# DATABEHANDLERAVTALE

# Innholdsfortegnelse

# 1. Avtalens formål

Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig på bakgrunn av avtale mellom partene. Databehandleravtalens formål er å regulere den behandlingen av personopplysninger som Databehandler skal utføre på vegne av Behandlingsansvarlig. Databehandleravtalen skal sikre at behandlingen av personopplysninger skjer i samsvar med gjeldende regelverk for behandling av personopplysninger.

Formålet med behandlingen, behandlingens art, de typer personopplysninger som skal behandles og kategorier av registrerte følger av vedlegg 1 til Avtalen.

Avtalen skal sikre at personopplysninger behandles i samsvar med de til enhver tid gjeldende krav til behandling av personopplysninger, herunder 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 personopplysningsloven

Databehandler skal behandle personopplysningene på den måte som er beskrevet i Avtalen, samt på annen måte dersom dette er skriftlig avtalt mellom Databehandleren og Behandlingsansvarlig.

# 2. Definisjoner

Behandling av personopplysninger er underlagt krav og forpliktelser med hjemmel i lov. Databehandleravtalens begrepsbruk skal forstås i samsvar med EU-forordning 2016/679 artikkel 4. Følgende definisjoner hitsettes:

- «Personopplysning» skal bety enhver opplysning om en identifisert eller identifiserbar fysisk person, som definert i til enhver tid gjeldende regelverk for behandling av personopplysninger.
- «Behandling» av personopplysninger, skal bety enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring, som definert i til enhver tid gjeldende regelverk for behandling av personopplysninger.

## 3. Databehandlers plikter

Så lenge avtalen gjelder skal Databehandler:

i. sikre at Databehandlers behandling av personopplysninger er i overensstemmelse med all relevant lovgivning om personopplysninger og eventuelle gjeldende bransjenormer;
ii. bare behandle personopplysninger etter dokumenterte instrukser som den Behandlingsansvarlig til enhver tid har bestemt skal gjelde, og ikke behandle personopplysninger utover hva som er nødvendig for å oppfylle Databehandlers forpliktelser i sammenheng med avtalen;
iii. ikke utlevere eller overlate personopplysninger til andre, herunder til stater utenfor EØS, med mindre Behandlingsansvarlig har godkjent dette skriftlig;
iv. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovens bestemmelser, herunder kravene etter personvernforordningen artikkel 32. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av personopplysninger som ikke er i overensstemmelse med denne avtalen og tiltak for å gjenopprette tilgjengelighet og tilgang til personopplysninger ved hendelser;
v. ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for drift av tjenestene. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre driften, og tilgangen skal være basert på individuelle brukernavn og passord;
vi. i henhold til Databehandlers rutiner avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på sikkerheten i datasystemet. Slik dokumentasjon skal oppbevares hos Databehandler;
vii. varsle Datatilsynet ved uautorisert utlevering av personopplysninger;
viii. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Behandlingsansvarlig. Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det driftsavtalen spesifiserer;

ix. bistå Behandlingsansvarlig, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for Databehandleren, med å sikre overholdelse av forpliktelsene knyttet til personvernforordningen artiklene 32–36, dvs;
    a. sikkerhet ved behandlingen;
    b. melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten
    c. underretning av den registrerte om brudd på personopplysningssikkerheten
    d. vurdering av personvernkonsekvenser og forhåndsdrøftinger
x. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen;
xi. idet det tas hensyn til behandlingens art og i den grad det er mulig, samarbeide med og assistere Behandlingsansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.;
xii. omgående underrette den Behandlingsansvarlige dersom vedkommende mener at en instruks er i strid med personopplysningslovgivningen, eller om Databehandler ikke er i stand til å overholde sine plikter overfor Behandlingsansvarlige;
xiii. holde Behandlingsansvarlig skadesløs for eventuelle utgifter relatert til erstatningskrav eller overtredelsesgebyrer som kan henføres til forhold hos Databehandler.

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

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for den behandlingsansvarlige.

Databehandler plikter å påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig, er kjent med denne avtalen og underlagt avtalens bestemmelser.

Meddelelser, underretting, varsel eller annen kommunikasjon mellom behandlingsansvarlig og databehandler, skal sendes elektronisk til på epost mellom selskapene.

## 4. Den behandlingsansvarliges plikter

Behandlingsansvarlig skal etterleve de forpliktelser som følger av personopplysningsloven, forordningen og annen lovgivning samt denne avtalen, herunder å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med det foran nevnte.

## 5. Taushetsplikt

Databehandler behandler en rekke typer informasjon som må behandles konfidensielt.

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne avtalen (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), er underlagt taushetsplikt. Personer som er autorisert til å behandle personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører. Databehandler skal påse at alle som behandler personopplysninger under avtalen er kjent med taushetsplikten.

Ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Taushetsplikten gjelder også etter avtalens opphør.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

## 6. Innsyn og revisjon mv.

Behandlingsansvarlig kan til enhver tid kreve innsyn i Databehandlers behandling av personopplysninger tilhørende Behandlingsansvarlig, herunder i dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen av opplysningene som utføres av Databehandler på vegne av Behandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov. En Behandlingsansvarlig som ber om innsyn skal gjøre generell informasjon fra revisjonen tilgjengelig for andre Behandlingsansvarlige som benytter samme tjeneste.

Behandlingsansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid før krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Behandlingsansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere behandlingsansvarlige som får levert tjenester fra databehandler. Innsyn og kontroll kan gjennomføres av Behandlingsansvarlig eller den tredjepart behandlingsansvarlige måtte velge til gjennomføring. Databehandler kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet slik tilgang og innsyn i behandlingen av personopplysninger som følger av personopplysningsloven.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Behandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

## 7. Bruk av underleverandør

Behandlingsansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under avtalen.

Databehandler skal sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under denne avtalen. Databehandler er fullt ut ansvarlig overfor Behandlingsansvarlig for alt arbeid som utføres av egne underleverandører.

Databehandleren skal underrette den Behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere. Endringer i bruk av underleverandører må kommuniseres tydelig i skriftlig, samme sted, slik at Behandlingsansvarlige gis mulighet til å motsette seg endringen.

Tilgang til personopplysninger for eksterne tredjeparter krever konkret avtale mellom partene utover denne avtalen for alle andre enn Databehandlers underleverandører.

## 8. Avtaleperiode

Avtalen gjelder fra den er signert av partene og til det tidspunkt tjenesten er utført.

Avtalen skal revideres ved endringer som går utover avtalt formål og omfang etter denne avtalen. Databehandler vil ta initiativ til slik revisjon og foreslå nødvendige endringer. Avtalen skal også revideres hvis sikkerhetsrevisjoner eller nye krav gjennom lovgivning viser at dette er nødvendig.

## 9. Opphør av avtalen

En avtalepart kan heve Databehandleravtalen dersom den andre avtaleparten i vesentlig grad misligholder sine forpliktelser etter denne Databehandleravtale.

Ved opphør av avtalen, uansett årsak, skal Databehandler stanse all behandling av personopplysninger fra dato bestemt av den Behandlingsansvarlige. Databehandler skal videre tilrettelegge for og medvirke til tilbakeføring av alle opplysninger som Databehandler har behandlet på vegne av Behandlingsansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til Behandlingsansvarlig og bekreftet mottatt av denne, skal Databehandler slette opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre ufravikelige rettsregler krever at personopplysningene fortsatt lagres.

Databehandler skal gi Behandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

## 10. Tolkning, Revisjon og Verneting

Øvrige plikter og rettigheter følger av Hovedavtalen som gjelder mellom Databehandleren og Behandlingsansvarlige om tjenestene som nødvendiggjør behandling av personopplysninger og denne Avtale. De samme kontaktpersoner gjelder for Avtalen som etter Hovedavtalen.

Databehandleravtalen er underlagt norsk rett, og skal tolkes og anvendes deretter. Ingenting i Databehandleravtalen skal forstås som en innskrenkning av de plikter som avtalepartene er underlagt etter gjeldende rett for behandling av personopplysninger.

Avtalepartene er enige om å revidere denne Databehandleravtale i den grad det er nødvendig for å oppfylle nye krav som måtte følge av: EU-forordning 2016/679, rettspraksis, eller lovgivning for øvrig.

Verneting er den Behandlingsansvarliges alminnelige verneting.

***

# 11. Vedlegg 1

### Formålet med behandlingen

Kunde har valgt Cipher Bergen AS som IT driftsleverandør, i tillegg vil det kunne komme avrop på andre oppdrag / tjenester / rådgivning fra Kunde til Cipher Bergen. I forbindelse med dette oppdraget, kan Cipher Bergen AS komme i kontakt med personopplysninger.

### Varigheten av behandlingen

Behandlingen skal vare så lenge Databehandleren yter tjenestene etter Driftsavtalen til Behandlingsansvarlig.

### Behandlingens art

Cipher Bergen AS kan komme i kontakt med personopplysninger i forbindelse med avtalen og oppdrag som nevnt over. Denne behandlingen er nødvendig for Cipher Bergen AS for å kunne gjennomføre tjenestene etter avtalen.

### Typer personopplysninger som skal behandles

Følgende personopplysninger skal behandles under Avtalen / kan komme til å behandles under Avtalen:

- Personopplysninger om ansatte i Kunde.
- Dette gjelder i hovedsak navn, fødselsnummer, adresse og telefonnummer for de ansatte.
- Personopplysninger om ansatte hos Kunde sine leverandører
- Personopplysninger om andre enn de nevnte

### Kategorier av registrerte

Ansatte, Leverandører, andre

### Underdatabehandlere ved inngåelse av Avtalen

Ingen underleverandører på avtale

# 12. Vedlegg 2

## 12.1. Varsling til Datatilsynet

Alle avvik som skyldes brudd på datasikkerheten, skal meldes til Datatilsynet av Kunde. Unntak fra varslingsplikten gjelder der det er usannsynlig at avviket har medført en risiko for enkeltpersoners rettigheter eller personvern.

Kunde skal varsle Datatilsynet innen 72 timer fra avvik oppdages. Partene må ha en intern beredskap slik at de kan prioritere arbeid med avvik som mistenkes eller oppdages slik at fristen kan overholdes.

## 12.2. Varsling til berørte (de registrerte)

Partene skal gi varsel til de registrerte når det er sannsynlig at avviket vil medføre en høy risiko for personvernet til de som er berørt. Partene kan imidlertid la være å varsle de berørte på visse vilkår:

Dersom det er iverksatt beskyttelsestiltak for personopplysningene som er omfattet av sikkerhetsbruddet, særlig dersom tiltakene gjør opplysningene uleselige for uvedkommende, for eksempel ved kryptering.

Dersom det er iverksatt etterfølgende tiltak som gjør at risikoen sannsynligvis ikke lenger er reell.

Hvis et er uforholdsmessig vanskelig å varsle hver enkelt av de berørte. I slike tilfeller skal informasjonen isteden offentliggjøres eller deles på annen måte, slik at de berørte likevel underrettes på en effektiv måte.

Partene skal i løpet av 72 timer beslutte hvorvidt avviket skal medføre varsling til de registrerte og hvilken part som i det enkelte tilfelle gjør dette.

## 12.3. Varsel mellom partene

Dersom en av partene oppdager eller mistenker uautorisert utveksling av opplysninger, uautorisert tilgang, eller misbruk av opplysninger, skal den annen part varsles om dette og det skal iverksettes nødvendige tiltak.

Når avvik mistenkes eller oppdages skal den annen part varsles i rekkefølgen de er listet i bilag nr. 3 Kontaktpersoner (pkt 2) inntil det oppnås kontakt. Hver av partene skal ha interne rutiner for at den som mottar varsel kan involvere de rette personene i egen organisasjon.

Partene skal i fellesskap søke å håndtere situasjonen for å hindre ytterligere brudd og å begrense konsekvensene av avviket.

Avvik skal rapporteres skriftlig og inneholde informasjon om hva som har inntruffet, hvor og når hendelsen inntraff, strakstiltak som ble iverksatt, hvilke konsekvenser hendelsen har og hvem som er ansvarlig for videre oppfølging.

Varsling av avtalebrudd eller sikkerhetsbrudd skal loggføres hos hver av partene. Varslingen skal skje via oppnevnte kontaktpersoner, jf. bilag nr. 3 Kontaktpersoner (punkt 1).