Versjonsnummer: 2.0

DATABEHANDLERAVTALE

Avtaleteksten må tilpasses hver enkelt tjeneste, prosjekt eller tjenesteleverandør.

mellom

Tromsø kommune

Org.nr.: 940 101 808

Behandlingsansvarlig

og

[Virksomhetens navn]

Org.nr.: 000 000 000

Databehandler

Datert: xx.xx.20xx

1. Om avtalen

Denne databehandleravtalen (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Behandlingsansvarlig og Databehandler (heretter omtalt som "partene") etter gjeldende personvernlovgivning, herunder Lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven) og EUs personvernforordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

Ved motstrid mellom Avtalens regulering og de rammer som følger av personvernforordningen eller annen relevant lovgivningen, viker Avtalens regulering.

Databehandleravtalen erstatter eksisterende databehandleravtale av DD.MM.ÅÅÅÅ.

2. Definisjoner

Begrepene "personopplysninger", "behandling", "behandlingsansvarlig", "databehandler" og "brudd på personopplysningssikkerhet" skal forstås slik de er definert i personvernforordningen artikkel 4.

"Avvik": brudd på personopplysningssikkerhet og bruk av informasjonssystemet i strid med fastlagte rutiner.

3. Avtalens bakgrunn og formål

Denne Avtalen er inngått mellom partene og skisserer de generelle vilkårene for den behandling av personopplysninger som Databehandler utfører på vegne av Behandlingsansvarlig.

Formålet med Avtalen er å sikre behandlingen av personopplysninger på vegne av Behandlingsansvarlig slik at personopplysningene ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjenglighet.

4. Omfang

Denne Avtalen kommer til anvendelse på all behandling av personopplysninger som Databehandler foretar på grunnlag av [*skriv navn på tjeneste/oppdragsavtale*] (heretter omtalt som "Tjeneste/oppdragsavtalen"). I tilfelle konflikt mellom denne Avtalen og Tjeneste/oppdragsavtalen, skal denne Avtalen gjelde.

Tjenester som inngår i denne Avtalen er de tjenester som inngår i Tjeneste/oppdragsavtalen og som innebærer behandling av personopplysninger.

Denne Avtalen vil i tillegg gjelde for ytterligere behandling av personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne Avtalens virksomhetsperiode og som innebærer at Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene").

Personopplysninger skal kun benyttes til de formålene som følger av denne Avtalen, Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene i den utstrekning det er strengt nødvendig for å gjennomføre og imøtekomme kravene i avtalene.

5. Behandlingens formål, opplysninger og behandlinger

Formålet med behandling av personopplysninger er [*husk at hver behandling må være knyttet til spesifikke og uttrykkelig angitt formål*].

XX

Følgende personopplysninger behandles: *[her listes opp hvilke personopplysninger som omfattes – se eksempler nedenfor].*

Vanlige personopplysninger
Navn
Telefonnummer
Fødselsnummer
Bosted
E-postadresser
Sensitive personopplysninger
Rasemessig/etnisk opprinnelse
Religion
Fagforeningsmedlemskap
Helseopplysninger
Biometriske opplysning
Politisk oppfatning
Filosofisk overbevisning
Genetiske opplysninger
Straffbare forhold
Seksuelle forhold/seksuell orentering

Kategorier av registrerte

Følgende kategorier av personer behandles det opplysninger om (registrerte): *[her listes opp hvilke kategorier av registrerte som omfattes – se eksempler nedenfor*

Innbyggere Pasienter Barn Elever Foresatte	Ansatte Tidligere ansatte	Leverandører Ansatte i samarbeidende firma Virksomheter

Behandlingsansvarlig har rett til å bestemme hvilke hjelpemidler som kan benyttes i behandlingen.

Følgende behandlinger omfattes av Avtalen: *[her listes opp hvilke behandlinger av personopplysninger som omfattes – se eksempler nedenfor]*

Behandling	Behandlingsaktiviteter
Innsamling	Databehandler samler inn opplysninger i eget system
Registrering	Innbyggers registreringer Ansattes registreringer
Lagring	Mellomlagring av ikke ferdig utfylt skjema Varig lagring av personopplysninger Lagring i henhold til begrenset lagringstid som angitt i lov/forskrift eller avtale
Strukturering	
Organisering	
Tilpasning eller endring	
Gjenfinning	
Sammenstilling	
Sletting eller tilintetgjøring	
Utlevering	

Nærmere beskrivelse av behandlingen, behandlingens formål og hvilke personopplysninger som omfattes fremgår av Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene [*hvis relevant*].

6. Rammene for behandling av personopplysninger

Databehandleren skal bare behandle personopplysningene basert på dokumenterte instrukser fra den behandlingsansvarlige. Databehandler skal varsle behandlingsansvarlig om instrukser og rutiner som Databehandler mener innebærer brudd på gjeldende lovgivning om behandling av personopplysninger.

Behandlingsansvarlig har til enhver tid full rådighet over de personopplysningene som Databehandler har anledning til å behandle etter denne Avtalen. Databehandler har ikke selvstendig råderett over personopplysningene, og kan ikke behandle disse til egne formål.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysninger som behandles på vegne av Behandlingsansvarlig hos Databehandleren.

7. Behandlingsansvarliges plikter

Behandlingsansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen og annen særlovgivning, samt denne Avtalen.

8. Databehandlers plikter

8.1. Generelt

Databehandler forplikter seg til å behandle personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Behandlingsansvarliges dokumenterte instruksjoner og andre gjeldende avtaler mellom partene. Databehandler skal ikke ved noen handling eller unnlatelse, sette Behandlingsansvarlig i en slik situasjon at Behandlingsansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Databehandler skal ikke:

a. behandle personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;
b. behandle personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;
c. utlevere, overlate eller overføre personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Behandlingsansvarlig eller Behandlingsansvarlig har godkjent dette skriftlig;
d. samle inn fra eller overføre personopplysninger til en tredjepart;
e. behandle personopplysninger de får tilgang eller adgang til gjennom oppdraget fra

Behandlingsansvarlig på annen måte enn hva som er angitt i denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene.

Databehandler skal:

a. ha et internkontrollsystem som dekker alle behandlingsaktiviteter utført på vegne av Behandlingsansvarlig ;
b. gi Behandlingsansvarlig tilgang til og innsyn i personopplysninger som behandles hos Databehandleren;
c. dersom det er påkrevd etter personvernforordningen artikkel 30 (5), føre og vedlikehold en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30(2);
d. treffe alle rimelige tiltak for å sikre at personopplysningene til enhver tid er korrekt og oppdatert;
e. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer;
f. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;
g. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;
h. i rimelig utstrekning og så langt det er mulig, gi Behandlingsansvarlig nødvendig bistand slik at Behandlingsansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;
i. så langt det er mulig og hensyntatt behandlingens art, samarbeide med og bistå Behandlingsansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;
j. omgående underrette den Behandlingsansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;
k. hensyntatt behandlingens art, bistå Behandlingsansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet. Ved vurderinger av personvernkonsekvenser plikter Databehandler å vurdere sikkerhetstiltak som kan bidra til å redusere risikoen behandlingen medfører for de registrerte.

Databehandlerens bistand i forbindelse med ovennevnte skal gjøres kostnadsfritt dersom ikke annet er avtalt.

8.2. Tekniske, organisatoriske og sikkerhetsmessige tiltak

Databehandler plikter å treffe og gjennomføre alle nødvendige og adekvate planlagte og systematiske tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er

tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger.

Databehandleren skal:

a. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personvernforordningen artikkel 32. 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, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;
b. ha gode og hensiktsmessige internkontrollrutiner;
c. ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre oppdraget. Databehandler skal trekke tilbake tilganger dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder for personen;
d. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten blant annet rutiner for avviksmelding, og skal på forespørsel gi Behandlingsansvarlig tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av personopplysninger;
e. avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på personopplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;
f. ved mistanke om eller konstatering av avvik, omgående varsle Behandlingsansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket;
g. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;
h. omgående varsle Behandlingsansvarlig ved uautorisert utlevering av personopplysninger;
i. 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 hos Databehandler, underleverandører og Behandlingsansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;
j. bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs:
   - sikkerhet ved behandlingen;
   - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
   - underretning av den registrerte om brudd på personopplysningssikkerheten;
k. i forbindelse med sikkerhetsrevisjon som utføres av Behandlingsansvarlig eller en tredjepart utpekt av Behandlingsansvarlig, framlegge interne revisjonsrapporter,

interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen. Behandlingsansvarlig eller tredjepart som behandlingsansvarlig utpeker kan utføre tilsyn etter behov eller XX (spesifikt) for å sikre at databehandleravtalen overholdes.

l. varsle Behandlingsansvarlig om alle forhold som medfører endring i risikobildet for behandling av personopplysningene;

m. innhente godkjenning av Behandlingsansvarlig før gjennomføring av enhver endring av databehandlingen hos Databehandler som har eller kan ha betydning for informasjonssikkerheten.

Nærmere krav til Databehandlerens informasjonssikkerhet er angitt i **Vedlegg 1** hvis relevant. Dersom kravene er dekket av kravspec eller annen avtale, kan vedlegg 1 utelates.

Ved brudd på denne Avtalen eller på bestemmelsene i forordningen eller personopplysningsloven eller annen relevant lovgivning kan Behandlingsansvarlig kreve endringer i behandlingsmåten eller pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Behandlingsansvarlig.

9. Bruk av underleverandør

Behandlingsansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter underleverandører som angitt i **Vedlegg 2** for de der angitte tjenester og bekrefter at det er ingen andre underleverandører som benyttes. Databehandler skal ikke engasjere andre underleverandører enn de som er nevnt i Vedlegg 2 uten at dette på forhånd er skriftlig godkjent av Behandlingsansvarlig.

Databehandler skal:

a. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under Avtalen og gjeldende lovgivning;

b. sørge for at underleverandører kun behandler personopplysninger i samsvar med denne Avtalen og ikke i større utstrekning enn det som er nødvendig for å oppfylle den aktuelle tjenesten som underleverandøren leverer;

c. holde en oppdatert liste over identiteten og stedlig plassering av underleverandører som angitt i **Vedlegg 2**;

d. gjennomføre en risikovurdering av bruk av underleverandør og betydningen for tjenesten før det inngås avtale med underleverandør og på Behandlingsansvarliges forespørsel, dele vurderingen med Behandlingsansvarlig;

e. på Behandlingsansvarliges forespørsel, legge frem kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile betingelser). Slike avtaler skal senest være inngått før underleverandørene starter med behandling av personopplysninger;

f. underrette Behandlingsansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Slike bytter skal varsles i god tid slik at Behandlingsansvarlig gis mulighet til å motsette seg endringen. Ved bytte av underleverandør skal **Vedlegg 2** oppdateres og oversendes Behandlingsansvarliges kontaktperson. Oppdatert liste dateres og undertegnes av begge parter;

g. sikre at Behandlingsansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Behandlingsansvarlig har overfor Databehandler etter Avtalens punkt 12;

h. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å slette eller forsvarlig destruere alle personopplysninger personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene som framgår av Avtalens punkt 13 på samme måte som Databehandler så langt det ikke strider mot andre lovbestemmelser.

Databehandler er til enhver tid fullt ut ansvarlig overfor Behandlingsansvarlig for alt arbeid som utføres av underleverandører og for underleverandørenes etterlevelse av bestemmelsene i denne Avtalen.

Tilgang til personopplysninger for tredjeparter krever konkret avtale utover denne Avtalen mellom partene for alle andre enn Databehandlers underleverandører.

10. Overføring av personopplysninger til utlandet

Hovedregelen er at ingen av personopplysningene som behandles under denne Avtalen skal føres ut av Norge. I tillegg skal personopplysninger være plassert på servere i Norge. Eventuelle unntak som innebærer overføring til utlandet skal godkjennes skriftlig av Behandlingsansvarlig før behandlingen starter.

Databehandler bekrefter at ingen av underleverandørene overfører personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer som er angitt i **Vedlegg 2**. Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Behandlingsansvarlig på forhånd. Ved overføring av personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.

Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Databehandler gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Behandlingsansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Behandlingsansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Behandlingsansvarliges egen risikovurdering.

11. Taushetsplikt

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne Avtalen, Tjeneste/oppdragsavtale og senere skriftlige avtaler mellom partene (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), er underlagt taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle

underleverandører.

Databehandler skal påse at alle som behandler personopplysninger under Avtalen er kjent med taushetsplikten.

Ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet, som er formidlet i forbindelse med oppdraget, herunder konfidensiell informasjon Behandlingsansvarlig eller tredjepart får tilgang til i forbindelse med revisjon etter Avtalens punkt 12.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

Taushetsplikten gjelder også etter Avtalens opphør.

12. Innsyn, verifikasjon og revisjon

Behandlingsansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Databehandlers behandling av personopplysninger tilhørende Behandlingsansvarlig, herunder innsyn i og verifikasjon av dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Databehandler på vegne av Behandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov. Hvis Behandlingsansvarlig ber om innsyn skal generell informasjon fra revisjonen gjøres tilgjengelig for andre behandlingsansvarlige som benytter samme tjeneste hos Databehandler.

Behandlingsansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Behandlingsansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere behandlingsansvarlige som får levert tjenester fra Databehandler. Innsyn og kontroll kan gjennomføres av Behandlingsansvarlig eller tredjepart som Behandlingsansvarlig utpeker. Databehandler kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet tilgang og innsyn i behandlingen av personopplysninger slik det følger av relevant lovgivning.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Behandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

13. Varighet og opphør

Denne Avtalen gjelder fra den er signert av partene og gjelder til Avtalen og alle gjeldende avtaler mellom partene, som innebærer at Databehandler skal behandle personopplysninger på vegne av Behandlingsansvarlig, er opphørt.

Ved opphør av Avtalen skal Databehandler tilrettelegge for og medvirke til tilbakeføring av alle opplysninger som Databehandler har mottatt og behandlet på vegne av Behandlingsansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til Behandlingsansvarlig og bekreftet mottatt av denne, skal Databehandler irreversibelt slette eller forsvarlig destruere alle opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre ufravikelige rettsregler krever at personopplysningene fortsatt lagres.

Benyttes delt infrastruktur der direkte sletting ikke er teknisk mulig skal Databehandler sørge for at data gjøres utilgjengelig inntil disse dataene er overskrevet av systemet. Databehandlerens bistand i forbindelse med ovennevnte skal gjøres kostnadsfritt dersom ikke annet er avtalt.

Databehandler skal gi Behandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

14. Endring av avtale

I tilfelle endringer i gjeldende lovverk, endelig dom som gir en annen tolkning av gjeldende lov, eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

15. Meddelelser

Meddelelser, underretting, varsel eller annen kommunikasjon mellom Behandlingsansvarlig og Databehandler skal gis skriftlig, eller bekreftes skriftlig til:

Behandlingsansvarlig	**Databehandler**
Tromsø kommune	**[Virksomhetens navn]**
Att. Navn: Rolle: E-post:	Att: Navn: Rolle: E-post:

16. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Nord-Troms tingrett som verneting. Dette gjelder også etter opphør av Avtalen.

17. Undertegning

Denne Avtalen foreligger i to originaler, hvorav partene beholder et eksemplar hver.

Sted og dato: XX, XX.XX.XX

På vegne av Behandlingsansvarlig

På vegne av Databehandler

…….. ……

(underskrift) (underskrift)

VEDLEGG 1 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET

Databehandler har en selvstendig plikt til å gjennomføre egnede sikkerhetstiltak etter artikkel 32. Følgende opplistede er krav som må oppfylles [her listes opp detaljerte krav til informasjonssikkerhet – se eksempler nedenfor]

Nr	**Krav**	**Ja/Nei/IR** (angi IR hvis kravet ikke er relevant i denne sammen-heng)	**Databehandlers beskrivelse** Utdyp kort hvorfor det er svart Ja eller Nei. Hvis det refereres til andre dokumenter må referansen være nøyaktig mht dokument, sidenr, avsnitt, URL, etc.
1	Har databehandler inngående kunnskap om, og opptrer databehandler i henhold til, alle relevante punkter i GDPR (personvernforordningen)?		
2	Har databehandler et levende styringssystem (ISMS) for informasjons-sikkerhet, basert på god praksis som f.eks. angitt i ISO27001/2?		
3	Er ansvar og oppgaver for informasjonssikkerhet dokumentert i et organisasjonskart?		
4	Er ansvar og oppgaver beskrevet på alle nivåer?		
5	Er ansvarsforholdene gjort kjent for alle i organisasjonen?		
6	Er alle sikkerhetstiltak dokumentert (organisatoriske, fysiske og tekniske)?		
7	Er sikkerhetsmål for virksomheten fastsatt?		
8	Er sikkerhetsstrategi for å nå sikkerhetsmålene utarbeidet?		
9	Er det utarbeidet rutiner for gjennomføring av risikovurderinger, inkludert oppfølging av tiltak?		
10	Er alle medarbeidere informert om sin taushetsplikt og klar over dens innhold og omfang?		
11	Er konsekvenser ved brudd på taushetsplikten		

	beskrevet?		
12	Gjennomføres det sikkerhetsrevisjon jevnlig og minimum årlig?		
13	Dekker sikkerhets-revisjonen minimum:		
	a) Plassering av ansvar og organisering av sikkerhetsarbeidet		
	b) Kvalitet på sikkerhetsmål og sikkerhetsstrategi		
	c) Overholdelse av prosedyrer for bruk av informasjons-systemer og person-opplysninger		
	d) Resultat av opplæring		
	e) Forvaltning og bruk av person-opplysninger		
	f) Tilgang til person-opplysninger og tiltak mot uautorisert innsyn?		
	h) Effekten av etablerte sikkerhetstiltak?		
	i) Ivaretakelse av informasjons-sikkerhet hos kommunikasjons-partnere, databehandlere og leverandører?		
14	Er det etablert prosedyre for oppfølging av resultatet (avvik) av sikkerhetsrevisjoner?		
15	Er alle medarbeidere klar over ansvaret de har for å		

	melde avvik?		
16	Er det etablert prosedyre som sikrer at Databehandlingsansvarlig varsles umiddelbart ved uautorisert utlevering eller endring av personopplysninger, eller andre sikkerhetsbrudd?		
17	Gjennomføres og dokumenteres ledelsens gjennomgang av sikkerheten minimum årlig?		
18	Er det iverksatt tiltak for å hindre at teknisk personell misbruker sin autorisasjon?		
19	Er det etablert prosedyre for administrasjon av nøkler/adgangskort i adgangskontrollsystemet?		
20	Er det iverksatt tekniske og organisatoriske tiltak for sikker tilgang fra ikke-sikrede lokaler (som f.eks. hjemmekontor, og via mobilt utstyr)?		
21	Er det etablert sikkerhetstiltak slik at kun autorisert personell får adgang til driftsutstyr (servere, nettverksutstyr, SAN, backupmedia med mer)?		
22	Er det utarbeidet konfigurasjonskart over informasjonssystemene?		
23	Er det utarbeidet teknisk beskrivelse av konfigurasjonen?		
24	Er kommunens data separert fra andre kunders data?		
25	Har løsningen tilstrekkelig kapasitet, uavhengig av den totale lasten leverandør har fra andre kunder		
26	Har leverandøren beredskapsplaner for bortfall av løsning?		
27	Har databehandler forsvarlige backup- og restore-rutiner som testes		

	regelmessig?		
28	Har leverandøren gjennomført tekniske eller organisatoriske tiltak mot hacking?		
29	Gjøres det regelmessig penetrasjonstester for å avdekke svakheter?		
30	Har databehandler forsvarlige rutiner for autorisering og autentisering av brukere?		
31	Har databehandler tekniske tiltak mot tjenestenektangrep?		
32	Har databehandler gode løsninger for logging og sporbarhet?		
33	Benytter databehandler egne «dummy» testdata?		
34	Krypteres data ved lagring?		
35	Krypteres data i transit (kommunikasjon)?		
36	Har løsningen mulighet for å gi kommunen tilgang til logger, samt fortløpende eksportere loggdata til kommunens SIEM løsning?		
37	Ved bruk av IoT devices, har leverandøren et godt regime for bruk av sterke passord, og regelmessig endring av disse?		

VEDLEGG 2 – UNDERLEVERANDØRER

[her listes opp hvilke underleverandører som benyttes av Databehandler – se eksempler nedenfor]

Navn på underleverandør	Virksomhetstype/tjeneste som leveres	Stedlig plassering
ABC	Databehandlers datasenter, hosting	Stockholm
XYZ	Tredjepart leverandør, IT-supporttjenester	Paris