**DATABEHANDLERAVTALE**

# Bakgrunn og formål

## Dette Databehandleravtalen er vedlegg til hovedavtalens navn datert dato ("**Hovedavtalen**") mellom virksomhetens navn (den "**Behandlingsansvarlige**") og virksomhetens navn ("**Databehandleren**").

## Formålet med denne Databehandleravtalen er å fastlegge partenes rettigheter og plikter vedrørende Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige under Hovedavtalen.

## I tilfelle uoverensstemmelse mellom Hovedavtalen og denne Databehandleravtalen om forhold spesifikt knyttet til personvernvern, skal Databehandleravtalen gis forrang.

# Definisjoner

## I denne Databehandleravtalen skal følgende ord og uttrykk ha den betydning som er angitt nedenfor.

## "**Gjeldende personvernregler**": Gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR (fra og med 25. mai 2018).

## "**GDPR**": EUs personvernforordning 2016/679.

## "**Standardklausuler**": Standardklausuler for overføring av personopplysninger til databehandlere etablert i tredjestater, etablert ved EU-kommisjonens vedtak av 5. februar 2010 og/eller som etablert av EU-kommisjonen eller en relevant tilsynsautoritet i henhold til GDPR artikkel 28(7) eller 28(8);

## "**Underdatabehandler**": En annen databehandler engasjert av Databehandleren.

## "**Tredjestat**": Et land utenfor EØS som EU-kommisjonen ikke har fastslått at sikrer et tilstrekkelig beskyttelsesnivå.

## For øvrig skal ord og uttrykk ha samme mening som de er tillagt i GDPR.

# Omfang

## Denne Databehandleravtalen gjelder alle personopplysninger som Databehandleren har mottatt, er gitt tilgang til eller har generert i forbindelse med Hovedavtalen.

## Denne Databehandleren skal så langt det er relevant gjelde tilsvarende for data som ikke er personopplysninger, med unntak for punkt 4 og 5.

## Databehandlingens formål og art, typen personopplysninger som behandles, samt kategorier av registrerte, fremgår av Vedlegg 1. Databehandleren skal behandle personopplysningene utelukkende for det formål og innenfor det omfang som er angitt i Vedlegg 1 og for øvrig i samsvar med den Behandlingsansvarliges dokumenterte instrukser.

# Generelle plikter

## Den Behandlingsansvarlige skal etterleve sine forpliktelser etter gjeldende personvernregler, herunder ved å sørge for behandlingsgrunnlag og at de registrerte har mottatt nødvendig personverninformasjon.

## Databehandleren garanterer å ha gjennomført egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i henhold til gjeldende personvernregler og ivaretar de registrertes rettigheter, og at disse tiltakene vil etterleves i hele avtaleperioden.

## Databehandleren skal omgående underrette den Behandlingsansvarlige skriftlig hvis den har rimelig grunn til å tro at (i) en instruks fra den Behandlingsansvarlige kan medføre at Databehandleren bryter med gjeldende personvernlovgivning, eller (ii) gjeldende rett i EØS-området krever at Databehandleren behandler personopplysninger utover omfanget av den Behandlingsansvarliges dokumenterte instrukser, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater det). I tilfelle av (i) eller (ii) skal partene i god tro diskutere hvordan problemet kan løses uten at det negativt påvirker vernet av de registrertes rettigheter.

## Hvis Databehandleren er underlagt godkjente atferdsnormer i henhold til GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme i henhold til GDPR artikkel 42, garanterer Databehandleren at den vil etterleve slike atferdsnormer eller sertifiseringsmekanismer.

# Bistand til den behandlingsansvarlige

## Databehandleren skal, ved hjelp av egnede tekniske og organisatoriske tiltak, bistå den Behandlingsansvarlige i den grad det er mulig med å oppfylle den Behandlingsansvarliges plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i GDPR kapittel 3, herunder anmodninger om informasjon, innsyn, korrigering, sletting, begrensning av behandlingen, dataportabilitet, innsigelser, og det å ikke være underlagt automatiserte individuelle avgjørelser.

## Databehandleren skal føre en protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av den Behandlingsansvarlige. Protokollen skal gjøres tilgjengelig for den Behandlingsansvarlige på forespørsel.

## Med hensyn til behandlingens art og den informasjon som er tilgjengelig for Databehandleren, skal Databehandleren bistå den Behandlingsansvarlige med forpliktelsene i henhold til GDPR artikkel 32 til 36, herunder forpliktelsene til datasikkerhet (som nærmere beskrevet i punkt 6), melding om brudd på personopplysningssikkerhet (som nærmere beskrevet i punkt 9), vurdering av personvernkonsekvenser, samt forhåndsdrøftinger.

## Databehandleren skal ikke kommunisere direkte med de registrerte eller med tilsynsmyndigheter med mindre dette er forhåndsgodkjent av den Behandlingsansvarlige. Databehandleren skal umiddelbart videresende til den Behandlingsansvarlige forespørsler eller klager som den eventuelt mottar fra de registrerte. Databehandleren skal også umiddelbart videresende eventuelle forespørsler fra en tilsynsmyndighet som gjelder inspeksjoner, undersøkelser, eller tilgang til eller informasjon om personopplysninger, med mindre loven forbyr det (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart loven tillater det).

# Tekniske og organisatoriske sikkerhetstiltak

## Databehandleren skal gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak for å verne personopplysningene mot utilsiktet eller ulovlig tilintetgjøring, tap, endring, ikke-autorisert utlevering eller tilgang. Databehandleren skal som et minimum gjennomføre de tiltakene som er påkrevd i henhold til GDPR artikkel 32, samt de tiltak som er angitt eller referert til i Vedlegg 2.

## Databehandleren skal ikke utlevere eller tilgjengeliggjøre personopplysninger for tredjeparter uten skriftlig forhåndsgodkjennelse fra den Behandlingsansvarlige, med unntak for eventuelt godkjente underdatabehandlere i den utstrekning de har behov for opplysningene for å kunne utføre sine oppgaver.

## Databehandleren skal påse at alle personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av slike personers signerte taushetsavtaler.

# Bruk av underdatabehandlere

## [**Alt. 1**]Databehandleren kan kun engasjere underdatabehandlere etter særlig skriftlig tillatelse fra den Behandlingsansvarlige. Eventuelle godkjente underdatabehandlere er oppført i Vedlegg 3. [**Alt. 2**]Den Behandlingsansvarlige tillater at Databehandleren engasjerer underdatabehandlere. På forespørsel skal den Behandlingsansvarlige motta informasjon om hvem underdatabehandlerne er, samt hvor de behandler personopplysningene. Databehandleren skal underrette den Behandlingsansvarlige om eventuelle planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere og gi den Behandlingsansvarlige rett til å motsette seg slike endringer eller å kreve at denne Databehandleravtalen opphører.

## I henhold til punkt 7.1 skal Databehandleren kun engasjere underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at databehandlingen oppfyller kravene etter gjeldende personvernregler og som sikrer de registrertes personvern. Databehandleren skal gjennomføre egnede kontroller av underdatabehandlerne for å verifisere deres databeskyttelsesnivå. Databehandleren skal fremlegge rapporter fra slike kontroller for den Behandlingsansvarlige.

## Databehandleren skal inngå skriftlig avtale med hver underdatabehandler som pålegger egne forpliktelser med hensyn til vern av personopplysninger. Når underdatabehandleren er engasjert for å utføre spesifikke databehandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal Databehandleren ved skriftlig avtale pålegge underdatabehandleren de samme forpliktelsene med hensyn til vern av personopplysninger som fastsatt i denne Databehandleravtalen. På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av avtaler med underdatabehandlere. Forretningsmessig og annen forretningssensitiv informasjon kan dog sladdes.

## Databehandleren har fullt ansvar for underdatabehandlerens utførelse av sine forpliktelser.

# Internasjonal dataoverføring

## Databehandleren kan kun overføre personopplysninger til tredjestater eller en internasjonal organisasjon dersom slik overføring oppfyller vilkårene i GDPR kapittel 5 og kun etter dokumenterte instrukser fra den Behandlingsansvarlige.

## Databehandleren kan imidlertid overføre personopplysninger uten instruks hvis det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater dette).

## Dersom bruk av en godkjent underdatabehandler krever overføring av personopplysninger til en tredjestat, og slike overføringer er godkjent av den Behandlingsansvarlige, gir den Benhandlingsansvarlige Databehandleren fullmakt til å inngå standardklausuler i uendret form med underdatabehandleren på vegne av den Behandlingsansvarlige dersom dette er nødvendig for å tilfredsstille krav etter gjeldende personvernregler. Så snart en slik avtale er inngått skal underdatabehandleren fremlegge en kopi av denne for den Behandlingsansvarlige. Alle slike standardklausuler skal automatisk opphøre ved opphøret av denne Databehandleravtalen.

# Brudd på personopplysningssikkerheten

## Databehandleren skal gi skriftlig melding til den Behandlingsansvarlige om eventuelle brudd på denne Databehandleravtalen eller personopplysningssikkerheten. Meldingen skal gis senest 36 timer etter at Databehandleren ble oppmerksom på bruddet.

## Melding om brudd på personopplysningssikkerheten må minst, i den grad det er relevant:

### beskrive arten av bruddet, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt;

### inneholde, når det er mulig, de berørte registrertes identitet;

### formidle navn og kontaktinformasjon til personvernrådgiveren eller et annet kontaktpunkt hos Databehandleren for ytterligere innhenting av informasjon;

### beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;

### beskrive de tiltak som er truffet eller foreslått for å håndtere bruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger;

### inkludere annen informasjon som kreves for at den Behandlingsansvarlige kan overholde gjeldende personvernregler.

## Databehandleren skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e. ovenfor, samt gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende brudd på personopplysningssikkerheten. Databehandleren skal tillate den Behandlingsansvarlige å undersøke, fastlegge årsaken til og å verifisere de tiltak som er gjennomført eller foreslått av den Behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten. Databehandleren skal, så langt det er mulig, rådføre seg med den Behandlingsansvarlige med hensyn til de tiltak som skal gjennomføres samt overveie innspill fra den Behandlingsansvarlige i den forbindelse.

## Kun den Behandlingsansvarlige har rett til å informere den relevante tilsynsmuligheten og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandleren skal avstå fra å informere allmennheten eller tredjepart om brudd på personopplysningssikkerheten.

# Revisjon

## Databehandleren skal dokumentere, samt gjøre tilgjengelig for den Behandlingsansvarlige, informasjon som er nødvendig for å påvise etterlevelse av denne Databehandleravtalen og gjeldende personvernregler.

## Databehandleren skal muliggjøre og bidra ved revisjoner av Databehandlerens behandlingsaktiviteter som utføres av den Behandlingsansvarlige eller av annen revisor på fullmakt fra den Behandlingsansvarlige. Databehandleren skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

## Databehandleren skal, på egen hånd eller via annen revisor på fullmakt fra Databehandleren, foreta jevnlige revisjoner av sine behandlingsaktiviteter. Databehandleren skal oversende kopi av revisjonsrapporter fra slike revisjoner til den Behandlingsansvarlige. Den Behandlingsansvarlige skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.

## Databehandleren skal umiddelbart varsle den Behandlingsansvarlige hvis den mottar forespørsel fra en myndighet om å utlevere personopplysninger som er behandlet under denne Databehandleravtalen. Med mindre loven krever det, skal Databehandleren ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra den Behandlingsansvarlige.

## Dersom en revisjon avdekker avvik fra forpliktelsene i denne Databehandleravtalen, skal Databehandleren så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandleren gjør det samme). Den Behandlingsansvarlige kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet.

## Hver av partene dekker sine egne kostnader forbundet med en revisjon. Hvis en revisjon avdekker ikke-uvesentlige avvik fra forpliktelsene i denne Databehandleravtalen, skal alle kostnader forbundet med revisjonen dekkes av Databehandleren, herunder den Behandlingsansvarliges og eksterne revisorers rimelige kostnader.

# [alt.]Skadesløsholdelse

## Databehandleren skal holde den Behandlingsansvarlige skadesløs fra eventuelle kostnader (herunder rimelige saksomkostninger) og tap som følge av et krav fra en tredjepart (inkludert tilsynsmyndigheter og registrerte) om at behandlingen av personopplysningene innebærer brudd på gjeldende personvernregler, og kravet skyldes Databehandlerens mislighold av sine forpliktelser i denne Databehandleravtalen, herunder behandling av personopplysninger utover den Behandlingsansvarliges skriftlige instrukser.

## Skadesløsholdelsen er betinget av (i) at den Behandlingsansvarlige umiddelbart varsler Databehandleren om kravet, og (ii) at Databehandleren får mulighet til å samarbeide med den Behandlingsansvarlige i forsvaret mot og oppgjøret av kravet.

# [alt.]andre behandlingsansvarlige

## Databehandleren anerkjenner at personopplysningene også behandles på vegne av den Behandlingsansvarliges konsernselskaper/kunder/klienter. Slike andre behandlingsansvarlige har samme rettigheter som den Behandlingsansvarlige som er avtalepart, og de kan håndheve denne Databehandleravtalen som om de var avtaleparter. Slik håndheving skal imidlertid skje gjennom den Behandlingsansvarlige som er avtalepart.

## Den Behandlingsansvarlige kan videresende enhver instruks fra slike andre behandlingsansvarlige, og Databehandleren skal handle i samsvar med slike instrukser som om de var den Behandlingsansvarliges egne.

## Den Behandlingsansvarlige kan videresende enhver dokumentasjon og informasjon mottatt av Databehandleren til slike andre behandlingsansvarlige.

# Varighet og oppsigelse

## Denne Databehandleravtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige i forbindelse med Hovedavtalen.

## Ved opphør eller oppsigelse av Databehandleravtalen skal Databehandleren, dersom den Behandlingsansvarlige ønsker det, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige og slette eksisterende kopier, og bekrefte overfor den Behandlingsansvarlige at dette er gjort, med mindre gjeldende rett i EØS-området krever at Databehandleren lagrer personopplysningene (i så fall skal Databehandleren besørge sikker lagring, men ikke aktivt behandle, personopplysningene, og skal slette personopplysningene så snart loven tillater dette).

[signaturfelt på neste side]

|  |  |
| --- | --- |
| For den Behandlingsansvarlige:Signatur: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Navn:Dato: | For Databehandleren:Signatur: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Navn:Dato: |

**VEDLEGG 1: DATABEHANDLINGENS OMFANG**

**Behandlingens formål**

Formålet med databehandlingen er at Databehandleren skal kunne utføre sine forpliktelser i henhold til Hovedavtalen.

**Behandlingens art og hensikt**

Sett inn beskrivelse av hvordan personopplysninger vil behandles (f.eks. innsamling, lagring osv.) eller sett inn referanse til relevante deler av Hovedavtalen eller vedlegg til Hovedavtalen. Eksempel kan være *lagring av data på en skybasert plattform.*

**Varighet**

Sett inn informasjon dersom noen av behandlingsaktivitetene vil opphøre før utløpet av Databehandleravtalen.

**Kategorier av registrerte**

Sett inn.

*Eksempler: Den Behandlingsansvarliges nåværende, tidligere og potensielle ansatte; nåværende, tidligere og potensielle ansatte hos den Behandlingsansvarliges kunder.*

**Typen personopplysninger**

Sett inn.

*Eksempler: Navn, kjønn, fødselsdato, telefonnummer, adresse, epostadresse, funksjoner/stilling, ansatt-ID, , tjenestetid, lønn, utdannelse og andre yrkesmessige kvalifikasjoner, opplysninger vedrørende nåværende og tidligere pensjonsordninger og pensjonsbeløp, pensjonsinnskudd, ytelser til ansatte, sivilstand, stønader, bankopplysninger, personnummer og/eller helsetilstand, lønn; kredittopplysninger, forhold til myndigheter og myndighetspersoner, informasjon mottatt gjennom søk i offentlige kilder og samtaler/intervjuer; transaksjoner, atferdsopplysninger (f.eks. besøkte nettsteder, aktiviteter utløst ved definerte handlinger slik som sideinnlastinger, klikk, innlogginger og kjøp); geolokaliseringsdata.*

**Særlige kategorier av personopplysninger (hvis relevant)**

Sett inn.

**VEDLEGG 2: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK**

Databehandleren skal som et minimum gjennomføre alle de tiltak som er angitt eller henvist til nedenfor. Databehandleren kan ikke uten skriftlig samtykke fra den Behandlingsansvarlige gjøre endringer i disse tiltakene som reduserer graden av datasikkerhet. Databehandleren skal kontinuerlig arbeide for å forbedre sikkerhetstiltakene og sørge for at de oppdateres i takt med den teknologiske utviklingen.

**Alt 1**: [Sett inn referanse til Retningslinjene for datasikkerhet]

**Alt 2**:

**Pseudonymiseringstiltak**

*Pseudonymisering vil si behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsinformasjon, forutsatt at slik tilleggsinformasjon oppbevares separat og er gjenstand for tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar person*.

Sett inn beskrivelse av eventuelle pseudonymiseringstiltak.

**Krypteringstiltak**

*Kryptering er prosessen med koding av data på en slik måte at bare autoriserte personer har tilgang til opplysningene*.

Sett inn beskrivelse av eventuelle krypteringstiltak.

**Tiltak for å sikre personopplysningenes fortrolighet**

Sett inn beskrivelse. Eksempler kan være tiltak for å kontrollere tilgang, og for å skille opplysningene fra opplysninger som Databehandleren behandler på vegne av andre behandlingsansvarlige.

**Tiltak for å sikre personopplysningenes integritet**

Sett inn beskrivelse. Et eksempel kan være tiltak for å overvåke endringer i opplysningene.

**Tiltak for å sikre tilgjengeligheten til personopplysningene**

Sett inn beskrivelse. Et eksempel kan være backup-tiltak.

**Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene**

Sett inn beskrivelse. Eksempler kan være tiltak for katastrofegjenoppretting og redundans.

**Andre datasikkerhetstiltak**:

Sett inn beskrivelse, eller "ikke relevant".

**VEDLEGG 3: GODKJENTE UNDERDATABEHANDLERE**

|  |  |  |
| --- | --- | --- |
| Selskapets navn | Selskapets adresse | Behandlingssted |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |