

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 AVTALEINNGÅESEN

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	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 Underdatabehandlere	7	
B.1	Behandlingsansvarliges godkjenning av bruk av Underdatabehandlere	7	
B.2	Godkjente Underdatabehandlere	8	
C.	Instruks vedrørende behandling av personopplysninger	9	
C.1	Behandlingens omfang og formål	9	
C.2	Sikkerhet ved behandlingen	9	
C.2.1	Angivelse av sikkerhetsnivå	9	
C.2.2	Styringssystem for informasjonssikkerhet	9	
C.3	Dokumentasjon	10	
C.4	Overføring av personopplysninger - Lokasjon for behandling og tilgang	10	
C.5	Rutiner for revisjon og tilsyn	10	
C.6	Sletting og tilbakelevering av personopplysninger ved avtalens opphør	11	
C.7	Sektorspesifikke bestemmelser om behandling av personopplysninger	12	
C.8	Kontaktinformasjon	13	
D.	Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen	14	

A. OPPLYSNINGER OM BEHANDLINGEN

A.1 Hovedavtalen og formålet med behandlingen av personopplysninger og annen taushetsbelagt informasjon (Opplysninger)

Databehandlerens behandling av opplysninger på vegne av den Behandlingsansvarlige er knyttet til å levere tjenester som beskrevet i Hovedavtalen.

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

«Utvikling og forvaltning av digitale tjenester i Oslo kommune»

Behandlingen har følgende formål:

Sikre at personopplysninger om de registrerte eller annen taushetsbelagt informasjon (opplysninger), ikke brukes urettmessig eller kommer uberettigede i hende.

Beskrivelse av behandlingsformål:

Drift, vedlikehold og videreutvikling av kommunens utviklingsplattformer og tjenesteportefølje, deriblant utvikling av nye tjenester. Tjenesteporteføljen består hovedsakelig av mikrotjenester ("komponenter"), herunder systemintegrasjoner og webapplikasjoner.

A.2 Databehandlerens behandling av personopplysninger og annen taushetsbelagt informasjon på vegne av den Behandlingsansvarlige

Databehandlerens behandling av opplysninger på vegne av den Behandlingsansvarlige omhandler (karakteren av behandlingen):

- Tilgang til produksjonsmiljøene med produksjonsdata på meldingskøer, i feillogger, i databaser, offentlige register og på lagringsområder. Innsamling, registrering, sletting, sammenstilling og lagring skal kun skje på kommunens utviklingsplattformer eller utstyr kommunen har godkjent.
- Tilgang til kildekode, dokumentasjon (inkludert sikkerhetsdokumentasjon), test-miljøer og testdata under utviklings- og testfaser.

Bilag A, B, C, og D til Databehandleravtalen

- Eventuell utlevering og annen transport av opplysninger etter godkjenning fra kommunen.

A.3 **Typer av personopplysninger og annen informasjon underlagt taushetsplikt**

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

☒	<i>Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1). F.eks. helseopplysninger, rasemessig eller etnisk opprinnelse og fagforeningstilhørighet.</i>
☒	<i>Andre opplysninger med særlig behov for beskyttelse: For eksempel dybdeopplysninger om person, om ansatte, personnummer eller andre identifikatorer om kan knyttes direkte til fysisk person.</i>
☒	<i>Andre personopplysninger: F. eks. navn og kontaktinformasjon, utdanning, kommunikasjonspreferanser osv.</i>

Behandlingen omfatter følgende typer av informasjon underlagt taushetsplikt:

☒	<i>Lovbestemt taushetsplikt</i>
☒	<i>Informasjon unntatt offentlighet – Offentleglova kap.3</i>
☒	<i>Avtalefestet taushetsplikt</i>

Bilag A, B, C, og D til Databehandleravtalen

☒	<i>Intern informasjon uten restriksjon/uten innsynsrett</i>
☒	<i>Informasjon som skal lagres i nærmere angitte land (regnskapsmaterieell)</i>
☒	<i>Informasjon som skal lagres i Norge (arkivmateriale)</i>
☒	<i>Annen informasjon av betydning for informasjonssikkerheten, f.eks. teknisk informasjon som muliggjør tilgang til skjermet informasjon</i>

A.4 Kategorier av registrerte:

Behandlingen omfatter følgende kategorier av registrerte:

- Ansatte, herunder ansatte med spesielle beskyttelsesbehov.
- Innbyggere i Oslo kommune, herunder særlig sårbare eller utsatte gruppe som f.eks. barn eller handikappede.
- Leverandører
- Samarbeidspartnere

A.5 Varighet av behandlingen

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

Bilag A, B, C, og D til Databehandleravtalen

☒	Behandlingen er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen og tilhørende avropsavtaler.
☐	Behandlingen er tidsbegrenset, og gjelder frem til <i><angi dato eller kriterium for avslutning, eksempelvis avslutningen av et prosjekt. Merk at behandlingen normalt ikke kan avslutte før Hovedavtalen utløper></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:

☐	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

Bilag A, B, C, og D til Databehandleravtalen

	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.

B.2 Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere:

Navn	Org.nr.	Beskrivelse av behandling	Behandlingssted	Kontaktinformasjon	Særlige kategorier personopplysninger

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 OPPLYSNINGER

C.1 Behandlingens omfang og formål

opplysningene skal utelukkende behandles i det omfang og for de formål som er beskrevet i

- Hovedavtalen
- Databehandleravtalen med bilag

Databehandler har ikke råderett over opplysningene 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 opplysninger 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:

Behandlingen omfatter blant annet store mengder av «særlige kategorier av personopplysninger» i henhold til GDPR artikkel 9 (1) som krever særlig beskyttelse.

☐ Ikke krever et høyt sikkerhetsnivå. Begrunnelse:

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 opplysningene, herunder (flere valg mulig):

☐	Sikkerhetskrav som beskrevet i Hovedavtalen:
--------------------------	--

☒	Sikkerhetskrav som beskrevet nedenfor: Styringssystemet eller kvalitetssystemet til leverandøren skal dekke prosesser for personellsikkerhet og håndtering av sikkerhetsavvik. Under personellsikkerhet inngår inngåelse av taushetserklæringer med den enkelte konsulent. Innleide konsulenter skal i det operative forholde seg til kommunens rutiner og prosesser som beskrevet i kommunens styringssystem.

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 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 (prosesserer)
- 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; • 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.

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.
☒	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. Dette gjelder primært konsulentenes arbeidsstasjoner som har vært under kommunens administrasjon. Tilbakelevering er ikke relevant for denne avtalen. Meddelelse om sletting og destruksjon skal sendes til: kjersti.myhra@uke.oslo.kommune.no merket «Meddelelse om sletting av data, saksnummer 22/232. Ved opphør av avtalen plikter Leverandøren å avvikle alle tilganger til Kundens data.
☐	<Sett inn eventuelle andre avtalte rutiner for sletting eller tilbakelevering>

C.7 Sektorspesifikke bestemmelser om behandling av personopplysninger

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: 468 44 285

kjersti.myhra@uke.oslo.kommune.no

Andre henvendelser:

Navn: *Kjersti Myhra*

Stilling: Rådgiver avtaleforvaltning

Telefon: 468 44 285

kjersti.myhra@uke.oslo.kommune.no

Hos Leverandøren

Sikkerhetsbrudd:

Telefon: 900 39 317

E-post: bjarne.brokke@visma.com

Andre henvendelser:

Navn: *Bjarne Brokke*

Stilling: CSO

Telefon: 900 39 317

E-post: bjarne.brokke@visma.com

D. ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER ETTER AVTALEINNGÅELEN

D.1 Endringer til Databehandleravtalens standardtekst

D.1.1 *Avtalens henvisning til personopplysninger*

Databehandleravtalens begrep «personopplysninger» er i standardteksten endret til «Opplysninger», ref. endringen som det er redegjort for i dette bilagets pkt. D.1.2 under. Merk: denne endringen er gjennomført gjennomgående i standardteksten.

D.1.2 *Avtalens pkt. 1.1 får to nye avsnitt mellom eksisterende avsnitt 1 og 2:*

Nytt avsnitt lyder:

Videre regulerer Databehandleravtalen partenes rettigheter og plikter i forhold til behandling av data og informasjon som er underlagt taushetsplikt i medhold av annen lov eller avtale.

Ovennevnte typer informasjon vil i det følgende bli benevnt som «Opplysninger», med mindre aktuelt avtalepunkt bare berører enkelte av informasjonstypene.

For annen taushetsbelagt informasjon enn personopplysninger, plikter Databehandler å sikre at behandling skjer i henhold til de retningslinjene i lovgrunnlaget og eventuell avtale, som gjelder for behandling av sensitive personopplysninger (så langt disse passer).

D.1.3 *Avtalen får et nytt pkt. 11 B mellom eksisterende pkt. 11 og 12*

Forholdet mellom Databehandleravtalen og det enkelte avrop under rammeavtalen

Kravene til Databehandler i forhold til informasjonssikkerhet, dokumentasjon, risikovurderinger og revisjoner, gjelder så langt Databehandler har kontroll over aktuelt personell, tekniske løsninger, dokumentasjon m.m. I den grad det er Behandlingsansvarlig som instruerer aktuelt personell eller har kontroll over tekniske løsninger m.m. har behandlingsansvarlige selv ansvaret.