

Vedlegg 4
Databehandleravtale
Anskaffelse av kontrolltjenester i
Stor-Trondheim



Vedlegg 4

Databehandleravtale **(Databehandleravtalen)**

Vedrørende behandling av **personopplysninger**

mellom

AtB AS
(Behandlingsansvarlig)

og

(Navn Leverandør)
(Databehandler)

1. Innledning

I henhold til (Hovedavtale) mellom (Navn Leverandør) og AtB AS, vil (Navn Leverandør) (heretter kalt Databehandler) behandle personopplysninger på vegne av AtB AS (heretter kalt Behandlingsansvarlig).

Dette bilaget gjelder behandling av alle personopplysninger som Databehandler behandler på vegne av Behandlingsansvarlig som et ledd i gjennomføring av Hovedavtalen. Databehandler har ikke rett til å behandle personopplysningene på annen måte enn det som følger av denne databehandleravtalen. Databehandleravtalen gjelder tilsvarende så langt den passer for behandling av virksomhetskritiske opplysninger.

Databehandleravtalen skal sikre at personopplysninger ikke brukes urettmessig eller kommer uberettigede i hende.

Personopplysningene skal behandles i samsvar med de til enhver tid gjeldende kravene til behandling av personopplysninger, herunder bl. A. EU forordning 2016/679 av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger som er implementert i Norge ved lov av 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) med tilhørende forskrifter.

Databehandleravtalen fritar ikke Databehandleren for plikter som er pålagt i personopplysningslovgivningen eller enhver annen lovgivning, selv om forholdet ikke skulle være omtalt i denne Databehandleravtalen. Ved eventuell motstrid mellom Databehandleravtalens regulering og de rammer som følger av personopplysningsloven eller personvernforordningen, viker Databehandleravtalens regulering.

2. Formål

Databehandleravtalen skal klargjøre Databehandler og Behandlingsansvarliges ansvar for behandling av personopplysninger ved gjennomføring av Hovedavtalen. Dette for å sikre at krav til konfidensialitet, integritet, tilgjengelighet, robusthet og kvalitet ivaretas.

Følgende personopplysninger vil etter Databehandleravtalen bli behandlet i Databehandler sine løsninger:

- Navn

- Adresse
- Fødselsdato/personnummer
- Telefonnummer
- Foresattes navn, adresse og telefonnummer
- Studentbevis
- Honnørbevis
- Helseopplysninger
- Straffbart forhold (dokumentforfalskning)
- Navn og telefonnummer til andre enn passasjeren i forbindelse med;
 - o innsamling av bevis til sak om dokumentforfalskning
 - o vitner til hendelse/kontroll
- DUF-nummer
- Sjøfører-ID
-

Opplysningene skal bare brukes i nødvendig utstrekning i overensstemmelse med oppdraget i Databehandleravtalen.

Behandlingsansvarlig kan ved behov utstede en instruks for behandling av personopplysninger. Denne instruks vil være et vedlegg til denne avtale og oppdateres uavhengig av Databehandleravtalen.

3. Behandlingsansvarliges rolle

Behandlingsansvarlig bestemmer over bruken av personopplysningene som omfattes av denne avtale. Behandlingsansvarlig er videre ansvarlig for at det foreligger et lovlig behandlingsgrunnlag for personopplysningene, og at de aktuelle behandlingene er i overensstemmelse med gjeldende regelverk.

Med mindre annet følger av lov, har behandlingsansvarlig rett til tilgang til, og innsyn i, de personopplysningene som behandles av Databehandler på vegne av Behandlingsansvarlig. Behandlingsansvarlig har rett til tilgang til, og innsyn i, Databehandlers IT-systemer som benyttes til behandling av personopplysninger. Dette gjelder informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet i behandlingen. Databehandler plikter, om nødvendig, å gi behandlingsansvarlig nødvendig bistand til å gi tilgang til/innsyn i personopplysningene.

Behandlingsansvarlig har taushetsplikt om eventuelle virksomhetskritiske opplysninger han gjennom slik tilgang og/eller innsyn får tilgang til hos Databehandler, og som ikke er relatert til behandlingen av personopplysninger for Behandlingsansvarlig.

Behandlingsansvarlig skal rette seg etter Dataleverandørs skriftlige instruksjoner vedrørende pålogging og bruk av systemer, samt krav til oppdatert og vedlikeholdt datautstyr som brukes ved pålogging, for å opprettholde informasjonssikkerhet etablert av Dataleverandør, jf. 4.2 i denne avtale.

4. Databehandlers plikter

4.1 Innledning

Databehandleren behandler personopplysninger på vegne av Behandlingsansvarlig. Databehandleren har ikke anledning til å behandle personopplysninger på vegne av Behandlingsansvarlig for andre formål enn det som er beskrevet i denne Databehandleravtalen.

Databehandleren skal følge de dokumenterte rutiner og instruksjoner for behandlingen som den behandlingsansvarlige til enhver tid har bestemt skal gjelde. Personopplysningene skal ikke benyttes på annen måte, eller til annet formål, enn det som er avtalt med Behandlingsansvarlig. Opplysningene kan heller ikke overlates, selges, etc. til andre for lagring, bearbeidelse mv. uten forhåndsaksept av Behandlingsansvarlig. Databehandleren skal underrette Behandlingsansvarlig om rettslige krav om behandling som ikke bygger på Behandlingsansvarliges instruksjoner før behandlingen

skjer, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr en slik underretning.

Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks er i strid med personforordning eller andre bestemmelser om vern av personopplysninger.

4.2 Plikt til å treffe egnede tekniske og organisatoriske tiltak

Databehandler plikter å behandle personopplysninger i tråd med prinsipper for behandling av personopplysninger angitt i personvernforordningens artikkel 5. Databehandler har videre det praktiske ansvaret for å iverksette planlagte og systematiske tiltak for å sikre en tilfredsstillende informasjonssikkerhet og internkontroll i henhold til personvernforordningens artikkel 28.

Databehandler plikter å ha systemdokumentasjon og rutinebeskrivelser som er relevante i forbindelse med behandling av personopplysninger etter Databehandleravtalen. Med dokumentasjon menes rutiner for autorisasjon og bruk, ulike tekniske og organisatoriske sikkerhetstiltak etc. Databehandler er ansvarlig for at dokumentasjonen er tilgjengelig for Behandlingsansvarlig, og at dokumentasjonen oppdateres ved endringer. Denne dokumentasjonen skal kunne legges frem for Behandlingsansvarlig på forespørsel. Innsyn i dokumentasjonen skal reguleres strengt (gis til et begrenset antall autoriserte personer) slik at dette ikke svekker sikkerhetsnivået.

Databehandleren plikter å gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne Databehandleravtalen oppfyller kravene i personopplysningsloven om vern av registrertes rettigheter, herunder innfrir alle kravene etter personvernforordningens artikkel 32.

Tiltakene skal sørge for at hensynene til konfidensialitet, integritet, tilgjengelighet og robusthet ivaretas ved behandling av personopplysninger. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til, eller spredning av, data, så vel som enhver annen bruk av personopplysninger som ikke er i overensstemmelse med denne Databehandleravtalen. Det omfatter også tiltak for å gjenopprette tilgjengelighet og tilgang til personopplysninger etter uønskede hendelser.

Databehandleren skal ved hjelp av egnede tekniske og organisatoriske tiltak, bistå den behandlingsansvarlige med å oppfylle vedkommende sin plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.

4.3 Innsyn og retting av opplysninger

Dersom Databehandler mottar forespørsler, herunder krav om innsyn, fra registrerte (Behandlingsansvarliges kunder) eller fra andre i medhold av personopplysningsloven, skal Databehandler videreformidle forespørselen til Behandlingsansvarlig og bistå behandlingsansvarlig med å besvare slike forespørsler. Databehandler må uten ugrunnet opphold varsle Behandlingsansvarlig om forespørsler fra registrerte medfører økt ressursbruk.

Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, er Databehandler forpliktet til å rette opplysningene, bistå den behandlingsansvarlige, samt - så langt som mulig - å sørge for at feilen ikke får betydning for den registrerte (Behandlingsansvarliges kunde).

4.4 Plikt til å yte bistand

Databehandler skal, ved forespørsel fra behandlingsansvarlig, bistå i forbindelse med etterlevelse av diverse plikter den Behandlingsansvarlige har etter forordningens artikler 32-36, blant annet:

- bistå i forbindelse med å melde brudd på personopplysningssikkerheten til Datatilsynet
- bistå med å underrette den/de registrerte om brudd på personopplysningssikkerheten
- bistå når det skal gjennomføres konsekvensanalyser og/eller forhåndsdrøftelser

4.5 Adferdsnormer

Foreligger det godkjente adferdsnormer (bransjenormer) etter personvernforordningens artikkel 40, eller godkjent sertifiseringsordning etter artikkel 42 som Databehandleren har påtatt seg å overholde eller være sertifisert etter, plikter Databehandleren å etterleve slike adferdsnormer eller sertifiseringskrav.

4.6 Plikt til å føre protokoll

Dersom det er pliktig etter personvernforordningen artikkel 30, skal Databehandleren skal føre protokoll (logg) over behandlingsaktiviteter denne utfører på vegne av behandlingsansvarlig, for å sikre at Databehandler vet hvor data blir lagret. Loggen skal inneholde informasjon om på hvilket internt eller eksternt lagringsmedium data er lagret.

Databehandler skal videre registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres, skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte eller andre hos Databehandler, underleverandør og hos behandlingsansvarlig).

Loggen skal minimum inneholde den informasjonen som er pålagt etter personvernforordningen artikkel 30. Den behandlingsansvarlige kan til enhver tid kreve oversendt kopi av loggen. Loggen skal oppbevares av Databehandler til det ikke lenger antas å være bruk for dem.

5. Avvikshåndtering

Hvis det forekommer brudd på personopplysningssikkerheten eller annet avvik fra etablert informasjonssikkerhetsnivå, skal Databehandler som en del av avviksrutinen umiddelbart sende avviksrapporter til Behandlingsansvarlig for avvik. Dersom det avdekkes fare for at personopplysninger kan komme på avveie, skal det treffes strakstiltak for å forhindre dette, samt varsles i henhold til forrige punktum.

Databehandler skal snarest mulig etter at avvik er oppdaget sende avviksmelding til Behandlingsansvarlig. Avviksmelding skal skje ved at Databehandler umiddelbart melder avviket/sikkerhetsbruddet til Behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding sendes til Datatilsynet. Meldingen skal som minimum inneholde følgende informasjon:

- Hvilke personopplysninger som er på avveie
- Omfanget av avviket
- (Hvis mulig) årsaken til avviket
- Beskrivelse av konsekvensene og potensiell risiko for personopplysningene
- Beskrivelse av tiltak som er, eller vil bli, iverksatt for å hindre skade eller begrense skadeomfanget
- Eventuell annen relevant informasjon som er nødvendig for at Behandlingsansvarlig skal kunne ivareta sine forpliktelser

Resultatet av avviksbehandlingen skal dokumenteres.

Databehandler plikter å gjennomføre årlige sikkerhetsrevisjoner knyttet til behandlingen av personopplysninger etter denne Databehandleravtalen. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Resultatet av denne skal dokumenteres og forelegges Behandlingsansvarlig på forespørsel.

Dersom Behandlingsansvarlige finner at Databehandlers informasjonssikkerhet eller internkontroll når det gjelder behandling av personopplysninger ikke er tilfredsstillende, plikter Databehandler å justere sikkerhetsnivået etter instruks fra Behandlingsansvarlig.

Databehandler skal oversende rapport til Behandlingsansvarlig der minimum følgende fremgår:

- Registrerte avvik
- Sikkerhetsrevisjonsfunn
- En bekreftelse på at behandling fortsatt er begrenset av formålet angitt i denne Databehandleravtalen.

Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, er Databehandler forpliktet til å rette opplysningene, bistå den behandlingsansvarlige, samt - så langt som mulig - å sørge for at feilen ikke får betydning for den registrerte (Behandlingsansvarliges kunde).

6. Bruk av underleverandører

Databehandler forplikter seg til ikke å overføre personopplysninger som Databehandler behandler på vegne av Behandlingsansvarlig til tredjepersoner, uten forutgående avtale med Behandlingsansvarlig. Databehandleren skal underrette Behandlingsansvarlig om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi Behandlingsansvarlig muligheten til å motsette seg slike endringer. Databehandlers bruk av underoperatør skal avtales skriftlig med Behandlingsansvarlig før behandlingen starter.

Dersom Databehandler engasjerer en annen Databehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal nevnte andre Databehandler pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i Databehandleravtalen eller i et annet rettslig dokument mellom partene, jf. personvernforordningen artikkel 28 nr. 3.

Det skal inngås egen Databehandleravtale mellom Databehandler og Databehandlers underleverandør. Databehandlerplikter å påse at underleverandør pålegges de samme forpliktelsene med hensyn til vern av personopplysninger, som er fastsatt i denne databehandleravtalen, før personopplysninger overføres. Dersom nevnte underleverandør ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal Databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at nevnte andre Databehandler ikke oppfyller sine forpliktelser.

En oppdatert liste over underleverandører som Databehandler benytter beskrives i vedlegg 1. Dette vedlegget skal revideres, signeres av Databehandler og oversendes Behandlingsansvarlig ved endringer av underleverandører.

7. Overføring til utlandet

Databehandler har ikke - uten samtykke fra Behandlingsansvarlig - adgang til å overføre personopplysninger som omfattes av denne Databehandleravtalen til land og/eller tredjepersoner utenfor EU/EØS som ikke har tilfredsstillende beskyttelsesnivå, jf. personvernforordningen artikkel 45.

8. Revisjon

Behandlingsansvarlig, eller en annen inspektør på fullmakt fra den behandlingsansvarlige, skal ha muligheten til å gjennomføre sikkerhetsrevisjoner og andre relevante revisjoner av Databehandler. Behandlingsansvarlig vil gi varsel innen rimelig tid før slik revisjon utføres.

Databehandleren skal ved behov gi nødvendig bistand til behandlingsansvarlig i denne sammenheng, herunder å gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i personvernforordningen og denne Databehandleravtalen er oppfylt, samt muliggjøre og bidra til revisjoner.

Revisjonen kan omfatte gjennomgang av rutiner, inspeksjoner, stikkprøvekontroller, mer omfattende stedlige kontroller og/eller andre egnede kontrolltiltak, bl.a. i den hensikt å påvise at forpliktelsene i personvernforordningen artikkel 28 er oppfylt.

9. Taushetsplikt

Databehandler har taushetsplikt om all dokumentasjon og personopplysninger som vedkommende får tilgang til iht. Hovedavtalen og Databehandleravtalen. Dette gjelder også etter Hovedavtalen og Databehandleravtalens opphør.

Ansatte hos Databehandler og/eller andre som utfører arbeid for leverandøren, og som har tilgang til personopplysningene, skal signere taushetserklæring. Databehandler plikter å sikre at nevnte taushetserklæring er i henhold til bestemmelsene i denne Databehandleravtalen samt Hovedavtalen.

Tilgang til personopplysningene gis kun etter tjenstlig behov. Signerte taushetserklæringer skal på forespørsel gjøres tilgjengelige for Behandlingsansvarlig. Taushetsplikten gjelder også etter opphør av tjenesteleveransen.

Informasjon som partene blir kjent med i forbindelse med avtalen og gjennomføringen av avtalen, skal behandles konfidensielt og ikke gjøres tilgjengelig for utenforstående uten samtykke fra den annen part.

10. Mislighold

Ved brudd på denne Databehandleravtalen, personopplysningsloven eller annet regelverk kan behandlingsansvarlig pålegge Databehandler og/eller eventuelle underleverandører å stoppe den videre behandlingen av personopplysningene med øyeblikkelig virkning, samt iverksette eventuelle nødvendige sikkerhetstiltak for å beskytte opplysningene.

Brudd på denne Databehandleravtalen kan være å anse som mislighold, jf. misligholdsbestemmelsene i Hovedavtalen.

Databehandler skal holde Behandlingsansvarlig skadesløs for ethvert tap, kostnad eller ansvar for skade (økonomisk og ikke-økonomisk), herunder også potensielle bøter eller gebyrer, som Behandlingsansvarlig lider eller blir holdt ansvarlig for som følge av Databehandlers (eller Databehandlers underleverandørs) brudd på lov, forskrift eller plikter etter denne Databehandleravtalen. Behandlingsansvarlig skal holde Databehandler skadesløs for krav som oppstår som følge av Behandlingsansvarliges brudd på personopplysningslov med tilhørende forskrift eller plikter etter denne Databehandleravtalen.

11. Varighet

Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig, jf. denne Databehandleravtalen og Hovedavtalen, og frem til alle personopplysninger er tilbakelevert, slettet eller destruert, jf. punkt 12 i denne Databehandleravtalen.

12. Lagring, tilbakeføring og sletting/destruksjon ved opphør

Databehandler skal ikke lagre personopplysninger lenger enn det som følger av avtale med Behandlingsansvarlig eller forøvrig følger av regelverket.

Ved opphør av denne Databehandleravtalen plikter Databehandler etter nærmere instruksjoner fra den behandlingsansvarlige å slette/destruere eller tilbakelevere alle personopplysninger (herunder kopier/sikkerhetskopier, dokumenter, data, disketter, cd-er og annet som inneholder personopplysninger) som er behandlet på vegne av Behandlingsansvarlig og som omfattes av denne Databehandleravtalen, med mindre annet skriftlig avtales mellom partene eller er pålagt ved lov.

Databehandler skal videre, på forespørsel, gi behandlingsansvarlig utskrift av, eller gjøre tilgjengelig på annen måte, alt innhold i databaser og lignende som inneholder data som er omfattet av denne Databehandleravtalen eller av Driftsavtalen.

Databehandler skal innen rimelig tid skriftlig dokumentere at tilbakelevering, sletting og/eller destruksjon er foretatt i henhold til Databehandleravtalen. Tilbakelevering, sletting og/eller destruksjon skal skje kostnadsfritt for Behandlingsansvarlig, med mindre Databehandler kan dokumentere ekstraordinære merkostnader for et slikt arbeid, som ikke dekkes av de vanlig månedlige driftskostnadene.

13. Meddelelser

Meddelelser etter Databehandleravtalen skal sendes skriftlig til Behandlingsansvarlig ved Personvernombud, e-post: personvern@atb.no

Avvik skal også meldes til normalt etablert kontaktpunkt for service og vedlikehold.

14. Endring i lovverk mv.

Ved endring i lov eller forskrift, kan behandlingsansvarlig kreve endringer i denne Databehandleravtalen slik at den reflekterer eventuelle nye krav og forpliktelser.

15. Lovvalg og vernetting

Databehandleravtalen er underlagt norsk rett og partene vedtar Sør-Trøndelag tingrett som vernetting. Dette gjelder også etter at Databehandleravtalen er opphørt.

Denne Databehandleravtalen er signert i 2 – to – eksemplarer, hvorav partene får hvert sitt eksemplar.

Sted/ dato

Sted/ dato

Janne Sollie
Adm. Dir., AtB AS
(Behandlingsansvarlig)

Navn
Navn Leverandør
(Databehandler)

Vedlegg:

- Underleverandører
- Instruks for behandling av personopplysninger