

DATABASEHANDLERAVTALE

Denne databehandleravtalen («Databehandleravtalen») består av to likeverdige og nødvendige deler. Databehandleravtalen består av to deler. Del I angir standardbestemmelser for behandlingen av personopplysninger og del II angir instruks for, og utfyllende beskrivelse av behandlingen av personopplysninger under Databehandleravtalen.

DEL I

Databehandleravtalen regulerer behandling av personopplysninger tilknyttet [hovedavtalens navn] ("Hovedavtalen"), datert [dato], og er inngått mellom:

- (1) [Leverandør, adresse og organisasjonsnummer] ("Databehandler"); og
- (2) [Oppdragsgiver] ("Behandlingsansvarlig").

1. BAKGRUNN OG FORMÅL

- (A) Databehandleravtalen er inngått som følge av at Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig for å oppfylle Hovedavtalen.
- (B) Databehandler skal behandle Personopplysninger kun i henhold til de angitte og avtalte spesifiserte formål og dokumenterte instruks angitt i Databehandleravtalen.
- (C) Databehandleravtalen er inngått og utformet for å sikre etterlevelse av lov om behandling av personopplysninger (personopplysningsloven), og EU-forordning 2016/679, med tilhørende krav til reguleringen av forholdet mellom Databehandler og Behandlingsansvarlig, og til de sikkerhetsmessige og organisatoriske tiltakene som må implementeres for å sørge for lovlig og sikker Behandling av Personopplysninger. Databehandleravtalen er derfor inngått for å sikre at Personopplysninger kun behandles i henhold til enhver tid gjeldende lover og regler, og kun etter instruks fra Behandlingsansvarlig.
- (D) Databehandleravtalen er å anse som gyldig når den er signert av begge Parter og både Del I og Del II er utfylt med påkrevet informasjon i henhold til GDPR art. 28, herunder utfyllende beskrivelse av behandlingens art, formål, omfang, de registrerte det behandles personopplysninger om, Underdatabehandlere og eventuell annen tilleggsinformasjon.
- (E) Databehandleravtalen fritar ikke Databehandler fra plikter som Databehandler er pålagt etter personvernforordningen eller annen lovgivning.

2. DEFINISJONER

Databehandleravtalen bruker flere gjentakende begreper, og i alle sammenhenger skal begrepene ha den betydning som angitt nedenfor:

Gjeldende personvernlovgivning: Personopplysningsloven (LOV-2018-06-15-38) med forskrift, som gjennomfører personvernforordningen, EUs personvernforordning 2016/679 (GDPR) samt andre norske lover innenfor virkeområdet.

GDPR: EUs personvernforordning 2016/679.

Personopplysning betyr enhver opplysning som direkte eller indirekte kan identifisere en levende fysisk person, jfr. GDPR artikkel 4 (1). Merk at dette kan omfatte visse typer metadata og logger.

Registrert betyr en levende fysisk person som direkte eller indirekte kan identifiseres gjennom opplysninger som Behandlingsansvarlig for sitt formål har samlet inn og behandler, og dermed har ansvar for, jfr. GDPR artikkel 4 (1). I flertall omtalt som **Registrerte**.

Behandling av Personopplysninger betyr enhver operasjon eller rekke av operasjoner som gjøres med Personopplysninger, jfr. GDPR artikkel 4 (2).

Behandlingsansvarlig betyr den som alene eller sammen med andre bestemmer formålet med Behandlingen av Personopplysninger og hvilke midler som skal benyttes, jfr. GDPR artikkel 4 (7).

Databehandler betyr den juridiske enheten som Behandler Personopplysninger på vegne av den Behandlingsansvarlige, jfr. GDPR 4 (8).

Partene, brukes for å omtale Behandlingsansvarlig og Databehandler samlet. I entall omtalt som **Part**.

Underdatabehandler: En annen databehandler engasjert av Databehandleren.

Brudd på personopplysningssikkerheten: ethvert brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til Personopplysninger som er overført, lagret eller på annen måte behandlet.

Tredjeland betyr land utenfor EU/EØS som EU-kommisjonen ikke har fastslått at sikrer et tilstrekkelig beskyttelsesnivå for Behandling av Personopplysninger.

For øvrig skal ord og uttrykk ha samme mening som definert i GDPR artikkel 4.

3. BESKRIVELSE AV BEHANDLINGEN

Databehandler leverer [løsning for budsjett, prognose, rapportering og mål- og resultatstyring - sett inn/beskriv hva som er leveranser etter Hovedavtalen], og vil behandle Personopplysninger på vegne av Behandlingsansvarlige i den forbindelse. Databehandleravtalen gjelder alle Personopplysninger som Databehandleren har mottatt, er gitt tilgang til eller har generert på vegne av Behandlingsansvarlig i forbindelse med Hovedavtalen.

Nærmere beskrivelse av Behandlingen følger av Del II. Databehandleren skal behandle Personopplysningene utelukkende for de formål og innenfor det omfang som er angitt i Del II og for øvrig i samsvar med den Behandlingsansvarliges dokumenterte instruks.

4. BEHANDLINGSANSVARLIGES FORPLIKTELSE

Behandlingsansvarlig er ansvarlig for å sikre at Behandlingen av Personopplysninger ikke går utover de konkrete formål for Behandlingen, og er i tråd med Gjeldende personvernlovgivning. Behandlingsansvarlig er ansvarlig for å etterleve de plikter som gjelder for Behandlingsansvarlig under Gjeldende personvernlovgivning, herunder spesielt Behandlingsansvarlig sine konkrete plikter

angitt i GDPR. Behandlingsansvarlig skal også sørge for at det foreligger et gyldig behandlingsgrunnlag for Behandlingen av Personopplysningene under Databehandleravtalen.

Den Behandlingsansvarliges instruks til Databehandler fremgår av Databehandleravtalen Del II og Hovedavtalen.

5. DATABEHANDLERS FORPLIKTELSER

5.1 Grunnleggende forpliktelser

Databehandler skal etterleve de plikter som gjelder for Databehandler under Gjeldende personvernlovgivning. Databehandler skal kun behandle Personopplysninger på, og i samsvar med, skriftlige instruks fra Behandlingsansvarlig.

Databehandler skal ikke uten forutgående skriftlig avtale eller skriftlig instruks fra Behandlingsansvarlig behandle Personopplysninger på vegne av Behandlingsansvarlig, utover det som er nødvendig for de formålene som er spesifisert i Databehandleravtalen.

Databehandler skal ikke behandle Personopplysninger fra Behandlingsansvarlig til egne formål. Dersom Databehandler ønsker å behandle Personopplysninger om Registrerte til egne formål må dette reguleres i et eget avtaleforhold mellom den Registrerte og Databehandler, der Databehandler vil være å anse som behandlingsansvarlig og er ansvarlig for medfølgende plikter etter GDPR.

Databehandler skal omgående underrette Behandlingsansvarlig skriftlig dersom;

- (i) tvingende lovgivning krever at Databehandleren behandler Personopplysninger utover omfanget av den Behandlingsansvarliges dokumenterte instruks. Dersom lovgivning i EU/EØS av hensyn til viktige samfunnsinteresser forbyr slik underretning, skal Databehandleren underrette den Behandlingsansvarlige så snart dette er tillat, eller
- (ii) Databehandler mottar instruks fra Behandlingsansvarlig som er i strid med Gjeldende personvernlovgivning.

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.

Dersom Databehandler er underlagt godkjente atferdsnormer i henhold til GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme i henhold til GDPR artikkel 42, skal disse følges så lenge Databehandleravtalen gjelder.

Databehandleren skal ikke utlevere eller tilgjengeliggjøre Personopplysninger for tredjeparter uten skriftlig forhåndsgodkjennelse fra den Behandlingsansvarlige, med unntak for godkjente Underdatabehandlere som angitt i Del II, i den utstrekning de har behov for opplysningene for å kunne utføre sine oppgaver.

5.2 Informasjonssikkerhet

Databehandler skal ved planlagte, systematiske og egnede organisatoriske og tekniske tiltak sikretilstrekkelig informasjonssikkerhet med hensyn til konfidensialitet, integritet, tilgjengelighet og robusthet i forbindelse med Behandling av Personopplysninger. Databehandler skal treffe alle tiltak som er nødvendig i henhold til Gjeldende personvernlovgivning, herunder GDPR artikkel 32.

Del II bokstav f) beskriver eksempler på krav til Databehandlers tekniske og organisatoriske tiltak. Hvilke tiltak som er påkrevet vurderes konkret etter risikoen for hvert tilfelle. Sikkerhetstiltak utover de Databehandler leverer som en del av sin standard tjeneste skal vurderes og avtales nærmere i Del II mellom Behandlingsansvarlig og Databehandler. Databehandler har like fullt et selvstendig ansvar for å ivareta sikkerheten og vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen i Databehandlers system utgjør. Databehandler skal vederlagsfritt dokumentere sikkerhetstiltakene og informasjonssystemene som benyttes for Behandling av Personopplysninger på vegne av Behandlingsansvarlig under Databehandleravtalen.

5.3 Henveldeiser fra de Registrerte

Databehandler skal, med hensyn til behandlingens art og i den grad det er mulig, implementere tekniske og organisatoriske tiltak for å bistå Behandlingsansvarlig med å svare på henvendelser angående utøvelse av de Registrertes rettigheter fastsatt i GDPR kapittel III, ved anmodninger om informasjon, innsyn, korrigering, sletting, begrensning av Behandlingen, dataportabilitet, innsigelse, og retten til å ikke være underlagt automatiserte individuelle avgjørelser.

Ved innsynskrav skal Databehandler bistå ved å samle Personopplysninger som er lagret om den Registrerte, og gjøre opplysningene tilgjengelig for Behandlingsansvarlig for at den Behandlingsansvarlig kan vurdere innsynskravet.

Bistand som beskrevet her kompenseres etter Databehandleravtalen punkt 5.4

5.4 Bistand til Behandlingsansvarlig

«Bistand» som omtalt i dette punktet skal forstås som de tjenester og ytelser Databehandler utfører utover det som inngår i tjenesten som beskrevet i Hovedavtalen og utover de tiltak Databehandler selv plikter å gjennomføre for å påse egen etterlevelse av Gjeldende personvernlovgivning.

Databehandleren skal på forespørsel yte Bistand til Behandlingsansvarlig med å sikre etterlevelse av forpliktelser etter GDPR artikkel 32-36, i det det tas hensyn til Behandlingens art og den informasjon som er tilgjengelig for Databehandleren.

Databehandleren skal ikke kommunisere direkte med de Registrerte, og skal henvende Registrerte til Behandlingsansvarlig. Anmodninger fra Registrerte skal umiddelbart videresendes til Behandlingsansvarlig. Databehandler skal ikke kommunisere direkte med tilsynsmyndigheter om saker relatert til behandling av personopplysninger på vegne av Behandlingsansvarlig, med mindre dette er skriftlig avtalt med den Behandlingsansvarlige.

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).

Dersom Databehandler yter Bistand som faller inn under Databehandleravtalen punkt 5.4 første avsnitt, kan Databehandler kreve dekket sine dokumenterte kostnader knyttet til Bistanden. Arbeidet dekkes i henhold til prisbestemmelsene i Hovedavtalen.

5.5 Håndtering av avvik og varsling ved sikkerhetsbrudd

Enhver bruk av informasjonssystemene og Personopplysninger i strid med Databehandleravtalen, etablerte rutiner, instruksjoner fra Behandlingsansvarlig eller Gjeldende personvernlovgivning, så vel som brudd på personopplysningsikkerheten, skal Databehandler håndtere 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 gjentakelse.

Databehandler skal gi Behandlingsansvarlig all nødvendig informasjon for å sette Behandlingsansvarlig i stand til å overholde Gjeldende personvernlovgivning og besvare henvendelser fra tilsynsmyndigheter.

Databehandler skal skriftlig varsle Behandlingsansvarlig om ethvert avvik som ikke er brudd på personopplysningsikkerheten. Nærmere om hvordan Databehandler skal varsle Behandlingsansvarlig om avvik som ikke er brudd på personopplysningsikkerheten skal reguleres i Del II bokstav h).

5.5.1 Særlig om å varsle brudd på personopplysningsikkerheten

Databehandler skal alltid skriftlig varsle Behandlingsansvarlig om brudd på personopplysningsikkerheten, uten ugrunnet opphold og senest 72 timer etter bruddet er oppdaget.

Varsel om brudd på personopplysningsikkerheten skal sendes til vaktentralen@dss.dep.no, med kopi til postmottak@dss.dep.no.

I overensstemmelse med vilkår 5.4 (2) skal Databehandler bistå Behandlingsansvarlig med å melde bruddet til den kompetente tilsynsmyndigheten. Dette innebærer at Databehandleren skal bistå med å fremskaffe informasjon som listet opp nedenfor i bokstav a-f.

Melding om Brudd på personopplysningsikkerheten 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 personopplysningsikkerheten;
- 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 personvernlovgivning.

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 personopplysningsikkerheten. 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 personopplysningsikkerheten. 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 personopplysningsikkerheten. Databehandleren skal avstå fra å informere allmennheten eller tredjepart om Brudd på personopplysningsikkerheten.

5.6 Sletterutiner

Databehandler skal etter Behandlingsansvarliges instruksjoner tilbakelevere og/eller slette Personopplysninger, og skal på forespørsel fra Behandlingsansvarlig fremlegge dokumentasjon på sletterutiner og gjennomført sletting.

5.7 Taushetsplikt

Databehandler har taushetsplikt om Personopplysninger og skal sikre at alle som utfører arbeid for Databehandler, enten ansatte eller innleide, og som har nødvendig tilgang til eller er involvert i Behandling av Personopplysninger etter Databehandleravtalen;

- (i) er autorisert til å behandle personopplysninger for Databehandler, der dette er påkrevet,
- (ii) er underlagt taushetsplikt etter en signert taushetsavtale, og
- (iii) er informert om og overholder forpliktelsene etter Databehandleravtalen

Taushetsplikten som stadfestet i taushetsavtalen, gjelder også etter opphør av Databehandleravtalen.

På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av slike personers autorisasjon og signerte taushetsavtaler.

Databehandler skal sikre at autoriserte personer blir fratatt sin tilgang dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder personen. Det samme gjelder hvis behovet for å ha tilgang til Personopplysninger eller være involvert ikke lenger er til stede.

5.8 Revisjon

Databehandleren skal regelmessig dokumentere, samt gjøre tilgjengelig for den Behandlingsansvarlige, informasjon som er nødvendig for å påvise Databehandlers etterlevelse av Databehandleravtalen og Gjeldende personvernlovgivning. Slik dokumentasjon skal i tillegg til Databehandlers revisjonsrapporter, inneholde Databehandlers interne risikovurderinger, og dette skal oppgis vederlagsfritt.

Behandlingsansvarlig har rett til, selv eller ved hjelp av utpekt revisor, å gjennomføre revisjon av Databehandlerens etterlevelse av Databehandleravtalen og Gjeldende personvernlovgivning, med mindre Databehandleren velger å benytte ekstern revisor til å attestere at sikkerhetstiltak er etablert og virker etter hensikten. Slik revisjon skal gjennomføres én gang årlig i henhold til anerkjente attestasjonsstandarter, herunder, men ikke begrenset til ISAE3402, og utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring. Rapportene skal fremlegges for Behandlingsansvarlig på forespørsel.

Databehandleren skal bistå ved å muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

Hver av Partene dekker sine egne kostnader forbundet med ekstra revisjoner utover den regelmessige revisjonsrapporten som Databehandler plikter å fremlegge. Dersom en revisjon avdekker ikke-uvesentlige avvik fra Databehandlers forpliktelser etter Databehandleravtalen, skal Behandlingsansvarliges rimelige kostnader knyttet til revisjonen, inkludert bruk av revisor, dekkes av Databehandleren.

Dersom en revisjon avdekker avvik fra forpliktelsene i 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.

6. BRUK AV UNDERDATABEHANDLER

6.1 Bruk av Underdatabehandler

Enhver Underdatabehandler skal godkjennes skriftlig av Behandlingsansvarlig før Underdatabehandleren kan behandle Personopplysninger. Behandlingsansvarlig har gitt spesifikk godkjenning til bruk av Underdatabehandlere som angitt i Del II bokstav e). Databehandler plikter å inngå skriftlige avtaler med Underdatabehandleren i henhold til punkt 6.2 under.

Databehandler skal kun engasjere Underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at Behandlingen oppfyller kravene etter Databehandleravtalen, Gjeldende personvernlovgivning og som sikrer Registrertes Personopplysninger. Databehandleren skal gjennomføre egnede kontroller av Underdatabehandlerne for å verifisere deres databeskyttelsesnivå. Databehandleren skal fremlegge rapporter fra slike kontroller for den Behandlingsansvarlige.

Dersom Underdatabehandler ikke oppfyller sine forpliktelser i henhold til Databehandleravtalen eller Gjeldende personvernlovgivning skal Databehandler ha fullt ansvar overfor Behandlingsansvarlig.

6.2 Avtale med Underdatabehandler

Databehandleren skal inngå en skriftlig avtale med hver Underdatabehandler som pålegger Underdatabehandler de samme forpliktelser som gjelder for Databehandler etter Databehandleravtalen, med unntak av tilfeller som omfattes av punkt 6.3. Databehandler skal påse at Underdatabehandler ikke behandler Personopplysninger omfattet av Databehandleravtalen på annen måte enn det som er nødvendig for å levere tjenesten, og at Personopplysningene ikke overlates til andre for Behandling uten at dette følger av Databehandleravtalen eller på forhånd er skriftlig avtalt med Behandlingsansvarlig.

På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av avtaler med Underdatabehandlere. Forretningsmessig og annen forretnings sensitiv informasjon kan dog sladdes.

6.3 Forholdet til Underdatabehandleres standardavtaler

I den utstrekning Databehandler benytter en Underdatabehandler som leverer standardiserte tredjepartstjenester som Behandlingsansvarlig uttrykkelig har akseptert at leveres på Underdatabehandlerens standardvilkår («Standardavtalen»), og som Databehandleren følger opp på Behandlingsansvarliges vegne, kan Partene skriftlig bli enige om at Underdatabehandlerens standard databehandleravtale legges til grunn og gjøres gjeldende direkte overfor Behandlingsansvarlig som

et direkte databehandlerforhold forutsatt at den oppfyller kravene i Gjeldende personvernlovgivning. Databehandleren skal følge opp databehandleravtalen med Underdatabehandleren på vegne av Behandlingsansvarlig med mindre annet er avtalt i det enkelte tilfellet.

Dersom Behandlingsansvarlig etter en egen risikovurdering ikke anser Standardavtalen for å gi tilstrekkelig beskyttelse av personopplysninger i henhold til Gjeldende personvernlovgivning, kan Behandlingsansvarlig motsette seg bruk av Underdatabehandleren, og skal sammen med Databehandler forsøke å finne en Underdatabehandler som gir tilstrekkelige garantier for personvern og informasjonssikkerhet. Der Databehandler og Behandlingsansvarlig ikke finner en alternativ Underdatabehandler, kan Behandlingsansvarlig heve Hovedavtalen og Databehandleravtalen med umiddelbar virkning.

6.4 Bytte av Underdatabehandler

Hvis Databehandler ønsker å engasjere en ny Underdatabehandler eller gjøre andre endringer i Del II over Underdatabehandler som skal Behandle Personopplysninger under Databehandleravtalen, skal Databehandler skriftlig varsle Behandlingsansvarlig om endringen minimum 3 måneder før den iverksettes. Behandlingsansvarlig skal svare på henvendelsen fra Databehandler senest 1 måned etter at skriftlig varsel er mottatt om endringen aksepteres eller ikke. Hvis Behandlingsansvarlig ikke aksepterer endringen, og Databehandler ikke med rimelighet kan tilby et annet alternativ, kan Behandlingsansvarlig heve Hovedavtalen og Databehandleravtalen med umiddelbar virkning.

7. OVERFØRING TIL UTLANDET

Databehandleren skal bare overføre Personopplysninger til land utenfor EU/EØS-området (Tredjeland) eller internasjonale organisasjoner etter dokumentert instruks fra Behandlingsansvarlig, og slik overføring skal alltid skje i overensstemmelse med GDPR kapittel V. Behandlingsansvarlig har samtykket til overføring til land hvor Underdatabehandlerne angitt i Del II er lokalisert.

Dersom Behandlingsansvarlig har gitt skriftlig samtykke gjennom instruks til overføring av Personopplysninger til et Tredjeland, plikter Databehandleren å påse at slik overføring skjer i henhold til GDPR kapittel V. Databehandler plikter å dokumentere at det foreligger et gyldig overføringsgrunnlag i henhold til GDPR kapittel V. Databehandler skal til enhver tid påse at det foreligger et gyldig overføringsgrunnlag med påkrevde tekniske og organisatoriske tiltak som sikrer etterlevelse av GDPR i samsvar med relevant praksis og retningslinjer fra EDPB (European Data Protection Board). Som del av å dokumentere at gyldig overføringsgrunnlag foreligger skal Databehandler synliggjøre sine interne risikovurderinger for Behandlingsansvarlig, samt Databehandlerens tekniske og organisatoriske tiltak ved overføringen av Personopplysninger til Tredjeland.

Uten dokumentert instruks fra Behandlingsansvarlig kan Databehandler innenfor rammen av Databehandleravtalen således ikke:

- a. overføre personopplysninger til en behandlingsansvarlig eller databehandler i et tredjeland eller en internasjonal organisasjon
- b. overlate behandling av personopplysninger til en Underdatabehandler i et tredjeland,
- c. behandle personopplysninger i et tredjeland

Hvis Databehandler ønsker å overføre Personopplysninger til et Tredjeland gjennom Underdatabehandlere som ikke er angitt i Del II, skal Databehandler følge prosedyre i pkt. 6.3, herunder skriftlig varsle Behandlingsansvarlig om dette senest 3 måneder før overføringen finner sted. Behandlingsansvarlig skal svare på henvendelsen fra Databehandler senest innen 1 måned. Hvis Behandlingsansvarlig ikke samtykker til overføringen, og Databehandleren ikke med rimelighet kan tilby et annet alternativ, har Behandlingsansvarlig rett til å heve Hovedavtalen og Databehandleravtalen med umiddelbar virkning.

8. ERSTATNING

Dersom Databehandler ikke overholder sine plikter i henhold til denne Databehandleravtale og/eller Gjeldende personvernlovgivning, vil dette anses som mislighold av Hovedavtalen, og de plikter, frister, sanksjoner og ansvarsbegrensninger som følger av Hovedavtalens regulering av Leverandørens mislighold kommer til anvendelse, med unntak for regler om erstatningsbegrensning under den forutsetning at disse ikke er i samsvar med GDPR artikkel 82.

9. ANDRE BEHANDLINGSANSVARLIGE

Databehandleren anerkjenner at Personopplysningene også behandles på vegne av den Behandlingsansvarliges kunder. Slike andre behandlingsansvarlige har samme rettigheter som den Behandlingsansvarlige som er avtalepart, og de kan håndheve Databehandleravtalen som om de var avtalepart. 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 instruksjoner som om de var den Behandlingsansvarliges egne.

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

10. VARIGHET

Databehandleravtalen gjelder fra den dato den er signert av begge Parter og inntil opphør av Databehandlers tjenester til Behandlingsansvarlig. Unntak gjelder for de bestemmelser i Hovedavtalen og Databehandleravtalen som fortsetter å løpe etter avslutning av Hovedavtalen og Databehandleravtalen. Databehandleravtalen kan ikke sies opp så lenge Hovedavtalen består, med mindre den avløses av en ny databehandleravtale.

Ved avslutning av 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 Underdatabehandler 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 ufravikelig 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 Databehandleravtalen eller 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 og/eller slettet i henhold til Behandlingsansvarliges instruks, og at Databehandler ikke har beholdt noen kopi, utskrift eller beholdt dataene i annet medium.

Forpliktelsene etter pkt. 5.7 skal fortsetter å gjelde etter avslutning.

Partene skal revidere Databehandleravtalen i tilfelle relevante endringer i Gjeldende personvernlovgivning.

11. MISLIGHOLD OG PÅLEGG OM STANS

Ved brudd på Databehandleravtalen og/eller Gjeldende personvernlovgivning, kan Behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge Databehandler å stoppe hele eller deler av behandlingen av opplysningene med øyeblikkelig virkning.

Dersom Databehandler ikke overholder sine plikter i henhold til Databehandleravtalen og/eller Gjeldende personvernlovgivning, vil dette anses som vesentlig mislighold av Hovedavtalen, og gir Behandlingsansvarlig rett til å heve Databehandleravtalen og Hovedavtalen med umiddelbar virkning.

12. LOVVALG OG JURISDIKSJON

Databehandleravtalen skal være underlagt og tolkes i samsvar med norsk rett. Vernetings skal være Oslo tingrett.

Del II

Del II angir instruksjoner for, og utfyllende beskrivelse av behandlingen av personopplysninger under Databehandleravtalen, og utgjør en integrert del av Databehandleravtalen.

a) Behandlingens formål og karakter

Databehandlers behandling av Personopplysninger på vegne av den Behandlingsansvarlige omhandler (karakteren av Behandlingen):

- [Eksempel: Behandlingen av personopplysninger på vegne av Behandlingsansvarlig består i å stille system X til rådighet, samt utføre nødvendig vedlikehold av systemet.]
- [Eksempel: Behandlingen av personopplysninger på vegne av Behandlingsansvarlig består i å yte support og vedlikeholdstjeneste av system X, og i den relasjon koble seg på Behandlingsansvarlig sitt system]

Databehandler vil behandle Personopplysninger for følgende formål:

- [Fyll inn hva som er formålet eller formålene med Behandlingen]
- [Eksempel: Formålet med Behandlingen er å gi ansatte hos Behandlingsansvarlig tilgang til system X]
- [Eksempel: Formålet med Behandlingen er å yte support ved behov ved bruk av system X]

Databehandler vil behandle Personopplysninger på følgende måte:

- [Fyll inn på hvilken måte Databehandleren skal behandle personopplysninger]
- [Eksempel: Databehandler vil registrere og lagre kontaklinformasjon til ansatte hos Behandlingsansvarlig for å stille system X til disposisjon.]
- [Eksempel: Databehandler vil arkivere lyd- og filmopptak for fremtidig bruk på vegne av Behandlingsansvarlig mens Hovedavtalen løper]

b) Kategorier av Registrerte

Personopplysningene omhandler følgende personer:

- [Fyll inn hvilke(n) gruppe(r) av fysiske personer personopplysningene omhandler]
- [Eksempel: Kunder av Behandlingsansvarlig]
- [Eksempel: Ansatte og annet personell hos Behandlingsansvarlig]

c) Kategorier av Personopplysninger

Databehandler vil behandle følgende personopplysninger:

- [Fyll inn hvilke typer av personopplysninger som behandles, og hvem personopplysningene retter seg mot]
- [Eksempel: Kontaklinformasjon, som navn, epost, adresse, telefonnummer (...)]
- [Eksempel: Sensitive opplysninger som skatt- og lønn, og andre personlige forhold]

d) Særlige kategorier av personopplysninger

- [Fyll inn hvilke særlige kategorier av personopplysninger som eventuelt skal behandles]

Kommentert [Forfatter1]: Det skal gis en beskrivelse av Behandlingens karakter, følgelig hvilke konkrete oppgaver ved tjenesten som krever behandling av Personopplysninger.

Kommentert [Forfatter2]: Personopplysninger skal kun behandles for spesifikke, uttrykkelig angitte og berettigede formål.

At formålet skal være spesifikt, innebærer at det må være konkret angitt. Mer overordnede formål som for eksempel "personaladministrasjon" må normalt brytes ned i andre formål som for eksempel "rekruttering", "tilrettelegging av arbeidsforhold" og "adgangskontroll". Formålet må være så konkret at det er mulig å vurdere om de registrerte opplysningene er nødvendige, og om behandlingen skjer i samsvar med forordningens bestemmelser.

At formålet skal være uttrykkelig angitt, innebærer at det må formidles klart, og ikke kan være underforstått.

At formålet skal være berettiget, innebærer at behandlingen må være i samsvar med annet regelverk, og tilfredsstillende andre samfunnskrav. Formålet må i tillegg være saklig begrunnet i den behandlingsansvarliges virksomhet. Dette betyr at formålet må svare til hva som normalt kan forventes i den typen virksomhet som den behandlingsansvarlige driver.

Kommentert [Forfatter3]: Med *behandling* menes 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.

Kommentert [Forfatter4]: Det skal angis hvordan Personopplysningene behandles, herunder hvorvidt de samles inn, registreres, og/eller lagres.

Kommentert [Forfatter5]: Det skal angis konkret hvilke typer Personopplysninger som behandles. Opplysningene i eksemplene er ikke uttømmende for hva slags Personopplysninger som kan behandles.

Kommentert [Forfatter6]: Dette gjelder personopplysninger om

- rasemessig eller etnisk opprinnelse
- politisk oppfatning
- religion
- filosofisk overbevisning
- helseopplysninger
- fagforeningsmedlemskap
- genetiske opplysninger
- biometriske opplysninger (når behandlingsformålet er å entydig identifisere noen)
- seksuelle forhold
- seksuell legning

- [Helseopplysninger om ansatte: [sykmeldinger, tilrettelegging (...)]
- [Eksempel: Politisk oppfatning, etnisk opprinnelse og seksuell legning]

Kommentert [Forfatter7]: Eksempel.

e) Underdatabehandler, inkludert geografisk plassering av Behandlingen

Navn	Org. nr.	Adresse	Land	Beskrivelse av Behandling
Eksempel: Microsoft Ireland Operations Limited	IE 8256796	One Microsoft Place, South County Business Park, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	EU/EØS	Behandling av kontaktinformasjon for tilgang til Microsoft 365.

Kommentert [Forfatter8]: Det er lagt inn eksempel på hvordan en Underdatabehandler kan føres opp i oversikten over Underdatabehandlere.

f) Særlige sikkerhetstiltak som får anvendelse for Databehandler

Databehandler skal ha på plass sikkerhetstiltak som er adekvate sett i forhold til den risikoen Behandlingen av Personopplysninger på vegne av Behandlingsansvarlig representerer. Slike tiltak er som følger:

[Følgende er eksempler på sikkerhetstiltak som må vurderes konkret i hvert enkelt tilfelle, basert på risiko]:

- Dokumentere en ansvarsinndeling i Databehandlers virksomhet med klare ansvarsområder for ivaretagelse av informasjonssikkerheten.
- Kunne dokumentere en sikkerhetsstrategi for Behandlingen, herunder en strategi for å nå konkrete sikkerhetsmål, gjennomføre risikovurderinger, og virkemidler for å nå sikkerhetsmålene for Behandlingen.
- Databehandlers plikt til å gjennomføre risikovurderinger, herunder revidere eksisterende risikovurderinger ved endringer, samt at Behandlingsansvarlig får tilgang til vurderingene.
- Kunne dokumentere at alle som behandler Personopplysninger, herunder ansatte, Underdatabehandlere og andre mottakere av Personopplysninger, er underlagt krav som sikrer en Behandling i henhold til personvernprinsippene angitt i GDPR artikkel 5.
- Ha et system for tilgangskontroll til data som sikrer at bare ansatte med et arbeidsrelatert behov for tilgang til Personopplysninger har tilgang
- Ha et system for tilgangskontroll til bygninger og utstyr som sørger for at bare ansatte med et arbeidsrelatert behov for tilgang, har tilgang
- Dokumentere at Databehandlers virksomhet benytter verktøy for virusbeskyttelse, spam-filtre og brannmur og andre nødvendige tekniske tiltak, i den grad det er nødvendig ut fra risikoen ved den konkrete Behandlingen.
- Dokumentere loggføring av alle kritiske systemoperasjoner

- Kryptere kommunikasjon dersom det anses nødvendig eller påkrevet av hensyn til å gi tilstrekkelig informasjonssikkerhet etter GDPR. Helseopplysninger og andre Personopplysninger som krever særskilt beskyttelse under GDPR skal alltid krypteres
- Ha prosedyrer for sletting og anonymisering av Personopplysninger der formålet med Behandlingen er oppfylt.
- Utarbeide prosedyrer for lagring og avhendelse av datamedium.
- Ha systemer for backup/gjenopprettingsprosess for alle kritiske systemer og gjenopprettingstester for å hindre tap av data og Personopplysninger.
- Dokumentere interne retningslinjer for ivaretagelse av informasjonssikkerhet og personvern hos ansatte som håndterer personopplysninger, samt taushetsavtaler med ansatte, og gjennomføring av intern opplæring i informasjonssikkerhet ved håndtering av personopplysninger.

Dokumentere at Databehandler som del av sin tjeneste aktivt styrer og tar ansvar for å etterleve kravene til informasjonssikkerhet i GDPR gjennom nødvendige tekniske og organisatoriske tiltak.

Databehandler skal kunne dokumentere tiltakene som er opplistet ovenfor så langt Gjeldende personvernlovgivning krever dette. Dokumentasjonen skal være tilgjengelig for Behandlingsansvarlig.

g) Behandling av personopplysninger i forbindelse med testing [Dersom aktuelt]

- Databehandler vil, i forbindelse med levering av tjeneste som beskrevet her og i Hovedavtalen, behandle personopplysninger ved testing av programvare som innebærer overføring til Tredjeland. Slik testing er forhåndsgodkjent av Behandlingsansvarlig, og skal skje i henhold til Databehandleravtalens standardtekst punkt 7.
- Databehandler skal sørge for at Personopplysningene som behandles under testingen er adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»). I denne sammenheng skal Databehandler løpende vurdere tiltak som pseudonymisering og/eller andre egnede tiltak.
- Bruk av Underdatabehandlere i forbindelse med testing som kan involvere Behandling av Personopplysninger følger Databehandleravtalens standardtekst punkt 6.2 og 6.3.

h) [ANDRE SÆRLIGE REGULERINGER FOR BEHANDLING AV PERSONOPPLYSNINGER]

- **Sett inn andre aktuelle bestemmelser for regulering av den konkrete Behandlingen*

Kommentert [HE9]: Her skal det beskrives hvordan avvik som ikke er brudd på personopplysningssikkerheten skal meldes Behandlingsansvarlig, jf. Pkt. 5.5 avsnitt 4. Punktet må tilpasses hva som er mest hensiktsmessig for den enkelte behandling.
Forslag til formulering:
Ethvert avvik som ikke er brudd på personopplysningssikkerheten skal skriftlig meldes Behandlingsansvarlig i en ukentlig/månedlig/kvartalsvis/halvårlig/årlig rapport.

SIGNATUR

Databehandler

Signatur:
Navn:
Tittel:
Dato: [Klikk her for å velge dato.](#)

Behandlingsansvarlig

Signatur:
Navn:
Tittel:
Dato: [Klikk her for å velge dato.](#)