere: IT konsulentttjenester.

Hvilke personopplysninger som behandles i henhold til Hovedavtalen:

Fylles inn

Kategorier av registrerte:

Fylles inn

Hvilke behandlinger som omfattes av avtalen:

Leverandørens behandlinger som er nødvendige for å oppfylle Leverandørens plikter etter Hovedavtalen. I tillegg omfattes behandlinger som er nødvendige for at Databehandleren oppfyller dets plikter og rettigheter etter denne Databehandleravtalen, instruks fra Kunden eller relevant lovgivning eller for å foreslå forbedringer av datasikkerheten for personopplysninger som behandles.

Nærmere om rammene for behandlingen:

Leverandøren med Leverandørens underleverandører behandler kun personopplysninger [i Norge med sikker lagring i land i EU/EØS]. Dersom Databehandleren planlegger å overføre eller behandle personopplysninger utenfor EU/EØS, skal Databehandleren varsle Kunden før slik behandling starter og dokumentere at Databehandleren har inngått databehandleravtale med aktuell underleverandør som oppfyller de krav som stilles for slik overføring/behandling samt at sikkerheten for slik behandling oppfyller kravene i GDPR art. 32.

Oversikt over instruksjer fra Behandlingsansvarlig:

Databehandleren og enhver person som handler for Databehandleren som har tilgang til personopplysninger, skal behandle nevnte opplysninger bare etter dokumentert instruks fra Behandlingsansvarlig.

Databehandleravtalen anses som slike dokumenterte instruksjer. Epost fra Behandlingsansvarlig til Databehandleren om hvordan personopplysninger skal behandles, anses som slike dokumenterte instruksjer.

Databehandleren skal tilføye Behandlingsansvarlig som begunstiget tredjepart i sin avtale med underdatabehandlere [Rams opp eventuelle spesifikke underdatabehandlere denne plikten skal gjelde for hvis det kun er relevant for noen] for det tilfelle at dersom Databehandler går konkurs kan Behandlingsansvarlig tiltre og gjøre gjeldende Databehandlerens rettigheter overfor underdatabehandleren slik at Behandlingsansvarlig kan instruere underdatabehandleren om å slette eller tilbakelevere personopplysningene.

Innebygd personvern (*privacy by design* og *privacy by default*) skal være en grunnleggende del av Databehandlerens behandling av personopplysninger og alle tjenester Databehandler leverer til Behandlingsansvarlig. Databehandler skal sørge for, og kunne dokumentere, at Databehandler med valgte underleverandører så langt det er mulig etterlever grunnleggende prinsipper om innebygd personvern. Det samme gjelder for alle underleverandører Databehandleren har i den grad slike systemer kan behandle personopplysninger som Behandlingsansvarlig er behandlingsansvarlig for.

4. LISTE OVER UNDERLEVERANDØRER LEVERANDØREN HAR TILSVARENDE DATABEHANDLERAVTALE MED

| Under-leverandørens juridiske navn: | Angivelse av land/område: | Angivelse av leverte ytelser og hvilke personopplysninger som behandles: | Nettsted (URL): | Databehandler avtale inngått med slik under-leverandør: |
|-------------------------------------|---------------------------|---|---|---|
| [Sett inn navn] | [Sett inn land/område] | [Sett inn en angivelse av under-leverandørens leverte ytelser og hvilke personopplysninger som behandles] | [Sett inn url – enten til underleverandør eller til underleverandørs nettside som | [Leverandøren må svare Ja, og helst oppgi dato for når slik avtale ble inngått] |

| | | | | |
|--|--|--|--|--|
| | | | beskriver slik underdata-behandlers informasjons-sikkerhet som er relevant for det som skal leveres] | |
| | | | | |
| | | | | |
| | | | | |

Vedlegg 2: Databehandlers generelle informasjonssikkerhet

Databehandleren garanterer at egnede tekniske og organisatoriske sikkerhetstiltak til enhver tid er på plass for å sikre tilfredsstillende informasjonssikkerhet slik at personopplysninger beskyttes mot ulovlig eller ufrivillig destruksjon, tap, skade, endring og uautorisert tilgang. Dette gjelder særlig hvor behandlingen involverer overføring av data over et nettverk og for all annen ulovlige former for overføring av data.

Slike tekniske og organisatoriske sikkerhetstiltak inkluderer, men er ikke begrenset til: Digital adgangskontroll som passordbeskyttelse, tilgangskontroll, overførings-kontroll, begrensnig av tilgjengelighet.

Se også Leverandørens personvernerklæring tilgjengelig på: [Sett inn url].

For mer detaljert informasjon om de nyeste tekniske og organisatoriske sikkerhetstiltak, se [Sett inn url eller henvisning til sikkerhetsdokument eller annen beskrivelse av Leverandørens informasjonssikkerhet relevant for de løsningene hvor Kundens personopplysninger behandles, f.eks. «Leverandørens svar på Kundens krav til informasjonssikkerhet i Hovedavtalen»].