**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**

[A. Opplysninger om behandlingen 3](#_Toc29465057)

[A.1 Hovedavtalen og formålet med behandlingen av personopplysninger 3](#_Toc29465058)

[A.2 Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige 3](#_Toc29465059)

[A.3 Typer av personopplysninger 4](#_Toc29465060)

[A.4 Kategorier av registrerte 4](#_Toc29465061)

[A.5 Varighet av behandlingen 4](#_Toc29465062)

[B. Betingelser for Databehandlerens bruk og endring av eventuelle Underdatabehandlere 5](#_Toc29465063)

[B.1 Behandlingsansvarliges godkjennelse av bruk av Underdatabehandlere 5](#_Toc29465064)

[B.2 Godkjente Underdatabehandlere 6](#_Toc29465065)

[C. Instruks vedrørende behandling av personopplysninger 7](#_Toc29465066)

[C.1 Behandlingens omfang og formål 7](#_Toc29465067)

[C.2 Sikkerhet ved behandlingen 7](#_Toc29465068)

[C.2.1 Angivelse av sikkerhetsnivå 7](#_Toc29465069)

[C.2.2 Styringssystem for informasjonssikkerhet 8](#_Toc29465070)

[C.3 Dokumentasjon 8](#_Toc29465071)

[C.4 Overføring av personopplysninger - Lokasjon for behandling og tilgang 8](#_Toc29465072)

[C.5 Rutiner for revisjon og tilsyn 8](#_Toc29465073)

[C.6 Sletting og tilbakelevering av personopplysninger ved avtalens opphør 10](#_Toc29465074)

[C.7 Sektorspesifikke bestemmelser om behandling av personopplysninger 10](#_Toc29465075)

[C.8 Kontaktinformasjon 11](#_Toc29465076)

[D. Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen 12](#_Toc29465077)

# Opplysninger om behandlingen

## 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.****>*

Behandlingen har følgende formål:

Kontraktsoppfølging og ivaretakelse av lovkrav.

Med kontraktsoppfølging menes byggherrens kontroll av driftsentreprenørens arbeid, gjennomgang av dokumentasjon, og håndheving av bestemmelser i driftskontrakten, herunder på områdene HMS, fakturering, kvalitet på utført arbeide og etterlevelse av gjeldende lovverk. Det ligger innenfor formålet å sammenstille opplysninger fra en kontrakt, med tilsvarende informasjon fra andre SVV-kontrakter, og fra relevante kontrakter hos andre byggherrer. Formålet omfatter også det å dokumentere manglende etterlevelse.

Formålet omfatter videre særskilt kontraktoppfølging for å undersøke, avdekke og dokumentere potensielt useriøse og/eller kriminelle forhold, eller annen uønsket aktivitet, som skjer i ond tro hos driftsentreprenøren eller i dennes leverandørkjede (dvs. arbeid mot arbeidslivs- og annen kriminalitet). Det ligger innenfor denne særskilte kontraktoppfølgingen å sammenstille opplysninger fra en kontrakt, med informasjon innhentet fra åpne kilder, og å utlevere informasjon fra en kontrakt i tråd med gjeldende og relevant lovverk.

Formålet omfatter også å ivareta lovkrav i Statens vegvesen sine driftskontrakter (herunder byggherreforskriften og forskrift om arbeidsvilkår i off. kontrakter).

## Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige

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

For å oppfylle sine plikter etter Hovedavtalen, må entreprenøren som Databehandler behandle personopplysninger på vegne av byggherren som Behandlingsansvarlig. Behandlingsaktivitetene går blant annet ut på innsamling og registrering av opplysninger på vegne av byggherren, rapportering til byggherren, og annen behandling av opplysninger som krevd i kontrakten. Behandlingen skjer blant annet i forbindelse med:

ELRAPP:

* Produksjonsdata vinterdrift: Registrering av opplysninger om bevegelsesmønster, aktivitet og kjøretøyinformasjon, tilhørende strø- og brøytekjøretøy som opererer på driftskontraktene.
* Planverk.
* Registrering og rapportering i tråd med:
  + R2 Skade, feil og mangler på vegobjekt
  + R5 Skade på vegobjekt med kjent eller ukjent motorvogn
  + R10 Vær-, føre- og trafikkforhold
  + R11 Skred og skredfare
  + R12 Mengdedata pr måned
  + Saltjournal
  + R13 Naturfare, skredfarevurdering
  + R18 Uønsket hendelser, farlige forhold - HMS
  + R19 Månedsrapport HMS
  + R20 Samlerapport inspeksjoner

Utenfor ELRAPP:

* PLANIA.
* BRUTUS.
* UHF-samband og nødnett o.l. (ved utlevering av utstyr).
* Inspeksjonsdokument. R20 samledokument for inspeksjoner.
* Dokumentasjon utarbeidet ved utført arbeid.
* Objektregistrering.
* Vinterfriksjonsmålinger.
* Diverse innmeldinger og annen informasjon entreprenøren mottar som byggherrens representant ute på vegnettet.

Opplistingen er ikke uttømmende og det vises til Hovedavtalen for en fullstendig oversikt.

## 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:*  *- Lokasjonsdata (tid/klokkeslett, dato, GPS-posisjon)*  *- Kjøretøy-ID (unik identifikator)*  *- Kjøretøy hastighet*  *- Metode for utført arbeid (brøyting, høvling, salting, strø sand etc.)*  *- Mengder som blir benyttet (ved sanding og salting)*  *- Vegreferanse (sted)*  *- Navn på arbeidstaker, innmelder i registereringsskjema, epost*  *- Bosted eller forventet uttrykkingsted*  *- kan være foto av 3.mann eller registreringsnummer kjøretøy*  *- Kan unntaksvis forekomme personopplysninger jf. art. 9 og 10 i forbindelse med HMS* |

## Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

De som utfører arbeid på driftskontrakten (ansatte hos E, UE, UUE mm. eller innleide). Unntaksvis tredjemann.

## 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>.* |

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

# Betingelser for Databehandlerens bruk og endring av eventuelle Underdatabehandlere

## Behandlingsansvarliges godkjennelse 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 godkjennelse fra Behandlingsansvarlig. Underdatabehandleren kan ikke behandle personopplysninger under Hovedavtalen før slik godkjennelse er gitt. Godkjennelse kan ikke nektes uten saklig grunn. |

## 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]* |  |

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.

# Instruks vedrørende behandling av personopplysninger

## Behandlingens omfang og formål

Personopplysningene skalutelukkende 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.

## Sikkerhet ved behandlingen

### 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:  Interesseavveining er gjort i Mime dokument nr. 21/163647-2.  Behandlingen vil kun unntaksvis inneholde særlige kategorier av personopplysninger. De identifiserte personvernkonsekvensene er begrensede. Det er foretatt en rekke avhjelpende tiltak på behandlingen for å sikre dataminimering og å gjøre behandlingen så lite inngripende som mulig og eventuelle negative konsekvenser er ikke av en art som er nevneverdig. |

### 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:  Databehandler skal herunder, men ikke begrenset til, alltid iverksette følgende tiltak når det er relevant i lys av oppgavene og/eller tjenestene etter Hovedavtalen:  - Følge alminnelig anerkjente standarder for informasjonssikkerhet eller tilsvarende.  - Sikre at antallet medarbeidere med tilgang til personopplysninger begrenses til det som er nødvendig.  - Sikre at uautoriserte ikke har adgang til lokaler, filer, eller systemer, der personopplysninger som Databehandler får tilgang til under Databehandleravtalen oppbevares eller behandles.  - Sikre at personopplysninger omfattet av denne Databehandleravtale holdes logisk adskilt fra egne og andres opplysninger og tjenester. Med logisk adskilt forstås at nødvendige tekniske tiltak som sikrer data mot uønsket endring og innsyn, er iverksatt og opprettholdt.  - Sikre at lagringsmedier og/eller datautstyr som benyttes ved behandling av personopplysninger er beskyttet mot ødeleggelse, og mot at uvedkommende får adgang. Databehandler skal ha systemer for sikkerhetskopiering og gjenoppretting.  - Sikre at det er etablert tiltak mot ødeleggende programvare på de av Databehandlers systemer som benyttes til å behandle personopplysningene på vegne av Behandlingsansvarlig. Databehandler skal blant annet benytte brannmur og programvare for viruskontroll.  - Sikre at ansatte hos Databehandler får tilstrekkelig og nødvendig opplæring i relevant lov- og regelverk, samt innehar god sikkerhetskultur for håndtering av personopplysninger.  - Sikre at det er iverksatt tiltak som er nødvendige for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til data, spredning eller endring av data, så vel som urettmessig innsyn og enhver annen bruk av personopplysninger som ikke er i overensstemmelse med denne Databehandleravtale.  - Sikre at avvik fra krav til personopplysningssikkerhet registreres og rapporteres, herunder at Databehandler loggfører og dokumenterer ethvert forsøk på ikke-autorisert tilgang og andre henvendelser av betydning for personopplysningssikkerheten. Slik dokumentasjon skal oppbevares i minimum 3 måneder, samt varsles til Behandlingsansvarlig.  - Sikre at rutiner for å håndtere uønskede hendelser er tatt i bruk. |

## 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.

## 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 (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.

## 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:   1. gjennomføres én gang årlig, 2. utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402. 3. 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>* |

## 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.  Tilbakelevering skal skje på følgende måte:  Databehandler får kun tilgang til opplysninger i sanntid. Ingen data/informasjon lagres. |
|  | *<Sett inn eventuelle andre avtalte rutiner for sletting eller tilbakelevering>* |

## 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.*>

## 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** | **Hos Leverandøren** |
| Sikkerhetsbrudd:  *[Her oppgis personvernkontakt for divisjon Drift og vedlikehold: Kris Aleksander Mikkelsen. I tillegg oppgis epost til personvernombud for Statens vegvesen]* | Sikkerhetsbrudd: |
| Telefon: 47 410 12124 | Telefon: *[Fyll ut]* |
| E-post:  [kris.mikkelsen@vegvesen.no](mailto:kris.mikkelsen@vegvesen.no)  [personvernombud@vegvesen.no](mailto:personvernombud@vegvesen.no) | E-post *[Fyll ut]* |
| Andre henvendelser: | Andre henvendelser: |
| Navn: *[Byggeleder for aktuell kontrakt]* | Navn: *[Fyll ut]* |
| Stilling: *[Fyll ut]* | Stilling: *[Fyll ut]* |
| Telefon: *[Fyll ut]* | Telefon: *[Fyll ut]* |
| E-post: *[Fyll ut]* | E-post: *[Fyll ut]* |

# Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen