

## **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 .....                                                             | 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 .....                                                                           | 8  |   |
| C.4   | Overføring av personopplysninger - Lokasjon for behandling og tilgang .....                   | 8  |   |
| C.5   | Rutiner for revisjon og tilsyn .....                                                          | 8  |   |
| C.6   | Sletting og tilbakelevering av personopplysninger ved avtalens opphør .....                   | 10 |   |
| C.7   | Sektorspesifikke bestemmelser om behandling av personopplysninger .....                       | 10 |   |
| C.8   | Kontaktinformasjon .....                                                                      | 11 |   |
| D.    | Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen .....   | 12 |   |

## 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:

#### **26/2247 Rammeavtale for internrevisjonstjenester**

Behandlingen har følgende formål:

Gjennomføre internrevisjonsoppdrag, herunder undersøkelser.

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

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

I forbindelse med revisjon og andre undersøkelser vil databehandleren samle inn personopplysninger som en del av faktagrunnlaget for sine rapporter. Personopplysningene vil hentes fra ulike kilder, som interne dokumenter, gjennom intervju mv.

Ved eventuell åpning av epostkasser vil dette skje i samsvar med gjeldende lover og forskrifter. Behandlingsansvarlig er ansvarlig for at de nødvendige samtykker mm. er innhentet.

A.3 **Typer av personopplysninger**

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

|                                     |                                                                                                                                                                                                             |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | <i>Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1):</i><br>Eventuelle helseopplysninger som fremkommer av revisjoner/undersøkelser/kartlegginger/granskninger.                   |
| <input checked="" type="checkbox"/> | <i>Andre opplysninger med særlig behov for beskyttelse:</i><br>Eventuelle opplysninger om økonomi, opplysninger om enkeltpersoners arbeidsforhold, andre opplysninger om personlige forhold, fødselsnummer. |
| <input checked="" type="checkbox"/> | <i>Andre personopplysninger:</i><br>Alminnelige personopplysninger som navn, kontaktinformasjon mm.                                                                                                         |

A.4 **Kategorier av registrerte**

Behandlingen omfatter følgende kategorier av registrerte:

Ansatte i Boligbygg Oslo KF

Ansatte/eiere hos leverandører

Andre personer med relasjon til internrevisjonstjenestene

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 er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen. |
| <input type="checkbox"/>            | Behandlingen er tidsbegrenset, og gjelder frem til                            |

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 checked="" 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. |

Bilag A, B, C, og D til Databehandleravtalen

|                          |                                                                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | Hvis Behandlingsansvarlig motsetter seg endringen skal Databehandler underrettes så snart som mulig. Den behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn.                                                                                                                                    |
| <input type="checkbox"/> | 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.   | 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] |                                                                  |

Bilag A, B, C, og D til Databehandleravtalen

|  |  |  |  |                               |  |  |
|--|--|--|--|-------------------------------|--|--|
|  |  |  |  | på annen måte<br>behandles 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

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:

*Personopplysninger kan gjelde sensitive personlige forhold og må behandles konfidensielt.*

☐ 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 personopplysningene, herunder (flere valg mulig):

|                          |                                              |
|--------------------------|----------------------------------------------|
| <input type="checkbox"/> | Sikkerhetskrav som beskrevet i Hovedavtalen: |
|--------------------------|----------------------------------------------|

|                                     |                                                                                                                                                                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | <p>Sikkerhetskrav som beskrevet nedenfor:</p> <p>Databehandleren skal på Behandlingsansvarlige forespørsel fremlegge dokumentasjon på at Databehandleren har et egnet styringssystem for informasjonssikkerhet.</p> |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 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):

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" 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></ul> |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <ul style="list-style-type: none"> <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>gjennomføres én gang årlig,</li> <li>utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402.</li> <li>utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring</li> </ol> <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## C.6 Sletting og tilbakelevering av personopplysninger ved avtalens opphør

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

|                                     |                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | <p>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.</p> |
| <input type="checkbox"/>            | <p>Alle personopplysninger som behandles under denne Databehandleravtale, samt eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig, skal tilbakeleveres ved opphør av Hovedavtalen.</p>                                                                 |

|  |                                                                                                                                                                                                                                                        |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Etter tilbakelevering er skjedd, plikter Databehandler å slette alle personopplysninger og annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig innen 30 kalenderdager.</p> <p>Tilbakelevering skal skje på følgende måte:</p> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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:

Randi Anne Ervik, seksjonsleder IT

Telefon: 918 28 503

E-post

*randi.anne.ervik@bby.oslo.kommune.no*

Andre henvendelser:

Navn: *Marit J. Leganger*

Stilling: Administrerende direktør

Telefon: 920 67 676

E-post:

*marit.leganger@bby.oslo.kommune.no*

**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**