

**Avtale om levering av Facility Management system til Bergen kommune.**

**BILAG 10 Databehandleravtale**

**Databehandleravtaleinngått mellom**

<Angi navn på virksomhet og organisasjonsnummer>

(heretter kalt Behandlingsansvarlig)

**og**

<Angi navn på virksomhet og organisasjonsnummer>

(heretter kalt Databehandler)

i fellesskap kalt Partene.

**Sted og dato:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Avtalen er signert elektronisk

Avtaleparter

[Navn på den som signerer på vegne av Behandlingsansvarlig]

[Navn på den som signerer på vegne av Databehandler]

Alt 2:

|  |  |
| --- | --- |
| For Behandlingsansvarlig | For Databehandler |
| <Navn på den som signerer på vegne av Behandlingsansvarlig>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Underskrift | <Navn på den som signerer på vegne av Databehandler>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Underskrift |

Avtalen undertegnes i to eksemplarer, ett til hver part.

Denne avtalen er knyttet til avtale datert XX.XX.XXXX mellom partene, heretter omtalt som Hovedavtalen

**INNHOLDSFORTEGNELSE:**

[1 Formålet med denne Databehandleravtalen 3](#_Toc54833365)

[2 Generelt om Databehandleravtalen 3](#_Toc54833366)

[3 Definisjoner 4](#_Toc54833367)

[4 Behandlingsansvarliges plikter og rettigheter 4](#_Toc54833368)

[5 Behandlingsansvarliges instrukser til Databehandleren 5](#_Toc54833369)

[6 Konfidensialitet og taushetsplikt 5](#_Toc54833370)

[7 Bistand til behandlingsansvarlig 6](#_Toc54833371)

[8 Sikkerhet ved behandlingen 6](#_Toc54833372)

[9 Melding om brudd på personopplysningssikkerheten 7](#_Toc54833373)

[10 Bruk av Underleverandør 7](#_Toc54833374)

[11 Overføring av personopplysninger til land utenfor EU/EØS-området eller til internasjonale organisasjoner 9](#_Toc54833375)

[12 Generelt om revisjon 9](#_Toc54833376)

[13 Sletting og tilbakelevering av opplysninger 10](#_Toc54833377)

[14 Mislighold og pålegg om stans 11](#_Toc54833378)

[15 Erstatning 11](#_Toc54833379)

[16 Varighet og opphør 11](#_Toc54833380)

[17 Lovvalg og verneting 11](#_Toc54833381)

[18 Bilag til Databehandleravtalen 13](#_Toc54833382)

[BILAG A: Opplysninger om behandlingen 15](#_Toc54833383)

[BILAG B: Betingelser for Databehandlerens bruk og endring av eventuelle Underleverandører 17](#_Toc54833384)

[BILAG C: Instruks vedrørende behandling av personopplysninger 19](#_Toc54833385)

[BILAG D: Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen 25](#_Toc54833386)

# Formålet med denne Databehandleravtalen

## Denne avtalen ("Databehandleravtalen») fastsetter partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av Behandlingsansvarlig som del av leveransene under Hovedavtalen. Databehandleravtalen har som formål å sikre at partene etterlever Gjeldende personvernregler.

# Generelt om Databehandleravtalen

## Databehandleravtalen består av dette dokumentet, samt Bilag A, B, C, og D.

## Ved motstrid mellom Hovedavtalen og Databehandleravtalen, har Databehandleravtalen forrang når det gjelder forhold spesifikt knyttet til behandling av personopplysninger. Ved motstrid mellom Databehandleravtalen og dens bilag, har bilagene forrang.

## Databehandleravtalen og dens bilag har rang foran Databehandlers eventuelle egne personvernvilkår, hva gjelder behandling av personopplysninger etter denne avtalen. Dette omfatter også avtaler mellom Databehandler og dennes underleverandører eller tredjeparter/samarbeidspartnere og eventuelle personvernvilkår disse måtte ha.

## Databehandleravtalens Bilag A inneholder nærmere beskrivelse av behandlingen som skal foretas, herunder om behandlingsformål, behandlingenes art, kategorier av personopplysninger og registrerte, regler for sletting og tilbakelevering, partenes kontaktpersoner, samt hvilken eller hvilke underliggende avtaler behandlingen av personopplysninger er knyttet til (se definisjonen av Hovedavtalen nedenfor).

## Databehandleravtalens Bilag B inneholder betingelser for bruk av Underleverandør, samt en oversikt over godkjente Underleverandører.

## Databehandleravtalens Bilag C inneholder spesifikke instrukser for behandling av personopplysninger under Hovedavtalen, herunder sikkerhetstiltak og Behandlingsansvarliges rett til innsyn og revisjon av Databehandler og eventuelle Underleverandører, samt sektorspesifikke bestemmelser om behandling av personopplysninger.

## Databehandleravtalens Bilag D inneholder endringer til standardteksten og eventuelle senere avtalte endringer i Databehandleravtalen.

# Definisjoner

**Gjeldende personvernregler:** Den til enhver tid gjeldende versjon av EUs personvernforordning (2016/679) ("personvernforordningen"), samt lov om behandling av personopplysninger av 15.06. 2018 (personopplysningsloven) med tilhørende forskrifter mv., samt eventuell annen relevant lovgivning og rettsavgjørelser som gjelder behandling og vern av personopplysninger og som er angitt i Bilag C, punkt C.8.

**Hovedavtalen:** En eller flere avtaler mellom Behandlingsansvarlig og Databehandler om levering av tjenester som innebærer behandling av personopplysninger, som nærmere angitt i Bilag A. Databehandleravtalen kan gjelde flere underliggende avtaler.

**Underleverandør:** Annen virksomhet som benyttes av Databehandler til behandling av personopplysninger under Hovedavtalen.

For personvernbegreper som ikke er definert i denne Databehandleravtalen gjelder definisjonene i personvernforordningen artikkel 4.

# Behandlingsansvarliges plikter og rettigheter

## Behandlingsansvarlig har ansvaret for at behandlingen av personopplysninger skjer i samsvar med Gjeldende personvernregler. Behandlingsansvarlig skal i den forbindelse særskilt sørge for at:

1. behandlingen av personopplysninger er formålsbestemt og basert på et gyldig rettsgrunnlag;
2. de registrerte har mottatt nødvendig informasjon om behandlingen av personopplysningene;
3. Behandlingsansvarlig har gjennomført tilstrekkelige risikovurderinger; og
4. Databehandler til enhver tid har tilstrekkelige instrukser og informasjon for å oppfylle sine plikter i henhold til Databehandleravtalen og Gjeldende personvernregler.
5. Behandlingsansvarlig har rett til å bestemme hvilke hjelpemidler som skal brukes i behandlingen.
6. Behandlingsansvarlig har rett til å si opp avtalen dersom databehandleren ikke lenger oppfyller Gjeldende personvernregler.

# Behandlingsansvarliges instrukser til Databehandleren

## Databehandleren skal behandle personopplysningene i samsvar med Gjeldende personvernregler og Behandlingsansvarliges dokumenterte instrukser, jf. punkt 4.2. Hvis annen behandling er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, skal Databehandleren underrette Behandlingsansvarlig så langt dette er tillat ved lov, jf. personvernforordningen artikkel 28 (3) (a).

## Behandlingsansvarliges instrukser fremgår av Hovedavtalen og Databehandleravtalen med bilag. Databehandler skal omgående underrette Behandlingsansvarlig, dersom vedkommende mener at instruksene er i strid med Gjeldende personvernregler, jf. personvernforordningen artikkel 28 (3) (h).

## Eventuelle endringer i instrukser skal varsles til Databehandler gjennom oppdatering av Bilag D, og skal implementeres av Databehandler innen det tidspunkt Partene avtaler eller, om ingen konkret frist er avtalt, innen rimelig tid. Databehandler kan kreve at Behandlingsansvarlig dekker dokumenterte kostnader som påløper i forbindelse med implementeringen av slike endringer eller forholdsmessig justering av vederlaget under Hovedavtalen dersom den endrede instruksen innebærer løpende ekstra kostnader for Databehandleren. Det samme gjelder merkostnader som følge av endring av Gjeldende personvernregler som gjelder Behandlingsansvarliges virksomhet.

# Konfidensialitet og taushetsplikt

## Databehandleren skal sikre at ansatte og andre som har tilgang til personopplysninger er autorisert til å behandle slike personopplysninger på Databehandlers vegne. Dersom slik autorisasjon utløper eller trekkes tilbake, skal tilgangen til personopplysningene opphøre uten ugrunnet opphold.

## Databehandleren skal kun autorisere personer som trenger tilgang til personopplysningene i forbindelse med arbeid for å kunne oppfylle Hovedavtalen (i.e.: tjenstlig behov), Databehandleravtalen og eventuelt annen behandling som er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, se punkt 4.1 siste setning.

## Databehandleren skal sikre at personer som er autorisert til å behandle personopplysninger på vegne av Behandlingsansvarlig er underlagt taushetsplikt gjennom avtale eller lov. Taushetsplikten skal bestå også etter avtalens og/eller ansettelsesforholdets opphør.

## Databehandleren skal kunne dokumentere at de relevante personer er underlagt ovennevnte taushetsplikt på forespørsel fra Behandlingsansvarlig.

## Ved opphør av Databehandleravtalen plikter Databehandleren å frata tilganger fra alt autorisert personell som har tilgang til personopplysninger som behandles under avtalen.

# Bistand til behandlingsansvarlig

## Databehandleren skal på forespørsel bistå Behandlingsansvarlig med oppfyllelse av de registrertes rettigheter etter personvernforordningens kapittel III gjennom egnede tekniske eller organisatoriske tiltak. Plikten til å bistå gjelder likevel bare i den utstrekning dette er mulig og hensiktsmessig sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.

## Databehandler skal uten ugrunnet opphold videresende alle henvendelser som Databehandler eventuelt mottar fra den registrerte vedrørende den registrertes rettigheter i henhold til Gjeldende personvernregler til Behandlingsansvarlig. Slike henvendelser kan kun besvares av Databehandler når dette er skriftlig godkjent av Behandlingsansvarlig.

## Databehandleren skal bistå Behandlingsansvarlig med å overholde kravene til personopplysningssikkerhet i personvernforordningen artikkel 32-36, herunder yte bistand ved personvernkonsekvensvurdering og forhåndsdrøftinger med Datatilsynet, sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.

## Behandlingsansvarlig kan fastsette nærmere instrukser om hvilke bistand Databehandleren skal gi i Databehandleravtalens Bilag C.

# Sikkerhet ved behandlingen

## Databehandler skal iverksette egnede tekniske og organisatoriske tiltak for å oppnå et tilfredsstillende sikkerhetsnivå sett hen til behandlingens karakter og omfang, den tekniske utviklingen, implementeringskostnader og aktuelle risikoer for fysiske personers rettigheter og friheter. Databehandleren skal som minimum iverksette de tiltak som er spesifisert i Databehandleravtalens Bilag C.

## Databehandleren skal foreta risikovurderinger for å sikre at et egnet sikkerhetsnivå opprettholdes til enhver tid. Databehandleren skal herunder sørge for jevnlig testing, analyse og vurdering av sikkerhetstiltakene, særlig med hensyn til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester, samt evne til raskt å gjenopprette tilgjengeligheten av personopplysningene ved hendelser.

## Databehandler skal dokumentere risikovurderingen og sikkerhetstiltakene, og gjøre dem tilgjengelig for Behandlingsansvarlig på forespørsel, samt gi adgang til slik revisjon som er avtalt mellom partene, jf. Databehandleravtalens punkt 11. Databehandler skal gi tilgang til annen relevant informasjon for Behandlingsansvarlig, for å bistå sistnevnte i å overholdelse av pliktene etter personvernforordningen artikkel 32.

# Melding om brudd på personopplysningssikkerheten

## Databehandler skal uten ugrunnet opphold skriftlig underrette Behandlingsansvarlig om eventuelle brudd på personopplysningssikkerheten, samt for øvrig gi slik bistand og informasjon som er nødvendig for at Behandlingsansvarlig skal kunne melde bruddet til tilsynsmyndigheter i tråd med Gjeldende personvernregelverk.

## Underretning etter punkt 8.1 skal meldes til kontaktpunktet for Behandlingsansvarlig i henhold til Bilag C punkt C.9, og skal:

1. beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
2. inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,
3. beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten, og
4. beskrive de tiltak som 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 følge av bruddet.

Informasjonen kan, i den grad det det er nødvendig, gis trinnvis uten ytterligere ugrunnet opphold.

## Databehandler plikter å gjennomføre alle de tiltak som med rimelighet kan kreves for å utbedre og unngå tilsvarende brudd på personopplysningssikkerheten. Databehandler skal, så langt det er mulig, rådføre seg med Behandlingsansvarlig om de tiltak som skal gjennomføres, herunder vurdere Behandlingsansvarliges eventuelle forslag til tiltak.

## 

## Behandlingsansvarlig er ansvarlig for å underrette Datatilsynet og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandler skal ikke informere tredjeparter om brudd på personopplysningssikkerheten med mindre noe annet er påkrevd etter gjeldende rett eller det følger av uttrykkelig skriftlig instruks fra Behandlingsansvarlig.

# Bruk av Underleverandør

## Databehandler kan kun benytte Underleverandører etter spesifikk skriftlig tillatelse fra Behandlingsansvarlig i samsvar med Databehandleravtalens Bilag B. Oversikt over godkjente Underleverandører fremgår av Databehandleravtalens Bilag B.

## Dersom en Databehandler engasjerer en Underleverandør for å utføre spesifikke behandlingsaktiviteter på vegne av Behandlingsansvarlig, plikter Databehandler å inngå skriftlig avtale med Underleverandøren som pålegger denne tilsvarende forpliktelser med hensyn til vern av personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen. Se punkt 10.8 med hensyn til bruk av standard tredjepartstjenester.

## Databehandler skal kun engasjere Underleverandører som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene etter Gjeldende personvernregler. Databehandler skal gjennomføre kontroller av Underleverandører for å verifisere at tilfredsstillende tiltak er iverksatt. Databehandler skal kunne fremlegge rapporter fra slike kontroller for Behandlingsansvarlig på forespørsel.

## Dersom Behandlingsansvarlig motsetter seg endringer i bruken av en Underleverandør etter Databehandleravtalens Bilag B punkt B.1 skal Partene i god tro forhandle med sikte på å enes om en rimelig løsning på hvordan videre levering av tjenestene under Hovedavtalen skal gjennomføres, herunder om fordeling av eventuelle kostnader mellom Partene. Endringen i bruk av Underleverandører kan ikke gjennomføres før Partene har kommet til enighet.

## Dersom Underleverandøren ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal Databehandleren overfor Behandlingsansvarlig være fullt ut ansvarlig, på samme måte som om Databehandler selv sto for behandlingen.

## Databehandler plikter å forelegge avtaler med Underleverandører for Behandlingsansvarlig når disse er inngått og på forespørsel fra Behandlingsansvarlig. Dette gjelder likevel bare de delene av avtalen som er relevant for behandlingen av personopplysningene og med de begrensninger som eventuelt måtte følge av lov eller forskrift. Rent kommersielle vilkår kan uansett ikke kreves fremlagt.

## Avtale mellom Databehandler og underleverandør skal sikre at Behandlingsansvarlig har rett til å håndheve rettigheter iht. denne Databehandleravtalen overfor Underleverandør dersom Databehandleren går konkurs. Dette innebære bl.a. at Behandlingsansvarlig kan kreve at Underleverandør sletter eller tilbakeleverer personopplysninger.

## I den utstrekning Databehandleren benytter underleverandør som leverer standardiserte tredjepartstjenester som Behandlingsansvarlig uttrykkelig har akseptert at leveres på underleverandørens standardvilkår i henhold til Hovedavtalen, og som Databehandleren følger opp på Behandlingsansvarliges vegne, kan partene blir enige om at underleverandørens standard databehandleravtale legges til grunn og gjøres gjeldende direkte overfor Behandlingsansvarlig som et direkte databehandlerforhold (altså ikke som Underleverandør) forutsatt at den oppfyller kravene i Gjeldende personvernregler. Databehandleren skal følge opp databehandleravtalen med underleverandøren på vegne av Behandlingsansvarlig med mindre annet er avtalt i det enkelte tilfellet.

# Overføring av personopplysninger til land utenfor EU/EØS-området eller til internasjonale organisasjoner

## Personopplysninger kan bare overføres til et land utenfor EØS-området ('Tredjestat') eller til internasjonal organisasjon hvis Behandlingsansvarlig skriftlig har godkjent slik overføring og vilkårene i punkt 10.3 er oppfylt. Som overføring regnes blant annet å:

* 1. behandle personopplysningene i datasentre o.l. som er lokalisert i Tredjestat eller av personell som er lokalisert i Tredjestat (ved fjerntilgang);
  2. overlate behandlingen av personopplysninger til Underleverandør i Tredjestat;
  3. utlevere personopplysningene til en Behandlingsansvarlig i Tredjestat eller i en internasjonal organisasjon; eller
  4. gi personell i tredjestater tilgang til personopplysninger som befinner seg innenfor EU/EØS.

## Databehandler kan likevel overføre personopplysninger dersom det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandler underrette Behandlingsansvarlig så langt dette er tillat ved lov.

## Overføring til Tredjestater eller internasjonale organisasjoner kan kun finne sted dersom det foreligger nødvendige garantier for et tilstrekkelig beskyttelsesnivå for personvern i henhold til Gjeldende personvernregler. Med mindre annet er avtalt mellom Partene kan slik overførsel kun finne sted med grunnlag i:

1. en av EU-kommisjonens beslutninger om tilstrekkelig beskyttelsesnivå i henhold til personvernforordningen artikkel 45; eller
2. en Databehandleravtale som inkorporerer standard personvernbestemmelser som angitt i personvernforordningen artikkel 46 (2) (c) eller (d) (EU Model clauses); eller
3. bindende virksomhetsregler (Binding Corporate Rules) i henhold til personvernforordningen artikkel 47.
4. Godkjente atferdsnormer i henhold til personvernforordningen artikkel 46. (2) (e).

## Behandlingsansvarliges eventuelle godkjennelse av at personopplysninger overføres til en Tredjestat eller internasjonal organisasjon skal fremgå av Databehandleravtalens Bilag B.

# Generelt om revisjon

## Databehandler skal på forespørsel gjøre tilgjengelig for Behandlingsansvarlig, all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i personvernforordningen artikkel 28 og denne Databehandleravtalen er oppfylt.

## Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved inspeksjoner fra aktuelle tilsynsmyndigheter. Behandlingsansvarliges tilsyn med eventuelle Underleverandører skal skje gjennom Databehandleren med mindre annet er særskilt avtalt. Nærmere rutiner for gjennomføring av revisjoner fremgår av bilag C punkt C.6.

## Dersom en revisjon avdekker avvik fra forpliktelsene i Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler så snart som mulig utbedre avviket. Behandlingsansvarlig kan kreve at Databehandleren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Behandlingsansvarlig.

## Hver av Partene dekker sine egne kostnader forbundet med en årlig revisjon. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandleren likevel dekke Behandlingsansvarliges rimelige kostnader forbundet med revisjonen.

# Sletting og tilbakelevering av opplysninger

## Ved opphør av denne Databehandleravtalen plikter Databehandler å tilbakelevere og/eller slette alle personopplysninger som behandles på vegne av Behandlingsansvarlig under Databehandleravtalen i samsvar med bestemmelsene i Bilag C punkt C.7. Dette gjelder også eventuelle sikkerhetskopier.

## Behandlingsansvarlig bestemmer hvordan en eventuell tilbakelevering av personopplysninger skal skje. Behandlingsansvarlig kan kreve at tilbakelevering skjer på et strukturert og alminnelig anvendt maskinlesbart format. Behandlingsansvarlig skal dekke Databehandlerens dokumenterte kostnader til tilbakelevering med mindre dette er inkludert i vederlaget under Hovedavtalen.

## Hvis det benyttes delt infrastruktur eller backup der direkte sletting ikke er teknisk mulig, skal Databehandler sørge for at personopplysningene gjøres utilgjengelige inntil de er overskrevet.

## Databehandler skal bekrefte skriftlig overfor Behandlingsansvarlig at sletting eller utilgjengeliggjøring er foretatt og skal på forespørsel dokumentere hvordan det er gjennomført.

## Nærmere bestemmelser om sletting og tilbakeleveringer fremgår av bilag C.

# Mislighold og pålegg om stans

## Ved brudd på Databehandleravtalen og/eller Gjeldende personvernregler, 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 denne Databehandleravtale og/eller Gjeldende personvernregler, 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 mindre annet er uttrykkelig avtalt mellom partene i Bilag D.

# Erstatning

## Behandlingsansvarlig har krav på erstatning for tap som følge av at Databehandler ikke har overholdt sine forplikter i henhold til denne databehandleravtalen.

## Dette omfatter også Behandlingsansvarliges rett til å få tilbakebetalt eventuell utbetalt erstatning til den skadelidte ved et solidarisk ansvar og evt. overtredelsesgebyrer e.l. som Behandlingsansvarlig blir pålagt av aktuelle tilsynsmyndigheter og som kan tilbakeføres til forhold på Databehandlers hånd.

# Varighet og opphør

## Databehandleravtalen gjelder fra den er signert av begge Parter. Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig. Den gjelder også for eventuelle personopplysninger som måtte finnes hos Databehandler eller noen av dennes Underleverandører etter Hovedavtalens opphør.

## Reglene om oppsigelse i Hovedavtalen gjelder tilsvarende for Databehandleravtalen, så langt det passer. Databehandleravtalen kan ikke sies opp så lenge Hovedavtalen består med mindre den avløses av en ny databehandleravtale.

Partene har rett til å kreve at Databehandleravtalen reforhandles dersom det skjer endringer i Gjeldende personvernregler, gjennom f.eks. nye bestemmelser, nye lover, rettspraksis, e.l. som får betydning for avtaleforholdet mellom partene.

# Lovvalg og verneting

Avtalen er underlagt norsk rett. Tvister løses i samsvar med Hovedavtalens bestemmelser, herunder eventuelle bestemmelser om verneting (kontroller om dette er regulert i hovedavtale). For avtaler der Bergen kommune er behandlingsansvarlig er Bergen tingrett verneting.

\*\*\*

# Bilag til Databehandleravtalen

**Bilag A – OPPLYSNINGER OM BEHANDLINGEN**

**Bilag B - BETINGELSER FOR DATABEHANDLERENS BRUK AV UNDERLEVERANDØRE**

**Bilag C – INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER**

**Bilag D – ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST GO ENDRINGER ETTER AVTALEINNGÅELSEN**

[A. Opplysninger om behandlingen 3](#_Toc47965292)

[A.1 Hovedavtalen og formålet med behandlingen av personopplysninger 3](#_Toc47965293)

[A.2 Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig 3](#_Toc47965294)

[A.3 Typer av personopplysninger 4](#_Toc47965295)

[A.4 Kategorier av registrerte 4](#_Toc47965296)

[A.5 Varighet av behandlingen 4](#_Toc47965297)

[B. Betingelser for Databehandlerens bruk og endring av eventuelle Underdatabehandlere 5](#_Toc47965298)

[B.1 Behandlingsansvarliges godkjennelse av bruk av Underdatabehandlere 5](#_Toc47965299)

[B.2 Godkjente Underdatabehandlere 6](#_Toc47965300)

[C. Instruks vedrørende behandling av personopplysninger 7](#_Toc47965301)

[C.1 Behandlingens omfang og formål 7](#_Toc47965302)

[C.2 Sikkerhet ved behandlingen 7](#_Toc47965303)

[C.2.1 Angivelse av sikkerhetsnivå 7](#_Toc47965304)

[C.2.2 Styringssystem for informasjonssikkerhet 8](#_Toc47965305)

[C.3 Innebygd personvern og personvern som standardinnstilling 8](#_Toc47965306)

[C.4 Dokumentasjon 8](#_Toc47965307)

[C.5 Overføring av personopplysninger - Lokasjon for behandling og tilgang 8](#_Toc47965308)

[C.6 Rutiner for revisjon og tilsyn 9](#_Toc47965309)

[C.7 Sletting og tilbakelevering av personopplysninger ved avtalens opphør 10](#_Toc47965310)

[C.8 Sektorspesifikke bestemmelser om behandling av personopplysninger 10](#_Toc47965311)

[C.9 Kontaktinformasjon 11](#_Toc47965312)

[D. Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen 12](#_Toc47965313)

# BILAG A: Opplysninger om behandlingen

## **A.1** **Hovedavtalen og formålet med behandlingen av personopplysninger**

Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig er knyttet til å levere tjenester som beskrevet i Hovedavtalen.

Med Hovedavtalen menes følgende avtale(r) inngått mellom partene:

*<****Sett inn navn og dato for inngåelse av den eller de underliggende tjenesteavtalen(e) som Databehandleravtalen er knyttet til.****>*

*<Merknad: Hvis det er flere tjenesteavtaler som benytter samme databehandleravtale kan de angis samlet her eller det kan utarbeides et bilagssett for hver avtale, avhengig av om behandlingens art og omfang, og graden av ensartethet på Behandlingsansvarliges instrukser, er slik at det mest hensiktsmessig beskrives samlet eller hver for seg.>*

Behandlingen har følgende formål:

**<*Beskriv behandlingsformål, for eksempel:***

* *Analyse av brukertilfredshet i prosjekt X, som nærmere beskrevet i Hovedavtalens Bilag 1*
* *Levering av skylagringstjenester som nærmere beskrevet i Hovedavtalens Bilag 1*
* *Bruk av system X til innsamling og behandling av opplysninger om Behandlingsansvarliges ansatte som nærmere beskrevet i Hovedavtalens Bilag 1>*

## **A.2** **Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig** **(behandlingenes art)**

Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig omhandler (karakteren av behandlingen):

***<Beskriv hva behandlingen omfatter, for eksempel****:*

* *Innsamling, lagring og analyse av brukertilfredshetsundersøkelser som beskrevet i Hovedavtalens Bilag 1*
* *Registrering, organisering og oppbevaring av personopplysninger i system X**som nærmere beskrevet i Hovedavtalens Bilag 1>*

## **A.3** **Typer av personopplysninger**

Behandlingen omfatter følgende typer av personopplysninger om de registrerte (flere valg mulig):

|  |  |
| --- | --- |
|  | *Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1):*  <*Angi type, f.eks. helseopplysninger, rasemessig eller etnisk opprinnelse eller fagforeningstilhørighet*> |
|  | *Andre opplysninger med særlig behov for beskyttelse:*  *<Angi type, f.eks. fødselsnummer, opplysninger om økonomi, prestasjonsvurderinger i ansettelsesforhold osv.>* |
|  | *Ordinære personopplysninger:*  *<Angi type, f.eks. Identifisering og kontaktinformasjon, Kontonummer, økonomiske opplysninger, kommunikasjonspreferanser, kandidatopplysninger, atferd på nett, osv.>* |

## **A.4 Kategorier av registrerte**

Behandlingen omfatter følgende kategorier av registrerte:

**<Beskriv hvem behandlingen av personopplysninger omfatter*, for eksempel:*** *«Innbyggere i Bergen kommune", "Elev/barnehagebarn"* eller *"Foresatte til elev/barnehagebarn", «Pasient», «tjenestemottaker av avlastningstjester, støttekontakt med mer», «Tjenestemottaker i barnevernet», «Mottaker av sosialtjenester», «Brukere av kulturtilbud», «Tjenesteleverandører», «Ansatte og innleide», «Jobbsøkere».*

*Dersom det behandles opplysninger om en særlig sårbar eller utsatt gruppe som f.eks. barn eller handikappede bør det oppføres særskilt.****>***

## **A.5 Varighet av behandlingen**

Databehandlers behandling av personopplysninger under Hovedavtalen kan påbegynne når Databehandleravtalen har trådt i kraft. Behandlingen har følgende varighet (velg ett alternativ):

|  |  |
| --- | --- |
|  | Behandlingen er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen. |
|  | Behandlingen er tidsbegrenset, og gjelder frem til *<angi dato eller kriterium for avslutning, eksempelvis avslutningen av et prosjekt. Merk at behandlingen normalt ikke kan avsluttes før Hovedavtalen utløper>.* |

Ved opphør (av avtalen eller en behandling) skal personopplysninger tilbakeleveres og slettes i samsvar med Databehandleravtalen punkt 13 og instruksjonene i Bilag C.

databehandlerens bruk av underleverandører.

# 

# BILAG B: Betingelser for Databehandlerens bruk og endring av eventuelle Underleverandører

## **B.1 Behandlingsansvarliges godkjennelse av bruk av Underleverandører**

Ved inngåelse av Databehandleravtalen godkjenner Behandlingsansvarlig bruk av de Underleverandører som er oppført i punkt B.2. Merk at også mor-, søster- og datterselskaper til Databehandleren regnes som Underleverandører hvis de bidrar til leveransen og behandler personopplysninger.

For endringer i bruk av Underleverandører er det i tillegg avtalt følgende:

|  |  |
| --- | --- |
|  | Databehandleren kan benytte Underleverandør som i samme konsern (mor- søster- eller datterselskap) som er etablert i et land innenfor EØS-området. Databehandleren skal på forhånd informere Behandlingsansvarlig om bruken av slik Underleverandør. (Dette alternativet kan kombineres med et av de andre alternativene.) |
|  | Databehandler kan kun gjennomføre endringer i bruken av Underleverandører etter spesifikk og forutgående skriftlig godkjennelse fra Behandlingsansvarlig. Underleverandøren kan ikke behandle personopplysninger under Hovedavtalen før slik godkjennelse er gitt. Godkjennelse kan ikke nektes uten saklig grunn. |

<Merknad: Hvis Databehandler benytter underleverandør (tredjepart) som leverer standardiserte tredjepartstjenester (typisk skytjenester), og som oppfyller vilkårene i Databehandleravtalen punkt 10.7, slik at tredjepartens standard databehandleravtale kommer til anvendelse direkte overfor Behandlingsansvarlig, vil skifte av underleverandør hos tredjeparten følge bestemmelsene i tredjepartens databehandleravtale.>

## **B.2 Godkjente Underleverandører**

Behandlingsansvarlig har godkjent bruk av følgende Underleverandører:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Navn | Org.nr. | Adresse | Beskrivelse av behandling | Behandlingssted | Kontaktinformasjon | Særlige kategorier personopplysninger |
| *[Navn]* | *[Org.nr.]* | *[Adresse]* | *[Overordnet beskrivelse av behandlingen hos Underleverandøren]* | *[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i. Ved overføring utenfor EU/EØS må overføringsgrunnlag også oppgis]* | *[Kontaktinformasjon]* | *[Angi om det behandles særlige kategorier av personopplysninger]* |
| *[Navn]* | *[Org.nr.]* | *[Adresse]* | *[Overordnet beskrivelse av behandlingen hos Underleverandøren]* | *[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i. Ved overføring utenfor EU/EØS må overføringsgrunnlag også oppgis]* | *[Kontaktinformasjon]* | *[Angi om det behandles særlige kategorier av personopplysninger]* |
| *[Navn]* | *[Org.nr.]* | *[Adresse]* | *[Overordnet beskrivelse av behandlingen hos Underleverandøren]* | *[…]* | *[Kontaktinformasjon]* | *[Angi om det behandles særlige kategorier av personopplysninger]* |

Databehandleren kan ikke bruke den enkelte Underleverandøren til en annen behandling enn avtalt eller la en annen Underleverandør utføre den beskrevne behandlingen i andre tilfeller enn det som følger av Bilag B, punkt B.1 om skifte av Underleverandør.

# BILAG C: Instruks vedrørende behandling av personopplysninger

## **C.1 Behandlingens omfang og formål**

Personopplysningene skalutelukkende behandles i det omfang og for de formål som er beskrevet i

* Hovedavtalen
* Databehandleravtalen med bilag

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Databehandleravtalen, og kan ikke behandle disse til egne formål.

## **C.2 Sikkerhet ved behandlingen**

### C.2.1 Angivelse av sikkerhetsnivå

Ut fra en vurdering av omfanget av personopplysninger som blir behandlet, typen opplysninger og karakteren av behandlingen er det basert på en konkret risikovurdering fastsatt at behandlingen (velg ett alternativ):

|  |  |
| --- | --- |
|  | Krever et høyt sikkerhetsnivå. Begrunnelse:  *<Vis til risikovurderingen som er gjort og skriv begrunnelse>*  <*F.eks. Behandlingen* *omfatter store mengder av «særlige kategorier av personopplysninger» i henhold til GDPR artikkel 9 (1) som krever særlig beskyttelse>* |
|  |  |
|  | Ikke krever et høyt sikkerhetsnivå. Begrunnelse:  *<Vis til risikovurderingen som er gjort og skriv begrunnelse>*  < *F.eks.: Behandlingen omfatter bare opplysninger som er allment kjent som navn og adresse>* |

### C.2.2 Styringssystem for informasjonssikkerhet

Databehandleren skal ha et egnet styringssystem for informasjonssikkerhet. Databehandleren skal etablere og forvalte tilstrekkelige sikkerhetstiltak for å ivareta informasjonssikkerheten for behandling av personopplysningene, herunder (flere valg mulig):

|  |  |
| --- | --- |
|  | Sikkerhetskrav som beskrevet i Hovedavtalen: *<sett inn henvisning til konkret regulering i Hovedavtalen>* |
|  | Sikkerhetskrav som beskrevet nedenfor: *<Sett inn beskrivelse av relevante sikkerhetskrav>*   * Forhindre uautorisert utlevering, modifisering, fjerning eller ødeleggelse av informasjon, herunder: * Autentisering * Tilgangsstyring fysisk og systemteknisk * Logging og sporing * Kryptering * Fysisk sikring av områder og utstyr * Sikkerhetskopi * Fjernaksess og mobilt utstyr * Sikkerhetsarkitektur, Nettverksarkitektur og sikker sone * Overvåkning og avdekking av sikkerhetsbrudd og hendelser * Rutiner og prosedyrer for å overholde krav til personvern og informasjonssikkerhet i organisasjonen |

## **C.3 Innebygd personvern og personvern som standardinnstilling**

Databehandler skal ivareta kravene til innebygd personvern og personvern som standardinnstilling i løsninger/tjenester som Databehandler utvikler/bruker i behandlingen av personopplysninger.

## **C.4 Dokumentasjon**

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som fremkommer av Gjeldende personvernregler og Databehandleravtalen, herunder kravene til informasjonssikkerhet. Slik dokumentasjon skal oppbevares og ajourholdes så lenge Databehandleravtalen består, og gjøres tilgjengelig for Behandlingsansvarlig eller tilsynsmyndigheter på forespørsel.

## **C.5 Overføring av personopplysninger - Lokasjon for behandling og tilgang**

Behandling av de personopplysninger som avtalen omfatter kan ikke uten Behandlingsansvarliges forutgående skriftlige godkjennelse utføres på eller med tilgang fra andre lokasjoner enn de som er angitt i Bilag B.2. Med lokasjon menes:

## • Sted det er mulig å få tilgang til personopplysningene fra (aksessering)

## • Sted hvor personopplysningene bearbeides (prosesseres)

## • Sted hvor personopplysningene lagres

Begrensningen ovenfor gjelder ikke Databehandlerens mor-, søster- og datterselskaper som er etablert innenfor EØS-området. Databehandleren skal imidlertid på forespørsel fra Behandlingsansvarlig redegjøre for hvor personopplysningene til enhver tid behandles.

## **C.6 Rutiner for revisjon og tilsyn**

For å kontrollere etterlevelse av Gjeldende personvernregler og Databehandleravtalen er det avtalt følgende (flere valg mulig):

|  |  |
| --- | --- |
|  | Behandlingsansvarlig har rett til å utføre revisjon på Databehandlers forretningssted for å verifisere Databehandlers etterlevelse av sine plikter i henhold til denne Databehandleravtalen eller Gjeldende personvernregler.  Slike revisjoner skal:   * Gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året, med mindre sikkerhetsbrudd hos Databehandler eller andre særlige forhold gir grunn for hyppigere revisjoner; * Foregå innenfor normal arbeidstid og ikke forstyrre Databehandlers virksomhet unødvendig; * Utføres av ansatte hos Behandlingsansvarlig eller av tredjepart som er godkjent av Partene og underlagt taushetsplikt.   Databehandler plikter å stille til rådighet de ressurser som med rimelighet kan kreves for å gjennomføre revisjonen.  Behandlingsansvarlig skal dekke kostnader for eventuelle tredjeparter som benyttes til å gjennomføre revisjonen. For øvrig dekker Partene sine egne kostnader ved gjennomføring av revisjonen. Dersom revisjonen avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler likevel dekke Behandlingsansvarliges rimelige kostnader ved revisjonen. |
|  | Databehandleren skal benytte ekstern revisor til å attestere at sikkerhetstiltak er etablert og virker etter hensikten. Slik revisjon skal:   1. gjennomføres én gang årlig, 2. utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402. 3. utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring   Når ekstern revisor har ferdigstilt revisjonsrapport, skal den oversendes Behandlingsansvarlig. Revisjonsrapporter skal også fremlegges for Behandlingsansvarlig på forespørsel.  Databehandler skal i tillegg gi slik informasjon og bistand som er nødvendig for at Behandlingsansvarlig kan etterleve sine forpliktelser etter Gjeldende personvernregelverk. |
|  | For standardiserte tredjepartstjenester som leveres av Underleverandør kan det fremlegges tredjepartsrevisjon forutsatt at revisjonen er gjennomført etter alminnelig anerkjente prinsipper og av sertifisert revisor. |
|  | *<Sett inn eventuelle andre avtalte rutiner for revisjon, herunder eventuelle særskilte eller avvikende rutiner for revisjon hos Underleverandør>* |

## **C.7 Sletting og tilbakelevering av personopplysninger ved avtalens opphør**

Partene har avtalt følgende om sletting/tilbakelevering av personopplysninger (velg ett alternativ):

|  |  |
| --- | --- |
|  | Alle personopplysninger som behandles under denne Databehandleravtale skal slettes uten ugrunnet opphold og senest innen 90 kalenderdager etter opphør av Hovedavtalen. Det samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig. |
|  | Alle personopplysninger som behandles under denne Databehandleravtale, samt eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig, skal tilbakeleveres ved opphør av Hovedavtalen.  Etter tilbakelevering er skjedd, plikter Databehandler å slette alle personopplysninger og annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig innen 30 kalenderdager.  Tilbakelevering skal skje på følgende måte:  *<Angi hvordan og hvilket format som skal benyttes for tilbakelevering>* |
|  | *<Sett inn eventuelle andre avtalte rutiner for sletting eller tilbakelevering>* |

## **C.8 Sektorspesifikke bestemmelser om behandling av personopplysninger**

<*Sett inn eventuelle sektorspesifikke bestemmelser om behandling av personopplysninger som skal omfattes av begrepet "Gjeldende personvernregler", se databehandleravtalen punkt 2.*>

## **C.9 Kontaktinformasjon**

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningssikkerheten eller endring i bruk av underleverandører, skal følgende kanaler benyttes:

|  |  |
| --- | --- |
| **Hos Behandlingsansvarlig** | **Hos Leverandøren** |
| Sikkerhetsbrudd: | Sikkerhetsbrudd: |
| Telefon: *[Fyll ut]* | Telefon: *[Fyll ut]* |
| E-post *[Fyll ut]* | E-post *[Fyll ut]* |
| Andre henvendelser: | Andre henvendelser: |
| Navn: *[Fyll ut]* | Navn: *[Fyll ut]* |
| Stilling: *[Fyll ut]* | Stilling: *[Fyll ut]* |
| Telefon: *[Fyll ut]* | Telefon: *[Fyll ut]* |
| E-post: *[Fyll ut]* | E-post: *[Fyll ut]* |

# BILAG D: Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen

*< Beskriv eventuelle endringer til databehandleravtalens standardtekst, samt endringer etter avtaleinngåelsen som er avtalt mellom partene>*