

Bilag A, B, C, og D til Databehandleravtalen

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

A. OPPLYSNINGER OM BEHANDLINGEN

A.1 Hovedavtalen og formålet med behandlingen av personopplysninger

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige 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.>

Kommentert [A1]: Skriv inn navn og for anskaffelsen og kontrakten benyttet.

<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 den behandlingsansvarliges instruksjer, 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 (om SSA benyttes)
- Levering av skylagringstjenester som nærmere beskrevet i Hovedavtalens Bilag 1 (om SSA benyttes)
- Bruk av system X til innsamling og behandling av opplysninger om Behandlingsansvarliges ansatte>

Kommentert [A2]: Formålet skal være reelt, og det må være klart uttrykt og bestemt før behandlingen starter. For mer informasjon, se: [Fastsette formål](#) | [Datatilsynet](#)

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

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige 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>

Kommentert [A3]: Her skal databehandlers behandling fremgå.

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.>
☐	Andre personopplysninger: <Angi type, f.eks. navn og kontaktinformasjon, utdanning, kommunikasjonspreferanser osv.>

Kommentert [A4]: Velg en eller flere kategorier.

Merk at dersom det skal behandles særlige kategorier må det gjennomføres en DPIA (en vurdering av personvernkonsekvensene). DSS har et utkast til en pre-DPIA som kan sendes ut til leverandørene i forbindelse med tilbudsinnleveringen.

Se også [Veiledning om DPIA | Datatilsynet](#)

A.4 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

<Beskriv hvem behandlingen av personopplysninger omfatter, for eksempel: «Innbyggere i Oslo Kommune», «Brukere av skolefritidsordningen» eller «Ansatte og konsulenter i DFØ».

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

Kommentert [A5]: En registrert er personen hvis personopplysninger behandles.

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 avslutte før Hovedavtalen utløper>.

Kommentert [A6]: I de fleste tilfeller for departementet, vil det første alternativet være riktig.

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

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:

☐	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.)
☐	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.
☐	Databehandler kan kun gjennomføre endringer i bruken av Underdatabehandlere etter spesifikk og forutgående skriftlig godkjenning fra Behandlingsansvarlig. Underdatabehandleren kan ikke behandle personopplysninger under Hovedavtalen før slik godkjenning er gitt. Godkjenning 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 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.>

Kommentert [A7]: Alternativ 1 kan benyttes i kombinasjon med alternativ 2 og 3.

Alternativ 2 sier at Databehandler kan benytte underdatabehandlere uten skriftlig godkjenning fra Behandlingsansvarlig, men det må informeres om det senest 1 måned før endringen trer i kraft og Behandlingsansvarlig kan motsette seg det.

Alternativ 3 sier at Databehandler kun kan benytte underdatabehandlere ved Behandlingsansvarliges skriftlige samtykke.

Alternativ 3 er strengere enn alternativ 2.

Kommentert [A8]: Vær oppmerksom på dette.

Bilag A, B, C, og D til Databehandleravtalen

B.2 Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere:

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

Kommentert [A9]: Dette skal fylles inn av Databehandler. Behandlingsansvarlig bør alltid ha en oppdatert versjon av denne tabellen tilgjengelig.

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

Personopplysningene skal utelukkende 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>

Kommentert [A10]: I henhold til GDPR art. 32 skal Behandlingsansvarlig og Databehandler gjennomføre egnede tekniske og organisatoriske tiltak som sikrer et sikkerhetsnivå i behandlingen av personopplysninger i samsvar med risikoen.

Implisitt i art. 32 er Behandlingsansvarlig dermed pålagt å gjennomføre risikovurderinger for alle sine behandlinger.

Dersom behandlingen medfører høy risiko for den registrerte, skal det gjennomføres en DPIA, jf. Art. 35.

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>

- 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.

Kommentert [A11]: Eksempler på sikkerhetstiltak som kan fylles inn i tabellen over. Listen er på ingen måte uttømmende.

Husk å slett listen når du har kopiert inn de tiltakene du ønsker å benytte.

Bilag A, B, C, og D til Databehandleravtalen

C.3 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.4 Overføring av personopplysninger - Lokasjon for behandling og tilgang

Behandling av de personopplysninger som avtalen omfatter kan ikke uten den Behandlingsansvarliges forutgående skriftlige godkjenning 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 den Behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles.

C.5 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;
--------------------------	--

Bilag A, B, C, og D til Databehandleravtalen

	• 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: i. gjennomføres én gang årlig, ii. utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402. iii. utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring Rapportene skal 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 Underdatabehandler 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 Underdatabehandlere>

Kommentert [A12]: Velg ett eller flere alternativ.

Alternativ 1 er det "snilleste", mens alternativ 2 er litt strengere. Alternativ 3 bør benyttes i kombinasjon med andre alternativ.

C.6 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. Dette samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig.
-------------------------------------	---

Bilag A, B, C, og D til Databehandleravtalen

☐	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.7 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.>

Kommentert [A13]: Dette kan være supplerende bestemmelser om personvern i lov eller forskrift som er gjeldende for behandlingen.

C.8 Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningsikkerheten 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]

Bilag A, B, C, og D til Databehandleravtalen

D. ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER
ETTER AVTALEINNGÅElsen

Kommentert [A14]: Dersom man skal endre den generelle avtaleteksten, skal dette gjøres her.