

## **BILAG TIL DATABEHANDLERAVTALEN**

**DETTE DOKUMENT BESTÅR AV FØLGENDE BILAG:**

**BILAG A – OPPLYSNINGER OM BEHANDLINGEN**

**BILAG B - BETINGELSER FOR DATABEHANDLERENS BRUK AV UNDERDATABEHANDLERE**

**BILAG C - INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER**

**BILAG D - ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER  
ETTER AVTALEINNGÅElsen**

## Bilag A, B, C, og D til Databehandleravtalen

A.	Opplysninger om behandlingen .....	3
A.1	Hovedavtalen og formålet med behandlingen av personopplysninger .....	3
A.2	Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige.....	3
A.3	Typer av personopplysninger .....	5
A.4	Kategorier av registrerte .....	6
A.5	Varighet av behandlingen.....	6
B.	Betingelser for Databehandlerens bruk og endring av eventuelle Underdatabehandlere6	
B.1	Behandlingsansvarliges godkjenning av bruk av Underdatabehandlere.....	7
B.2	Godkjente Underdatabehandlere .....	9
C.	Instruks vedrørende behandling av personopplysninger .....	10
C.1	Behandlingens omfang og formål .....	10
C.2	Sikkerhet ved behandlingen .....	10
C.2.1	Angivelse av sikkerhetsnivå .....	10
C.2.2	Styringssystem for informasjonssikkerhet .....	11
C.3	Dokumentasjon .....	12
C.4	Overføring av personopplysninger - Lokasjon for behandling og tilgang .....	12
C.5	Rutiner for revisjon og tilsyn .....	13
C.6	Sletting og tilbakelevering av personopplysninger ved avtalens opphør .....	15
C.7	Sektorspesifikke bestemmelser om behandling av personopplysninger.....	16
C.8	Kontaktinformasjon .....	17
D.	Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen	
	18	

## A. OPPLYSNINGER OM BEHANDLINGEN

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

Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig er knyttet til følgende hovedavtale:

SSA-D avtale om IT-driftstjenester, *sak ref doffin ...* mellom Direktoratet for mineralforvaltning med Bergmesteren for Svalbard og Leverandøren, med tilhørende bilag.

Behandlingen har følgende formål:

Databehandler skal behandle personopplysninger i den utstrekning det er nødvendig for å levere, etablere, drifte, administrere, sikre, overvåke, supportere, dokumentere, rapportere, vedlikeholde, videreutvikle og avslutte IT-driftstjenestene som er omfattet av Hovedavtalen.

Dette omfatter blant annet behandling som er nødvendig for:

- servicedesk og brukerstøtte,
- identitets- og tilgangsadministrasjon,
- administrasjon av Microsoft Entra ID, M365, Intune og tilhørende tjenester,
- klient- og mobiladministrasjon,
- nettverksdrift,
- serverdrift og privat sky,
- drift av utviklings-, test- og produksjonsmiljø,
- backup, gjenoppretting og disaster recovery,
- sikkerhetsovervåking, SOC/MDR/IRT og hendelseshåndtering,
- logging, revisjonsspor og sikkerhetsanalyse,
- rapportering, dokumentasjon, fakturagrunnlag og kontraktsoppfølging,
- etablering, migrering, overgang og exit.

Databehandler kan ikke behandle personopplysninger til egne formål, herunder analyse, produktutvikling, modelltrening, finjustering av KI-modeller eller forbedring av tjenester for andre kunder, uten Behandlingsansvarliges uttrykkelige skriftlige forhåndsgodkjenning.

### A.2 Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige

Databehandlerens behandling omfatter blant annet:

- innsamling, mottak, registrering og organisering av personopplysninger i saks-, support- og driftsverktøy,
- lagring, hosting, backup og gjenoppretting,
- tilgangsstyring, autentisering, autorisasjon og administrasjon av brukere,

## Bilag A, B, C, og D til Databehandleravtalen

- drift, overvåking, logging, analyse og sikring av systemer, nettverk, klienter, servere og skytjenester,
- fjernhjelp og fjernadministrasjon etter avtalte rutiner,
- feilsøking, feilretting og hendelseshåndtering,
- sikkerhetsanalyse, varselhåndtering, isolering og respons ved sikkerhetshendelser,
- dokumentasjon, rapportering og eksport av data,
- sletting, tilbakelevering og utilgjengeliggjøring ved avtalens opphør.

Behandlingen skal begrenses til det som er nødvendig for å oppfylle Hovedavtalen, Databehandleravtalen og dokumenterte instruksjoner fra Behandlingsansvarlig.

A.3 Typer av personopplysninger

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

<input checked="" type="checkbox"/>	<p><i>Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1):</i></p> <p>Behandlingen har ikke som selvstendig formål å behandle særlige kategorier av personopplysninger. Slike opplysninger kan likevel forekomme indirekte eller tilfeldig i Kundens data, eksempelvis i e-post, dokumenter, arkivdata, supportsaker, logger, backup eller fagsystemer som Databehandler drifter, sikrer, sikkerhetskopierer eller gjenoppretter.</p> <p>Databehandler skal ikke aktivt søke, bruke, analysere eller viderebehandle slike opplysninger utover det som er nødvendig for å levere avtalte tjenester og følge dokumenterte instruksjoner.</p>
<input checked="" type="checkbox"/>	<p><i>Andre opplysninger med særlig behov for beskyttelse:</i></p> <ul style="list-style-type: none"> <li>• autentiserings- og tilgangsdata,</li> <li>• sikkerhetsinformasjon og hendelsesdata,</li> <li>• opplysninger om privilegerte brukere og administrative tilganger,</li> <li>• fødselsnummer eller andre entydige identifikatorer der slike opplysninger forekommer i Kundens systemer, arkivdata, supportsaker, logger, backup eller fagsystemer,</li> <li>• opplysninger om sikkerhetshendelser, sårbarheter, misbruk, kontokompromittering eller uautorisert tilgang.</li> </ul>
<input checked="" type="checkbox"/>	<p><i>Andre personopplysninger:</i></p> <ul style="list-style-type: none"> <li>• navn,</li> <li>• stilling, rolle, organisasjonstilhørighet og avdeling,</li> <li>• arbeidsadresse og kontaktinformasjon,</li> <li>• brukernavn, e-postadresse, telefonnummer og annen identitetsinformasjon,</li> <li>• bruker-ID, objekt-ID, gruppe- og rolletilhørighet,</li> <li>• tilgangsrettigheter, autorisasjoner og privilegerte tilganger,</li> <li>• enhetsinformasjon, herunder PC, mobil, nettbrett, operativsystem, serienummer, compliance-status og administrasjonsstatus,</li> <li>• IP-adresser, MAC-adresser, nettverksinformasjon og lokasjonsrelaterte tekniske data,</li> <li>• logger, hendelseslogger, revisjonslogger, autentiseringslogger, sikkerhetslogger og administrasjonslogger,</li> <li>• metadata fra M365, Entra ID, Intune, saksverktøy, driftsverktøy, sikkerhetsverktøy og backupverktøy,</li> <li>• opplysninger i supportsaker, herunder beskrivelser av feil, skjermbilder, vedlegg og kommunikasjon med bruker,</li> </ul>

	<ul style="list-style-type: none"><li>• opplysninger som fremgår av e-post, filer, dokumenter, samhandlingsløsninger, arkiv-/fagsystemer, backup eller logger dersom Databehandler får tilgang som ledd i drift, support, sikkerhetshendelse eller gjenoppretting.</li></ul>
--	--

#### A.4 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

- ansatte hos Behandlingsansvarlig,
- innleide konsulenter og andre brukere som utfører arbeid for Behandlingsansvarlig,
- tidligere ansatte og tidligere brukere der opplysninger inngår i logger, arkiv, backup eller historikk,
- kontaktpersoner hos leverandører, samarbeidspartnere, offentlige myndigheter og andre tredjeparter,
- eksterne brukere av Behandlingsansvarliges digitale tjenester,
- avsendere og mottakere av e-post og annen kommunikasjon med Behandlingsansvarlig,
- personer som omtales i dokumenter, arkivdata, fagsystemer, logger, supporthenvendelser eller sikkerhetshendelser som omfattes av driftstjenesten.

#### 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):

<input checked="" type="checkbox"/>	Behandlingen varer så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig i henhold til Hovedavtalen. Databehandleravtalen gjelder også etter Hovedavtalens opphør for personopplysninger som fortsatt finnes hos Databehandler eller eventuelle Underdatabehandlere, frem til opplysningene er tilbakelevert, slettet eller gjort utilgjengelige i samsvar med Databehandleravtalen og Bilag C.
<input type="checkbox"/>	Behandlingen er tidsbegrenset, og gjelder frem til <i>&lt;angi dato eller kriterium for avslutning, eksempelvis avslutningen av et prosjekt. Merk at behandlingen normalt ikke kan avslutte før Hovedavtalen utløper&gt;</i> .

Ved opphør (av avtalen eller en behandling) skal personopplysninger tilbakeleveres og slettes i samsvar med Databehandleravtalen punkt 12 og instruksjonene i Bilag C. databehandlerens bruk av underdatabehandlere

## B. BETINGELSER FOR DATABEHANDLERENS BRUK OG ENDRING AV EVENTUELLE UNDERDATABEHANDLERE

B.1 Behandlingsansvarliges godkjenning av bruk av Underdatabehandlere

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

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

<input type="checkbox"/>	Databehandleren kan benytte Underdatabehandler som i samme konsern (mor-søster- eller datterselskap) som er etablert i et land innenfor EØS-området. Databehandleren skal på forhånd informere Behandlingsansvarlige om bruken av slik Underdatabehandler. (Dette alternativet kan kombineres med et av de andre alternativene.)
<input type="checkbox"/>	Databehandler kan gjennomføre endringer i bruken av Underdatabehandlere forutsatt at den Behandlingsansvarlige underrettes og gis mulighet til å motsette seg endringene. En slik underretning skal være mottatt av Behandlingsansvarlig senest 1 måned før endringen trer i kraft, med mindre annet er avtalt skriftlig mellom partene. Merk at endringer som medfører overføring av personopplysninger til land utenfor EØS-området (Tredjestater) uansett krever skriftlig godkjenning etter Databehandleravtalens punkt 10.  Hvis Behandlingsansvarlig motsetter seg endringen skal Databehandler underrettes så snart som mulig. Den behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn.
<input checked="" type="checkbox"/>	Databehandler kan ikke ta i bruk nye Underdatabehandlere eller endre Underdatabehandlerens behandlingssted, behandlingsformål eller rolle i leveransen uten Behandlingsansvarliges spesifikke og forutgående skriftlige godkjenning.  Forespørsel om godkjenning av ny eller endret Underdatabehandler skal sendes skriftlig til Behandlingsansvarlig senest 60 kalenderdager før endringen planlegges iverksatt, med mindre endringen skyldes forhold Databehandler ikke med rimelighet kunne forutse.  Forespørselen skal som minimum inneholde: <ul style="list-style-type: none"><li>• navn, organisasjonsnummer og adresse for Underdatabehandler,</li><li>• beskrivelse av behandlingen Underdatabehandler skal utføre,</li><li>• kategorier av personopplysninger og registrerte som berøres,</li><li>• behandlingssted og eventuell tilgang fra andre land,</li><li>• sikkerhetstiltak og kontrollmekanismer,</li><li>• om det skjer overføring til tredjeland eller internasjonal organisasjon,</li><li>• konsekvenser for sikkerhet, personvern, revisjon, datauttrekk, sletting og exit,</li><li>• kopi eller sammendrag av relevante databehandlerforpliktelser der dette kan kreves.</li></ul>

## Bilag A, B, C, og D til Databehandleravtalen

	<p>Behandlingsansvarlig kan nekte godkjenning dersom det foreligger saklig grunn, herunder dersom endringen kan svekke informasjonsikkerhet, personvern, revisjonsmulighet, etterlevelse, behandlingssted, datakontroll eller Kundens mulighet til å oppfylle egne plikter etter personvernregelverket.</p> <p>For standardiserte tredjepartstjenester som Behandlingsansvarlig uttrykkelig har akseptert etter Hovedavtalen og hvor tredjepartens standard databehandleravtale gjelder direkte mellom Behandlingsansvarlig og tredjeparten, skal Databehandler beskrive forholdet i Bilag 2, Bilag 10 og dette Bilag B. Databehandler skal bistå Behandlingsansvarlig med oppfølgingen av slike tredjepartstjenester innenfor avtalens omfang.</p>
--	---

<Merknad: Hvis Databehandler benytter underleverandør (tredjepart) som leverer standardiserte tredjepartstjenester (typisk skytjenester), og som oppfylder vilkårene i Databehandleravtalen punkt 9.7, slik at tredjepartens standard databehandleravtale kommer til anvendelse direkte overfor den behandlingsansvarlige, vil skifte av underleverandør hos tredjeparten følge bestemmelsene i tredjepartens databehandleravtale.>

B.2 Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere (fylles ut av tilbyder):

<b>Navn</b>	<b>Org.nr.</b>	<b>Adresse</b>	<b>Beskrivelse av behandling</b>	<b>Behandlingssted</b>	<b>Kontaktinformasjon</b>	<b>Særlige kategorier personopplysninger</b>
<i>[Navn]</i>	<i>[Org.nr.]</i>	<i>[Adresse]</i>	<i>[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]</i>	<i>[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]</i>	<i>[Kontaktinformasjon]</i>	<i>[Angi om det behandles særlige kategorier av personopplysninger]</i>
<i>[Navn]</i>	<i>[Org.nr.]</i>	<i>[Adresse]</i>	<i>[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]</i>	<i>[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]</i>	<i>[Kontaktinformasjon]</i>	
<i>[Navn]</i>	<i>[Org.nr.]</i>	<i>[Adresse]</i>	<i>[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]</i>	<i>[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]</i>	<i>[Kontaktinformasjon]</i>	
<i>[Navn]</i>	<i>[Org.nr.]</i>	<i>[Adresse]</i>	<i>[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]</i>	<i>[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]</i>	<i>[Kontaktinformasjon]</i>	

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

## C. INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

### C.1 Behandlingens omfang og formål

Personopplysninger skal utelukkende behandles i det omfang og for de formål som følger av:

- Hovedavtalen,
- Databehandleravtalen,
- Bilag A–D til Databehandleravtalen,
- dokumenterte instruksjoner fra Behandlingsansvarlig.

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Hovedavtalen og Databehandleravtalen.

Databehandler skal ikke behandle personopplysninger til egne formål, herunder analyse, statistikk, produktutvikling, modelltrening, finjustering av KI-modeller, forbedring av tjenester for andre kunder eller kommersiell utnyttelse, uten Behandlingsansvarliges uttrykkelige skriftlige forhåndsgodkjenning.

Dette gjelder også metadata, logger, sikkerhetsdata, supportsaker, bruksmønstre, dokumentasjon og aggregerte eller anonymiserte data dersom slike data stammer fra Kundens bruk av driftstjenesten.

### 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:

Databehandler skal levere virksomhetskritiske IT-driftstjenester for en offentlig virksomhet. Behandlingen omfatter blant annet identitets- og tilgangsdata, logger, sikkerhetsdata, driftsdata, enhetsdata, supportsaker, backup og opplysninger i Kundens IT-miljø. Databehandler vil kunne ha administrativ eller teknisk tilgang til systemer, tjenester, logger, backup og informasjon som kan ha høy beskyttelsesverdi. Behandlingen kan også omfatte opplysninger med særlig behov for beskyttelse og særlige kategorier av personopplysninger dersom slike opplysninger inngår i Kundens data, supportsaker, arkiv, fagsystemer eller backup.

## Bilag A, B, C, og D til Databehandleravtalen

- 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):

<input checked="" type="checkbox"/>	<p>Sikkerhetskrav som beskrevet i Hovedavtalen: Databehandler skal ha et egnet styringssystem for informasjonssikkerhet og skal etablere, dokumentere og vedlikeholde tekniske og organisatoriske tiltak som er tilpasset behandlingens risiko.</p> <p>Sikkerhetskravene følger av Hovedavtalen, herunder særlig:</p> <ul style="list-style-type: none"><li>• Bilag 1 Kundens behovsbeskrivelse og kravspesifikasjon,</li><li>• Bilag 1.1 Kravtabeller og leverandørens besvarelse,</li><li>• Bilag 2 Leverandørens løsningsspesifikasjon,</li><li>• Bilag 5 Tjenestenivå og standardiserte kompensasjoner,</li><li>• Bilag 6 Administrative bestemmelser,</li><li>• Bilag 7 Samlet pris og prisbestemmelser,</li><li>• Bilag 11 Databehandleravtale.</li></ul> <p>Databehandler skal som minimum ivareta:</p> <ul style="list-style-type: none"><li>• tilgangsstyring basert på tjenstlig behov og minste privilegiums prinsipp,</li><li>• sterk autentisering for administrative tilganger,</li><li>• kontroll med privilegerte tilganger,</li><li>• logging og sporbarhet for administrativ tilgang og behandling av personopplysninger,</li><li>• sikker fjernadministrasjon,</li><li>• kryptering der dette er relevant for lagring, overføring, backup og administrasjon,</li><li>• segmentering og atskillelse mellom kunder og miljøer,</li></ul>
-------------------------------------	---

	<ul style="list-style-type: none"><li>• sårbarhetsstyring og sikkerhetsoppdatering,</li><li>• sikkerhetskopiering, gjenoppretting og robusthet,</li><li>• beskyttelse mot skadevare, ransomware, kontokompromittering og uautorisert tilgang,</li><li>• hendelseshåndtering og varsling,</li><li>• regelmessig testing, vurdering og evaluering av sikkerhetstiltak,</li><li>• kontroll med underdatabehandlere,</li><li>• sikker sletting, tilbakelevering og utilgjengeliggjøring ved opphør,</li><li>• menneskelig kontroll med KI- og automasjonsfunksjoner som behandler personopplysninger.</li></ul> <p>Databehandler skal kunne dokumentere sikkerhetstiltakene på forespørsel.</p>
<input type="checkbox"/>	Sikkerhetskrav som beskrevet nedenfor: <Sett inn beskrivelse av relevante sikkerhetskrav>

### C.3 Dokumentasjon

Databehandler skal dokumentere rutiner, kontroller og tiltak som er iverksatt for å oppfylle kravene i gjeldende personvernregler og Databehandleravtalen.

Dokumentasjonen skal holdes oppdatert og gjøres tilgjengelig for Behandlingsansvarlig eller tilsynsmyndighet på forespørsel.

Dokumentasjonen skal blant annet kunne omfatte:

- styringssystem for informasjonssikkerhet,
- risikovurderinger,
- tilgangsstyring og tilgangsrevisjoner,
- oversikt over behandlingsaktiviteter,
- oversikt over underdatabehandlere,
- behandlingssteder og tilgangssteder,
- sikkerhetstiltak,
- hendelses- og avvikshåndtering,
- revisjonsrapporter, sertifiseringer eller kontrollrapporter,
- slette- og tilbakeleveringsrutiner,
- dokumentasjon av KI-/automasjonsfunksjoner som behandler personopplysninger.

### C.4 Overføring av personopplysninger - Lokasjon for behandling og tilgang

Behandling av personopplysninger som omfattes av avtalen kan ikke uten Behandlingsansvarliges forutgående skriftlige godkjenning utføres på eller med tilgang fra andre lokasjoner enn de som er angitt i Bilag B.2.

Med lokasjon menes:

## Bilag A, B, C, og D til Databehandleravtalen

- sted hvor personopplysninger lagres,
- sted hvor personopplysninger bearbejdes eller prosesseres,
- sted hvor personopplysninger kan aksesseres fra, herunder ved fjernadministrasjon, support, drift, sikkerhetsovervåking eller underleverandørtilgang.

Personopplysninger skal som utgangspunkt behandles innenfor Norge/EØS. Overføring til tredjeland eller internasjonal organisasjon kan bare skje dersom Behandlingsansvarlig har godkjent dette skriftlig og vilkårene i Databehandleravtalen punkt 10 er oppfylt.

Databehandler skal på forespørsel kunne redegjøre for hvor personopplysninger, logger, metadata, backup og administrasjonsdata til enhver tid lagres, behandles eller er tilgjengelige fra.

### C.5 Rutiner for revisjon og tilsyn

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

<input type="checkbox"/>	<p>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.</p> <p>Slike revisjoner skal:</p> <ul style="list-style-type: none"><li>• Gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året, med mindre sikkerhetsbrudd hos Databehandler eller andre særlige forhold gir grunn for hyppigere revisjoner;</li><li>• Foregå innenfor normal arbeidstid og ikke forstyrre Databehandlers virksomhet unødvendig;</li><li>• Utføres av ansatte hos Behandlingsansvarlig eller av tredjepart som er godkjent av Partene og underlagt taushetsplikt.</li></ul> <p>Databehandler plikter å stille til rådighet de ressurser som med rimelighet kan kreves for å gjennomføre revisjonen.</p> <p>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.</p>
<input type="checkbox"/>	<p>Databehandleren skal benytte ekstern revisor til å attestere at sikkerhetstiltak er etablert og virker etter hensikten. Slik revisjon skal:</p> <ol style="list-style-type: none"><li>i. gjennomføres én gang årlig,</li></ol>

Bilag A, B, C, og D til Databehandleravtalen

	<p>ii. utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402.</p> <p>iii. utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring</p> <p>Rapportene skal fremlegges for Behandlingsansvarlig på forespørsel.</p> <p>Databehandler skal i tillegg gi slik informasjon og bistand som er nødvendig for at Behandlingsansvarlig kan etterleve sine forpliktelser etter Gjeldende personvernregelverk.</p>
<input type="checkbox"/>	<p>For standardiserte tredjepartstjenester som leveres av Underdatabehandler kan det fremlegges tredjepartsrevisjon forutsatt at revisjonen er gjennomført etter alminnelig anerkjente prinsipper og av sertifisert revisor.</p>
<input checked="" type="checkbox"/>	<p>Behandlingsansvarlig har rett til å gjennomføre revisjon for å kontrollere Databehandlers etterlevelse av Databehandleravtalen og gjeldende personvernregler.</p> <p>Ordinær revisjon kan gjennomføres én gang per kalenderår etter rimelig forhåndsvarsel, normalt minst 20 virkedager.</p> <p>Behandlingsansvarlig kan i tillegg gjennomføre eller kreve særskilt revisjon dersom:</p> <ul style="list-style-type: none"><li>• det foreligger brudd på personopplysningssikkerheten,</li><li>• det foreligger alvorlig eller gjentatt avvik,</li><li>• det skjer vesentlige endringer i behandlingen, behandlingssted, underdatabehandler eller sikkerhetstiltak,</li><li>• tilsynsmyndighet, departement eller annen offentlig myndighet krever dokumentasjon,</li><li>• revisjon er nødvendig for å oppfylle Behandlingsansvarliges plikter etter personvernregelverket.</li></ul> <p>Revisjon kan gjennomføres av Behandlingsansvarlig eller av tredjepart som Behandlingsansvarlig benytter, forutsatt at tredjeparten er underlagt taushetsplikt og ikke er direkte konkurrent av Databehandler.</p> <p>Databehandler skal stille til rådighet den dokumentasjon, informasjon og bistand som med rimelighet er nødvendig for revisjonen.</p> <p>Databehandler kan oppfylle deler av dokumentasjonsplikten ved å fremlegge relevante og oppdaterte tredjepartsrevisjoner, sertifiseringer eller attestasjonsrapporter, eksempelvis ISO 27001, ISAE 3402, ISAE 3000, SOC 2 eller tilsvarende, forutsatt at disse dekker den aktuelle behandlingen og sikkerhetstiltakene.</p> <p>For standardiserte tredjepartstjenester som leveres av Underdatabehandler, kan Databehandler fremlegge tredjepartsrevisjon eller tilsvarende dokumentasjon fra</p>

	den aktuelle tjenesteleverandøren, forutsatt at dokumentasjonen er relevant og tilstrekkelig for Behandlingsansvarliges kontrollbehov.
--	--

C.6 Sletting og tilbakelevering av personopplysninger ved avtalens opphør

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

<input type="checkbox"/>	Alle personopplysninger som behandles under denne Databehandleravtale skal slettes uten ugrunnet opphold og senest innen 90 kalenderdager etter opphør av Hovedavtalen. Dette samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig.
<input type="checkbox"/>	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>
<input checked="" type="checkbox"/>	Ved opphør av Hovedavtalen eller den relevante behandlingen skal personopplysninger som behandles på vegne av Behandlingsansvarlig tilbakeleveres i samsvar med Behandlingsansvarliges instruks.  Tilbakelevering skal skje i strukturert, alminnelig anvendt og maskinlesbart format, så langt dette er teknisk mulig og forholdsmessig. Format og fremgangsmåte skal beskrives i avslutningsplanen.  Etter at tilbakelevering er gjennomført og skriftlig bekreftet av Behandlingsansvarlig, skal Databehandler slette personopplysningene uten ugrunnet opphold og senest innen 30 kalenderdager, med mindre annet følger av lov eller skriftlig instruks fra Behandlingsansvarlig.  For sikkerhetskopier og backup der direkte sletting ikke er teknisk mulig uten å påvirke backupens integritet, skal personopplysningene gjøres utilgjengelige og slettes eller overskrives etter ordinær backupsyklus. Databehandler skal dokumentere forventet tidspunkt for slik sletting eller overskriving.

	Databehandler skal skriftlig bekrefte at tilbakelevering, sletting eller utilgjengeliggjøring er gjennomført, og skal på forespørsel dokumentere hvordan dette er gjort.
--	--

C.7 Sektorspesifikke bestemmelser om behandling av personopplysninger

I den grad de kommer til anvendelse for behandlingen under Hovedavtalen, skal Databehandler ivareta relevante krav som følger av:

- personopplysningsloven og personvernforordningen,
- forvaltningsloven, herunder regler om taushetsplikt,
- offentleglova,
- arkivlova med forskrifter,
- sikkerhetsloven med forskrifter dersom behandlingen eller leveransen omfattes av slike krav,
- andre lov- og forskriftskrav som gjelder for Behandlingsansvarliges virksomhet og som er gjort kjent for Databehandler.

Databehandler skal varsle Behandlingsansvarlig dersom Databehandler blir kjent med forhold som kan påvirke Behandlingsansvarliges etterlevelse av slike krav.

C.8 Kontaktinformasjon

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

**Hos Behandlingsansvarlig**

Sikkerhetsbrudd:

Telefon: *[Fyll ut]*

E-post *[Fyll ut]*

Andre henvendelser:

Navn: *[Fyll ut]*

Stilling: *[Fyll ut]*

Telefon: *[Fyll ut]*

E-post: *[Fyll ut]*

**Hos Leverandøren**

Sikkerhetsbrudd:

Telefon: *[Fyll ut]*

E-post *[Fyll ut]*

Andre henvendelser:

Navn: *[Fyll ut]*

Stilling: *[Fyll ut]*

Telefon: *[Fyll ut]*

E-post: *[Fyll ut]*

## D. ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER ETTER AVTALEINNGÅELEN

Det er ikke avtalt endringer i Databehandleravtalens generelle avtaletekst ved avtaleinngåelsen.

Utfyllende instruksjoner, sikkerhetskrav, revisjonsrutiner, behandlingssteder, kontaktpunkter, underdatabehandlere og slette-/tilbakeleveringsrutiner fremgår av Bilag A, B og C.

Punkt i Databehandleravtalens standardtekst	Endring
Ingen	Det er ikke avtalt endringer i standardteksten.