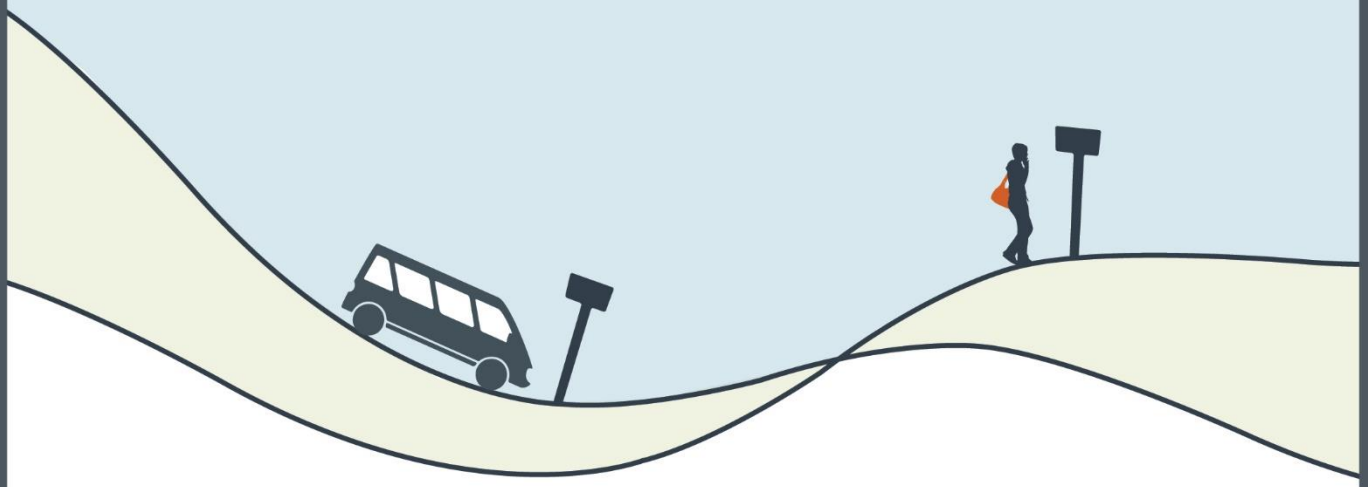

Anbud Region individuelt tilrettelagt skoleskyss og bestillingstransport 2019-2021

Vedlegg 4 Databehandleravtale

Databehandleravtale

(heretter «avtalen» eller «databehandleravtalen»)

I henhold til personopplysningslovens §13, jf. §15 og personopplysningsforskriftens kapittel 2, samt EUs personvernforordning (GDPR).

mellom

AtB AS

(heretter «Oppdragsgiver» eller «behandlingsansvarlig»)

og

[XXXX]

(heretter «Operatør» eller «databehandler»)

Partene er enige om at Databehandleravtalen fylles ut med mer konkret innhold etter kontraktsignering, men før oppstart av Oppdraget.

1 Avtalens formål

Avtalen skal sikre at all behandling av personopplysninger om den registrerte (Oppdragsgivers kunde) utføres i samsvar med lov og forskrift, ikke brukes urettmessig eller kommer uberettigede i hende.

Som følge av Kontrakt for anbud region 2019-2021 (heretter omtalt som «Hovedavtalen») og som et ledd i leveransen, vil databehandler jevnlig behandle personopplysninger på vegne av Oppdragsgiver. Se Databehandleravtalen punkt 3 for ytterligere presisering av behandlingene.

Denne avtalen regulerer databehandlerens bruk av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse. Avtalen regulerer videre rettigheter og plikter for partene i forbindelse med behandlingen av personopplysningene.

Personopplysningene skal behandles i samsvar med de til enhver tid gjeldende kravene til behandling av personopplysninger, herunder bl.a. EU-direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger som er implementert i Norge ved lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) med tilhørende forskrifter. Fra og med 25. mai 2018 må personopplysningene behandles i henhold til kravene etter Europaparlaments- og rådsforordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger og om oppheving av direktiv 95/46/EF (personvernforordningen/GDPR) som ble besluttet 27. april 2016, samt norsk lov med tilhørende forskrifter som innføres som en følge av personvernforordningen og vil erstatte personopplysningsloven.

Databehandleravtalen og Hovedavtalen er innbyrdes avhengige, og kan ikke sies opp særskilt. Databehandleravtalen kan dog – uten at Hovedavtalen sies opp – erstattes av en ny data-behandleravtale.

Databehandler har ikke rett til å behandle personopplysningene på annen måte enn det som følger av denne avtalen. Avtalen gjelder tilsvarende så langt den passer for behandling av virksomhetskritiske opplysninger.

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

2 Definisjoner

Det vises til definisjonene i den underliggende Hovedavtalen. I tillegg gjelder følgende definisjoner:

Behandlingsansvarlig: Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, dvs. Oppdragsgiver v/daglig leder, jf. personopplysningsloven § 2 nr. 4 og personvernforordningen artikkel 4 nr. 7.

Databehandler: Den som behandler personopplysninger *på vegne av* den behandlingsansvarlige, jf. personopplysningsloven § 2 nr. 5 og personvernforordningen artikkel 4 nr. 8.

Virksomhetskritiske opplysninger: Opplysninger som er av sentral betydning for oppdragsgivers virksomhet, for eksempel strategier, kontrakter, priser, regnskapstall og/eller lignende dokumenter.

Personopplysninger: Opplysninger og vurderinger som kan knyttes til en enkeltperson, jf. personopplysningsloven § 2 nr. 1 og personvernforordningen artikkel 4 nr. 1.

Behandling: Enhver bruk av Personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf. personopplysningsloven § 2 nr. 2 og personvernforordningen artikkel 4 nr. 2.

3 Nærmere om behandlingen av personopplysninger

3.1 Overordnet

I forbindelse med trafikkstyring og logistikk, billettering, rapportering og kontroll, vil databehandler behandle personopplysninger *på vegne av* behandlingsansvarlig i flere sammenhenger.

Følgende personopplysninger vil bli registrert og lagret av databehandler på vegne av behandlingsansvarlig:

- Kontaktdata om kunder, herunder navn, adresse, e-post, telefonnummer, utstedelsesdato for reisekortet, kjøpsdato for billetter og kortnummer
- Reiseopplysninger for kunde, blant annet hvilken sone og holdeplass reisen startet på, billettype, tidspunkt for avlesing av kort mv.
- Lokaliseringsinformasjon for buss med identifiserbar sjåfør
- Eventuelle personopplysninger i passasjertellingssystemet

3.2 Spesielt om billetteringssystemet, Operatørens egenkontroller og frikort

Operatøren vil få tilgang til personopplysninger i billetteringssystemet. Billetteringssystemet eies, driftes og finansieres av Oppdragsgiver. Operatøren skal i henhold til Hovedavtalen utføre oppgjørshåndtering, administrasjon av billettsalg, inntektssikring og kontroll *på vegne av* Oppdragsgiver. Behandling av personopplysninger i billetteringssystemet til disse formålene vil utføres av Operatøren som databehandler for Oppdragsgiver.

Oppdragsgiver ønsker å ha god inntektssikring. Et viktig ledd i dette arbeidet er å forebygge feil billettering og avvik mellom billettsalg og oppgjør for busser som har manuell betaling og kontantoppgjør.
Operatør skal - som en del av denne inntektssikringen - ha rutiner for egenkontroll av billetteringen for å påse korrekt billettering. Partene er enige om at Operatøren i denne sammenheng er behandlingsansvarlig for behandlingen av personopplysningene fra billetteringssystemet, da det er Operatøren som bestemmer formålet med, og virkemidlene i, denne *egen*behandlingen.

Operatøren vil i forbindelse med egenkontrollen kunne behandle følgende personopplysninger fra billetteringssystemet (og andre systemer) som behandlingsansvarlig:

- Bussjåførenes ID-nummer

- Tidspunkt for når sjåføren har vært pålogget billetteringsmaskinen
- Transaksjoner i billettsystemet og avvik i billetteringen, eksempelvis annullering av kjøp
- Opplysninger om eventuelle feil eller mulige straffbare handlinger begått av bussjåførene

Videre vil Operatøren selv være behandlingsansvarlig når Operatøren behandler personopplysninger i forbindelse med utstedelse av frikort. Operatøren vil i denne sammenheng kunne behandle følgende personopplysninger;

- ansattnummer for sjåfør
- navn på sjåfør

Listene oversendes til Oppdragsgiver (som i denne sammenheng er å anse som databehandler for Operatøren).

Videre vil Operatøren være behandlingsansvarlig når Oppdragsgivers kundesenter mottar og videreformidler klager fra kunder (bussreisende) til Operatøren, jf. Hovedavtalens punkt 10.4. Operatøren sammenstiller da opplysninger gitt fra Oppdragsgiver med personopplysninger om egne ansatte i billetteringssystemet. Operatøren bestemmer formålet med, og bruken av, personopplysningene i denne sammenheng, og er å anse som behandlingsansvarlig.

Også andre behandlinger kan være initierte fra databehandlers side, slik at Operatøren/databehandleren er å anse som behandlingsansvarlig. Det vil måtte vurderes konkret i hvert enkelt tilfelle om Operatøren er databehandler eller behandlingsansvarlig. I de tilfeller der Operatøren selv er behandlingsansvarlig, er man utenfor virkeområdet til denne databehandleravtalen. Oppdragsgiver oppfordrer Operatør til å inngå datOppdragsgiverehandleravtale med Oppdragsgiver for disse forhold.

4 Den behandlingsansvarliges (Oppdragsgivers) 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* Oppdragsgiver. 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 gis tilgang til/innsyn i personopplysningene.

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

5 Databehandlerens (Operatørens) plikter

5.1 Formål med behandlingen

Databehandleren behandler personopplysninger *på vegne av* Oppdragsgiver. Operatøren har ikke anledning til å behandle personopplysninger på vegne av Oppdragsgiver for andre formål enn det som er beskrevet i denne avtalen.

Databehandleren skal følge de dokumenterte rutiner og instrukser 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 Oppdragsgiver. Opplysningene kan heller ikke overlates, selges, etc. til andre for lagring, bearbeidelse mv. uten forhåndsaksept av Oppdragsgiver.

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

5.2 Plikt til å treffe egnede tekniske og organisatoriske tiltak

Databehandleren bekrefter at denne vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne avtalen 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 og tilgjengelighet 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 avtalen. 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 vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforodningen kapittel III.

Databehandler er i tillegg ansvarlig for at egen behandling av personopplysninger er i samsvar med personvernlovgivningen, se nærmere under punkt 3.2 i denne avtalen.

5.3 Innsyn og retting av opplysninger

Dersom databehandler mottar forespørsler, herunder krav om innsyn, fra registrerte (Oppdragsgivers kunder) eller fra andre i medhold av personopplysningsloven § 18, skal databehandler videreformidle forespørselen til Oppdragsgiver og bistå behandlingsansvarlig med å besvare slike forespørsler.

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 (Oppdragsgivers kunde).

5.4 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

5.5 Taushetsplikt

Databehandler har taushetsplikt om all dokumentasjon og alle personopplysninger som vedkommende får tilgang til iht. denne avtalen. Databehandleren skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. Taushetsplikten gjelder også *etter* avtalens opphør.

5.6 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.

5.7 Plikt til å føre protokoll

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, underoperatør 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.

6 Bruk av underoperatør/underleverandør

Databehandler forplikter seg til *ikke* å overføre personopplysninger som databehandler behandler på vegne av Oppdragsgiver til tredjepersoner, uten forutgående avtale med Oppdragsgiver. Databehandlers bruk av underoperatør skal avtales skriftlig med Oppdragsgiver før behandlingen starter.

Dersom en 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

avtalen eller i et annet rettslig dokument mellom partene,jf. personvernforordningen artikkel 28 nr. 3.
Det skal inngås egen databehandleravtale mellom databehandler og underoperatør. Databehandleravtalen skal godkjennes av Oppdragsgiver *før* personopplysninger overføres. Dersom nevnte underoperatør 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.

7 Overføring til utlandet

Databehandler har ikke - uten samtykke fra Oppdragsgiver - adgang til å overføre personopplysninger som omfattes av denne avtalen til land og/eller tredjepersoner utenfor EU/EØS som ikke har tilfredsstillende beskyttelsesnivå, jf. personopplysningsforskriftens kap. 6.

8 Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som til enhver tid følger av gjeldende regelverket.. Databehandler skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

(Se Vedlegg 4 til Bransjenormen - Veileder i Informasjonssikkerhet.)

Operatøren skal kunne dokumentere sitt informasjonssystem og sine sikkerhetstiltak. Dokumentasjonen skal - på forespørsel - gjøres tilgjengelig for Oppdragsgiver. Databehandler skal videre bistå, i de tilfeller der dette er relevant, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Databehandleren skal videre oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven med forskrifter samt personvernforordningens artikkel 32.
Databehandleren skal kunne dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal gjøres tilgjengelig på den behandlingsansvarliges forespørsel.

Databehandler må sørge for å ha forsvarlig sikring av servere, databaser og annet tilsvarende utstyr slik at ingen uvedkommende får tilgang til personopplysninger som behandles på vegne av Oppdragsgiver. Det samme gjelder utskrifter og utfylte skjemaer.
Databehandler skal videre ha et styringssystem for sikkerhet iht. personopplysningsforskriften.
Databehandler skal videre etablere og vedlikeholde slike sikkerhetstiltak som risikovurderinger har avdekket behov for.

Oppdragsgiver skal - på forespørsel - gis tilgang til, resultatet av risikovurderinger og sikkerhetsrevisjoner gjennomført av Operatøren.

Avviksmelding etter personopplysningsforskriftens § 2-6 skal skje ved at databehandler umiddelbart melder avviket/sikkerhetsbruddet til Oppdragsgiver. Oppdragsgiver 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 Oppdragsgiver skal kunne ivareta sine forpliktelser

Resultatet av avviksbehandlingen skal dokumenteres.

Databehandleren skal varsle Datatilsynet ved uautorisert utlevering av personopplysninger iht. forordningens artikkel 33.

9 Revisjoner

Behandlingsansvarlig, eller en annen inspektør på fullmakt fra den behandlingsansvarlige, skal jevnlig gjennomføre sikkerhetsrevisjoner og andre relevante revisjoner av databehandler. Oppdragsgiver vil normalt gi minimum 3 dagers varsel før slik revisjon, men forbeholder seg likevel retten til å komme på uanmeldte revisjoner. 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 avtale 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. Det vises til vedlegg 4 til Bransjenormen - «Veileder i Informasjonssikkerhet».

10 Konfidensialitet

Partene skal behandle alle personopplysninger konfidensielt. Ansatte hos databehandler og/eller andre som utfører arbeid for Operatøren, og som har tilgang til personopplysningene, skal signere taushetserklæring som er godkjent av Oppdragsgiver, jf. Hovedavtalen Vedlegg 13.

Tilgang til personopplysningene gis kun etter tjenstlig behov. Signerte taushetserklæringer skal på forespørsel gjøres tilgjengelige for Oppdragsgiver. Taushetsplikten gjelder også *etter* Hovedavtalens og databehandleravtalens opphør.

11 Mislighold

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

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

Databehandler skal holde Oppdragsgiver skadesløs for ethvert tap, kostnad eller ansvar for skade (økonomisk og ikke-økonomisk), herunder også potensielle bøter eller gebyrer, som Oppdragsgiver lider eller blir holdt ansvarlig for som følge av databehandlers (eller databehandlers underoperatørs) brudd på lov, forskrift eller plikter etter denne avtalen. For øvrig gjelder Hovedavtalen punkt 17 om ansvar for Operatøren.

12 Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av Oppdragsgiver, jf. denne avtalen og Hovedavtalen, og frem til alle personopplysninger er tilbakelevert, slettet/destruert, jf. punkt 13 i denne avtalen.

13 Lagring, tilbakeføring og sletting/destruksjon ved opphør

Databehandler skal ikke lagre personopplysninger lenger enn det som følger av avtale med Oppdragsgiver eller for øvrig følger av regelverket, herunder også bransjenorm for elektronisk billettering.

Ved opphør av denne avtalen plikter databehandler etter nærmere instruksjoner fra den behandlingsansvarlige å slette/destruere eller tilbakelevere alle personopplysninger (herunder kopier av personopplysninger) som er behandlet på vegne av Oppdragsgiver og som omfattes av denne avtalen, 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 avtalen eller av Hovedavtalen.

Ved opphør av avtalen skal databehandler videre slette/forsvarlig destruere alle dokumenter, data, disketter, cd-er og annet som inneholder personopplysninger som omfattes av avtalen. Dette gjelder også eventuelle sikkerhetskopier.

Databehandler skal innen 1 måned skriftlig dokumentere at tilbakelevering og/eller sletting /destruksjon er foretatt i henhold til avtalen. Tilbakelevering og/eller sletting /destruksjon skal skje kostnadsfritt for Oppdragsgiver.

14 Kompensasjon

Databehandler skal utføre de forpliktelser som følger av denne avtalen, lov og forskrifter uten kompensasjon, med mindre annet avtales mellom partene.

15 Skriftlige meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til: Eline Walleraunet via anbud@atb.no.

16 Endring i lovverk mv.

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

17 Lovvalg og verneting

Avtalen er underlagt norsk rett, og partene vedtar Sør-Trøndelag tingrett som verneting. Dette gjelder også *etter* opphør av avtalen.

* * *

Denne avtale er i 2 – to – eksemplarer, hvorav partene har hvert sitt.

[Sted og dato]

For Oppdragsgiver (behandlingsansvarlig)	**For Operatør** (databehandler)
…….. [Navn] [Tittel]	…… [Navn] [Tittel]