BILAG TIL DATABEHANDLARAVTALEN

DETTE DOKUMENTET BESTÅR AV FØLGJANDE BILAG:

BILAG A – OPPLYSNINGAR OM BEHANDLINGA

BILAG B - VILKÅR FOR DATABEHANDLAREN SIN BRUK AV UNDERDATABEHANDLARAR

BILAG C - INSTRUKS FOR BEHANDLING AV PERSONOPPLYSNINGAR

BILAG D - ENDRINGAR TIL STANDARDTEKSTEN I DATABEHANDLARAVTALEN OG ENDRINGAR ETTER AVTALEINNGÅINGA

A. Opplysningar om behandlinga 3
A.1 Hovudavtalen og føremålet med behandlinga av personopplysningar 3
A.2 Behandling av personopplysningar som Databehandlaren gjer på vegner av den Behandlingsansvarlege 3
A.3 Typar av personopplysningar 4
A.4 Kategoriar av registrerte 4
A.5 Kor lenge varer behandlinga 4
B. Vilkår for Databehandlaren sin bruk og endring av eventuelle Underdatabehandlarar 5
B.1 Godkjenning frå Behandlingsansvarleg for bruk av Underdatabehandlarar 5
B.2 Godkjende Underdatabehandlarar 6
C. Instruks for behandling av personopplysningar 7
C.1 Omfang og føremålet med behandlinga 7
C.2 Tryggleik ved behandlinga 7
C.2.1 Definering av tryggleiksnivå 7
C.2.2 Styringssystem for informasjonstryggleik 8
C.3 Dokumentasjon 8
C.4 Overføring av personopplysningar - Lokasjon for behandling og tilgang 8
C.5 Rutinar for revisjon og tilsyn 8
C.6 Sletting og tilbakelevering av personopplysningar ved opphøyr av avtalen 10
C.7 Sektorspesifikke føresegner om behandling av personopplysningar 10
C.8 Kontaktinformasjon 11
D. Endringar til standardteksten i Databehandlaravtalen og endringar etter avtaleinngåinga 12

A. OPPLYSNINGAR OM BEHANDLINGA

A.1 Hovudavtalen og føremålet med behandlinga av personopplysningar

Behandling av personopplysningar som Databehandlaren gjer på vegner av den Behandlingsansvarlege, er knytt til å levere tenester som skildra i Hovudavtalen.

Med Hovudavtalen meiner vi følgjande avtale/avtalar inngått mellom partane:

<Set inn namn og dato for inngåing av den eller dei underliggjande tenesteavtalen(-ane) som Databehandlaravtalen er knytt til.>

<Merknad: Dersom det er fleire tenesteavtalar som nyttar same databehandlaravtale, kan dei listast opp samla her eller det kan utarbeidast eit bilagssett for kvar avtale, avhengig av om art og omfang av behandlinga, og graden av kor einsarta dei er på instruksane frå den behandlingsansvarlege, er slik at det tener føremålet best at dei blir omtalt samla eller kvar for seg.>

Behandlinga har følgjande føremål:

<Skildre *behandlingsføremål, til dømes:*

- *Analyse av brukartilfredsheit i prosjekt X, som nærare skildra i Bilag 1 i Hovudavtalen (om SSA blir brukt)*
- *Levering av skylagringstenester som nærare skildra i Bilag 1 i Hovudavtalen (om SSA blir brukt)*
- *Bruk av system X til innsamling og behandling av opplysningar om tilsette hos den Behandlingsansvarlege>*

A.2 Behandling av personopplysningar som Databehandlaren gjer på vegner av den Behandlingsansvarlege

Behandling av personopplysningar som Databehandlaren gjer på vegner av den Behandlingsansvarlege omhandlar (karakteren av behandlinga):

<Skildre kva behandlinga omfattar, til dømes:

- *Innsamling, lagring og analyse av brukartilfredsheitsundersøkingar som skildra i Bilag 1 i Hovudavtalen*
- *Registrering, organisering og oppbevaring av personopplysningar i system X>*

A.3 Typar av personopplysningar

Behandlinga omfattar følgjande typar av personopplysningar om dei registrerte (fleire val moglege):

☒	*Særlege kategoriar av personopplysningar i samsvar med personvernforordninga artikkel 9 (1):* *<Før opp type, t.d. helseopplysningar, rasemessig eller etnisk opphav eller fagforeiningstilhøyrsle>*
☒	*Andre opplysningar med særleg behov for vern:* *<Før opp type, t.d. fødselsnummer, opplysningar om økonomi, prestasjonsvurderingar i tilsetjingstilhøve osv.>*
☐	*Andre personopplysningar:* *<Før opp type, t.d. namn og kontaktinformasjon, utdanning, kommunikasjonspreferansar osv.>*

A.4 Kategoriar av registrerte

Behandlinga omfattar følgjande kategoriar av registrerte:

<Skildre kven behandlinga av personopplysningar omfattar, *til dømes:* *«Innbyggjarar i Oslo Kommune», «Brukarar av skulefritidsordninga»* eller *«Tilsette og konsulentar i DFØ».*

*Dersom ein behandlar opplysningar om ei særleg sårbar eller utsett gruppe som t.d. barn eller handikappa, bør det oppførast særskilt.***>**

A.5 Kor lenge varer behandlinga

Behandling av personopplysningar som Databehandlaren gjer under Hovudavtalen, kan starte opp når Databehandlaravtalen har teke til å gjelde. Behandlinga varer i denne tida (vel eitt alternativ):

☐	Behandlinga er ikkje tidsavgrensa, og varer fram til Hovudavtalen opphøyrer.
☐	Behandlinga er tidsavgrensa, og gjeld fram til *<før opp dato eller kriterium for avslutning, eksempelvis avslutninga av eit prosjekt. Merk at behandlinga normalt ikkje kan avslutte før Hovudavtalen går ut>*.

Ved opphøyr (av avtalen eller ei behandling) skal personopplysningar leverast tilbake og slettast i samsvar med Databehandlaravtalen punkt 12 og instruksjonane i Bilag C.

databehandlaren sin bruk av underdatabehandlarar

B. VILKÅR FOR DATABEHANDLAREN SIN BRUK OG ENDRING AV EVENTUELLE UNDERDATABEHANDLARAR

B.1 Godkjenning frå Behandlingsansvarleg for bruk av Underdatabehandlarar

Ved inngåing av Databehandlaravtalen godkjenner Behandlingsansvarleg bruk av dei Underdatabehandlarane som er oppførte i punkt B.2. Merk at også mor-, søster- og dotterselskap til Databehandlaren blir rekna som Underdatabehandlarar dersom dei bidreg til leveransen og behandlar personopplysningar.

For endringar i bruk av Underdatabehandlarar er det i tillegg avtalt følgjande:

☐	Databehandlaren kan bruke Underdatabehandlar som er i same konsern (mor-søster- eller dotterselskap) som er etablert i eit land innanfor EØS-området. Databehandlaren skal på førehand informere Behandlingsansvarlege om bruken av slik Underdatabehandlar. (Dette alternativet kan kombinerast med eit av dei andre alternativa.)
☐	Databehandlar kan gjennomføre endringar i bruken av Underdatabehandlarar føresett at den Behandlingsansvarlege blir informert og får høve til å motsetje seg endringane. Slik informasjon skal vere motteken av Behandlingsansvarleg seinast 1 månad før endringa tek til å gjelde, med mindre anna er avtalt skriftleg mellom partane. Merk at endringar som medfører overføring av personopplysningar til land utanfor EØS-området (Tredjestatar), uansett krev skriftleg godkjenning etter punkt 10 i Databehandlaravtalen. Dersom Behandlingsansvarleg motset seg endringa, skal Databehandlar informerast så snart som råd. Den behandlingsansvarlege kan ikkje motsetje seg endringa utan sakleg grunn.
☐	Databehandlar kan berre gjennomføre endringar i bruken av Underdatabehandlarar etter spesifikk og føregåande skriftleg godkjenning frå Behandlingsansvarleg. Underdatabehandlaren kan ikkje behandle personopplysningar under Hovudavtalen før slik godkjenning er gjeven. Godkjenning kan ikkje nektast utan sakleg grunn.

<Merknad: Dersom Databehandlar bruker underleverandør (tredjepart) som leverer standardiserte tredjepartstenester (typisk skytenester), og som oppfyller vilkåra i Databehandlaravtalen punkt 9.7, slik at tredjeparten sin standard databehandlaravtale skal gjelde direkte overfor den behandlingsansvarlege, vil skifte av underleverandør hos tredjeparten følgje vilkåra i tredjeparten sin databehandlaravtale.>

B.2 Godkjende Underdatabehandlarar

Den Behandlingsansvarlege har godkjent bruk av følgjande Underdatabehandlarar:

Namn	Org.nr.	Adresse	Skildring av behandling	Behandlingsstad	Kontaktinformasjon	Særlege kategoriar personopplysningar
[Namn]	*[Org.nr.]*	*[Adresse]*	*[Overordna skildring av behandlinga hos Underdatabehandlaren]*	*[Før opp land der opplysningane blir lagra, ein oppnår tilgang frå eller dei på annan måte blir behandla i]*	*[Kontaktinformasjon]*	*[Opplys om det blir behandla særlege kategoriar av personopplysningar]*
[Namn]	*[Org.nr.]*	*[Adresse]*	*[Overordna skildring av behandlinga hos Underdatabehandlaren]*	*[Før opp land der opplysningane blir lagra, ein oppnår tilgang frå eller dei på annan måte blir behandla i]*	*[Kontaktinformasjon]*	
[Namn]	*[Org.nr.]*	*[Adresse]*	*[Overordna skildring av behandlinga hos Underdatabehandlaren]*	*[Før opp land der opplysningane blir lagra, ein oppnår tilgang frå eller dei på annan måte blir behandla i]*	*[Kontaktinformasjon]*	
[Namn]	*[Org.nr.]*	*[Adresse]*	*[Overordna skildring av behandlinga hos Underdatabehandlaren]*	*[Før opp land der opplysningane blir lagra, ein oppnår tilgang frå eller dei på annan måte blir behandla i]*	*[Kontaktinformasjon]*	

Databehandlaren kan ikkje bruke den enkelte Underdatabehandlaren til ei anna behandling enn avtalt eller la ein annan Underdatabehandlar utføre den skildra behandlinga i andre tilfelle enn det som følgjer av Bilag B, punkt B.1 om skifte av Underdatabehandlar.

C. INSTRUKS FOR BEHANDLING AV PERSONOPPLYSNINGAR

C.1 Omfang og føremålet med behandlinga

Personopplysningane skal utelukkande behandlast i det omfanget og for dei føremåla som er skildra i

- Hovudavtalen
- Databehandlaravtalen med bilag

Databehandlar har ikkje råderett over personopplysningane utover det som er nødvendig for å oppfylle pliktene sine etter Databehandlaravtalen, og kan ikkje behandle desse til eigne føremål.

C.2 Tryggleik ved behandlinga

C.2.1 Definering av tryggleiksnivå

Ut frå ei vurdering av omfanget av personopplysningar som blir behandla, typen opplysningar og karakteren av behandlinga er det basert på ei konkret risikovurdering fastsett at behandlinga (vel eitt alternativ):

☒ Krev eit høgt tryggleiksnivå. Grunngjeving:

<Vis til risikovurderinga som er gjort og skriv grunngjeving>

<T.d. Behandlinga omfattar store mengder av «særlege kategoriar av personopplysningar» i samsvar med personvernforordninga artikkel 9 (1) som krev særleg vern>

☐ Ikkje krev eit høgt tryggleiksnivå. Grunngjeving:

<Vis til risikovurderinga som er gjort og skriv grunngjeving>

<T.d.: Behandlinga omfattar berre opplysningar som er ålment kjende som namn og adresse>

C.2.2 Styringssystem for informasjonstryggleik

Databehandlaren skal ha eit eigna styringssystem for informasjonstryggleik. Databehandlaren skal etablere og forvalte tilstrekkelege tryggingstiltak for å vareta informasjonstryggleiken for behandling av personopplysningane, medrekna (fleire val moglege):

☒	Tryggleikskrav som skildra i Hovudavtalen: *<set inn tilvising til konkret regulering i Hovudavtalen>*
☐	Tryggleikskrav som skildra nedanfor:

C.3 Dokumentasjon

Databehandlar skal dokumentere dei rutinane og tiltaka som er sette i verk for å oppfylle krava som går fram av Gjeldande personvernreglar og Databehandlaravtalen, medrekna krava til informasjonstryggleik. Slik dokumentasjon skal oppbevarast og haldast a jour så lenge Databehandlaravtalen består, og gjerast tilgjengeleg for Behandlingsansvarleg eller tilsynsorgan på førespurnad.

C.4 Overføring av personopplysningar - Lokasjon for behandling og tilgang

Behandling av dei personopplysningane som avtalen omfattar, kan ikkje utan føregåande skriftleg godkjenning frå den Behandlingsansvarlege utførast på eller med tilgang frå andre lokasjonar enn dei som er førte opp i Bilag B.2. Med lokasjon meiner vi:

- stad det er mogleg å få tilgang til personopplysningane frå (aksessering)
- stad der ein tilarbeider (prosesserer) personopplysningane
- stad der ein lagrar personopplysningane

Avgrensinga ovanfor gjeld ikkje Databehandlaren sine mor-, søster- og dotterselskap som er etablerte innanfor EØS-området. Databehandlaren skal likevel på førespurnad frå den Behandlingsansvarlege gjere greie for kvar personopplysningane til kvar tid blir behandla.

C.5 Rutinar for revisjon og tilsyn

For å kontrollere etterleving av Gjeldande personvernreglar og Databehandlaravtalen er det avtalt følgjande (fleire val moglege):

☒	Behandlingsansvarleg har rett til å utføre revisjon på forretningsstaden til Databehandlaren for å verifisere at Databehandlar etterlever pliktene sine i samsvar med denne Databehandlaravtalen eller Gjeldande personvernreglar. Slike revisjonar skal: • gjennomførast etter rimeleg førehandsvarsel og maksimalt éin gong i året, med mindre brot på tryggleiken hos Databehandlar eller andre særlege forhold gjev grunn for hyppigare revisjonar; • gå føre seg innanfor normal arbeidstid og ikkje forstyrre verksemda til Databehandlaren unødvendig; • utførast av tilsette hos Behandlingsansvarleg eller av tredjepart som er godkjend av Partane og underlagd teieplikt. Databehandlar pliktar å stille til rådvelde dei ressursane som det er rimeleg å krevje for å gjennomføre revisjonen. Behandlingsansvarleg skal dekkje kostnader for eventuelle tredjepartar som blir brukte til å gjennomføre revisjonen. Elles dekkjer Partane sine eigne kostnader ved gjennomføring av revisjonen. Dersom revisjonen avdekkjer vesentlege brot på forpliktingane etter Gjeldande personvernreglar eller Databehandlaravtalen, skal Databehandlar likevel dekkje dei rimelige kostnadene Behandlingsansvarleg har ved revisjonen.
☒	Databehandlaren skal nytte ekstern revisor til å attestere at tryggingstiltak er etablerte og verkar etter føremålet. Slik revisjon skal: i. gjennomførast éin gong årleg, ii. utførast i samsvar med anerkjende attestasjonsstandardar, til dømes ISAE 3402. iii. utførast av ein uavhengig tredjepart med tilstrekkeleg kunnskap og erfaring Rapportane skal leggjast fram for Behandlingsansvarleg på førespurnad. Databehandlar skal i tillegg gje slik informasjon og bistand som er nødvendig for at Behandlingsansvarleg kan etterleve forpliktingane sine etter Gjeldande personvernregelverk.
☒	For standardiserte tredjepartstenester som blir leverte av Underdatabehandlar, kan det leggjast fram tredjepartsrevisjon føresett at revisjonen er gjennomført etter alminneleg anerkjende prinsipp og av sertifisert revisor.
☐	*<Set inn eventuelle andre avtalte rutinar for revisjon, medrekna eventuelle særskilde eller avvikande rutinar for revisjon hos Underdatabehandlarar>*

C.6 Sletting og tilbakelevering av personopplysningar ved opphøyr av avtalen

Partane har avtalt følgjande om sletting/tilbakelevering av personopplysningar (vel eitt alternativ):

☐	Alle personopplysningar som blir behandla under denne Databehandlaravtalen, skal slettast utan ugrunna opphald og seinast innan 90 kalenderdagar etter opphøyr av Hovudavtalen. Det same gjeld eventuell annan relevant informasjon som blir forvalta på vegner av Behandlingsansvarleg.
☐	Alle personopplysningar som blir behandla under denne Databehandlaravtalen, og eventuell annan relevant informasjon som blir forvalta på vegner av Behandlingsansvarleg, skal leverast tilbake ved opphøyr av Hovudavtalen. Etter tilbakelevering er skjedd, pliktar Databehandlar å slette alle personopplysningar og annan relevant informasjon som blir forvalta på vegner av Behandlingsansvarleg innan 30 kalenderdagar. Tilbakelevering skal skje på følgjande måte: *<Før opp korleis og kva format som skal nyttast for tilbakelevering>*
☐	*<Set inn eventuelle andre avtalte rutinar for sletting eller tilbakelevering>*

C.7 Sektorspesifikke føresegner om behandling av personopplysningar

<Set inn eventuelle sektorspesifikke føresegner om behandling av personopplysningar som skal omfattast av omgrepet «Gjeldande personvernreglar», sjå databehandlaravtalen punkt 2.>

C.8 Kontaktinformasjon

Ved kontakt i samsvar med denne avtalen, eksempelvis ved varsling om brot på personopplysningstryggleiken eller endring i bruk av underdatabehandlarar, skal følgjande kanalar nyttast:

Hos Behandlingsansvarleg	**Hos Leverandøren**
Tryggleiksbrot:	Tryggleiksbrot:
Systemforvaltar (systemansvarleg) Telefon: *[Fyll ut]* E-post *[Fyll ut]*	Telefon: *[Fyll ut]* E-post *[Fyll ut]*
Sikkerheitskoordinator Telefon: *[Fyll ut]* E-post *[Fyll ut]*	
Personvernombod Telefon: *[Fyll ut]* E-post *[Fyll ut]*	
Andre førespurnader:	Andre førespurnader:
Namn: *[Fyll ut]*	Namn: *[Fyll ut]*
Stilling: *[Fyll ut]*	Stilling: *[Fyll ut]*
Telefon: *[Fyll ut]*	Telefon: *[Fyll ut]*
E-post: *[Fyll ut]*	E-post: *[Fyll ut]*

D. ENDRINGAR TIL STANDARDTEKSTEN I DATABEHANDLARAVTALEN OG ENDRINGAR ETTER AVTALEINNGÅINGA

Endring til standardtekst i DBA punkt 8.4:

Databehandlar kan i tilfelle der det er hensiktsmessig, og etter instruksjon frå Behandlingsansvarleg varsle/melde til Datatilsynet om brot på personopplysningstryggleiken.