



Databehandleravtale med Bilag

Er inngått mellom:

<Angi navn på virksomhet og organisasjonsnummer>
(heretter kalt Databehandler)

og

<Angi navn på virksomhet og organisasjonsnummer>
(heretter kalt Behandlingsansvarlig)

i fellesskap kalt Partene.

Sted og dato:

Avtalen er signert elektronisk i [sett inn navn på konkurransejennomførings- eller kontraktsoppfølgingsverktøy]

Avtaleparter

[Navn på den som signerer på vegne av Behandlingsansvarlig]

[Navn på den som signerer på vegne av Databehandler]

Eller: For Behandlingsansvarlig	For Databehandler
<Navn på den som signerer på vegne av Behandlingsansvarlig> _____ Underskrift	<Navn på den som signerer på vegne av Databehandler> _____ Underskrift

Avtalen undertegnes i to eksemplarer, ett til hver part.

**INNHALDSFORTEGNELSE:**

1	Formålet med denne Databehandleravtalen	3
2	Definisjoner	3
3	Behandlingsansvarliges plikter og rettigheter	4
4	Behandlingsansvarliges instruks til Databehandleren	4
5	Konfidensialitet og taushetsplikt.....	5
6	Bistand til Behandlingsansvarlig.....	5
7	Sikkerhet ved behandlingen.....	6
8	Melding om brudd på personopplysningssikkerheten	6
9	Bruk av Underdatabehandler	7
10	Overføring av personopplysninger til land utenfor EØS-området	8
11	Generelt om revisjon	9
12	Sletting og tilbakelevering av opplysninger.....	9
13	Mislighold og pålegg om stans	10
14	Varighet og opphør.....	10
15	Lovvalg og verneting.....	10
A.	Opplysninger om behandlingen.....	12
B.	Betingelser for Databehandlerens bruk og endring av eventuelle Underdatabehandlere.....	14
C.	Instruks vedrørende behandling av personopplysninger	16
D.	troms fylkeskommunes RETNINGSLINJE FOR LEVERANDØRSTYRING	20
E.	ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST og ENDRINGER ETTER AVTALEINNGÅELEN	23



1 Formålet med denne Databehandleravtalen

- 1.1 Denne avtalen ("Databehandleravtalen») fastsetter partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige som del av leveransene under Hovedavtalen. Databehandleravtalen har som formål å sikre at partene etterlever Gjeldende personvernregler.

Databehandleravtalen består av dette dokumentet, samt Bilag A, B, C, D og E.

- 1.2 Ved motstrid mellom Hovedavtalen og Databehandleravtalen, har Databehandleravtalen forrang når det gjelder forhold spesifikt knyttet til behandling av personopplysninger. Ved motstrid mellom Databehandleravtalen og dens bilag, har bilagene forrang.
- 1.3 Databehandleravtalens **Bilag A** inneholder nærmere beskrivelse av behandlingen som skal foretas, herunder om behandlingsformål, kategorier av personopplysninger og registrerte, regler for sletting og tilbakelevering, partenes kontaktpersoner, samt hvilken eller hvilke underliggende avtaler behandlingen av personopplysninger er knyttet til (se definisjonen av Hovedavtalen nedenfor).
- 1.4 Databehandleravtalens **Bilag B** inneholder betingelser for bruk av Underdatabehandlere, samt en oversikt over godkjente Underdatabehandlere.
- 1.5 Databehandleravtalens **Bilag C** inneholder spesifikke instruksjoner for behandling av personopplysninger under Hovedavtalen, herunder sikkerhetstiltak og Behandlingsansvarliges rett til innsyn og revisjon av Databehandler og eventuelle Underdatabehandlere, samt sektorspesifikke bestemmelser om behandling av personopplysninger.
- 1.6 Databehandleravtalens **Bilag D** inneholder Troms fylkeskommune sin retningslinje for leverandørstyring, som stiller krav til fylkeskommunens leverandører om ivaretagelse av informasjonssikkerhet og personvern, og skal gi anbefalte sikkerhetskrav for anskaffelse og forvaltning.
- 1.7 Databehandleravtalens **Bilag E** inneholder endringer til standardteksten og eventuelle senere avtalte endringer i Databehandleravtalen.

2 Definisjoner

Gjeldende personvernregler: Den til enhver tid gjeldende versjon av EUs personvernforordning (2016/679) ("personvernforordningen"), samt lov om behandling av personopplysninger av 15.06. 2018 (personopplysningsloven) med tilhørende forskrifter mv., samt eventuell annen relevant lovgivning som gjelder behandling og vern av personopplysninger og som er angitt i Bilag C, punkt C.7.

Hovedavtalen: En eller flere avtaler mellom Behandlingsansvarlig og Databehandler om levering av tjenester som innebærer behandling av personopplysninger, som nærmere angitt i Bilag A. Databehandleravtalen kan gjelde flere underliggende avtaler.

Underdatabehandler: Annen virksomhet som benyttes av Databehandler som underleverandør til behandling av personopplysninger under Hovedavtalen.

For personvernbegreper som ikke er definert i denne Databehandleravtalen gjelder definisjonene i personvernforordningen artikkel 4.

3 Behandlingsansvarliges plikter og rettigheter

Behandlingsansvarlige har ansvaret for at behandlingen av personopplysninger skjer i samsvar med Gjeldende personvernregler. Behandlingsansvarlige skal i den forbindelse særskilt sørge for at:

- i. behandlingen av personopplysninger er formålsbestemt og basert på et gyldig rettsgrunnlag;
- ii. de registrerte har mottatt nødvendig informasjon om behandlingen av personopplysningene;
- iii. Behandlingsansvarlig har gjennomført tilstrekkelige risikovurderinger; og
- iv. Databehandler til enhver tid har tilstrekkelige instruksjoner og informasjon for å oppfylle sine plikter i henhold til Databehandleravtalen og Gjeldende personvernregler.

4 Behandlingsansvarliges instruksjoner til Databehandleren

- 4.1 Databehandleren skal behandle personopplysningene i samsvar med Gjeldende personvernregler og den Behandlingsansvarliges dokumenterte instruksjoner, jf. punkt 4.2. Hvis annen behandling er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, skal Databehandleren underrette den Behandlingsansvarlige så langt dette er tillatt ved lov, jf. personvernforordningen artikkel 28 (3) (a).
- 4.2 Behandlingsansvarliges instruksjoner fremgår av Hovedavtalen og Databehandleravtalen med bilag. Databehandler skal omgående underrette den Behandlingsansvarlige, dersom vedkommende mener at instruksene er i strid med Gjeldende personvernregler, jf. personvernforordningen artikkel 28 (3) (h).
- 4.3 Eventuelle endringer i instruksjoner skal varsles til Databehandler gjennom oppdatering av Bilag E, og skal implementeres av Databehandler innen det tidspunkt Partene avtaler eller, om ingen konkret frist er avtalt, innen rimelig tid. Databehandler kan kreve at Behandlingsansvarlig dekker dokumenterte kostnader som påløper i forbindelse med implementeringen av slike endringer eller forholdsmessig justering av vederlaget under Hovedavtalen dersom den endrede instruksjonen innebærer løpende ekstra kostnader for



Databehandleren. Det samme gjelder merkostnader som følge av endring av Gjeldende personvernregler som gjelder den Behandlingsansvarliges virksomhet.

5 Konfidensialitet og taushetsplikt

- 5.1 Databehandleren skal sikre at ansatte og andre som har tilgang til personopplysninger er autorisert til å behandle slike personopplysninger på Databehandlers vegne. Dersom slik autorisasjon utløper eller trekkes tilbake, skal tilgangen til personopplysningene opphøre uten ugrunnet opphold.
- 5.2 Databehandleren skal kun autorisere personer som trenger tilgang til personopplysningene i forbindelse med arbeid for å kunne oppfylle Hovedavtalen, Databehandleravtalen og eventuelt annen behandling som er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, se punkt 4 siste setning.
- 5.3 Databehandleren skal sikre at personer som er autorisert til å behandle personopplysninger på vegne av den Behandlingsansvarlige er underlagt taushetsplikt gjennom avtale eller lov. Taushetsplikten skal bestå også etter avtalens og/eller ansettelsesforholdets opphør.
- 5.4 Databehandleren skal kunne dokumentere at de relevante personer er underlagt ovennevnte taushetsplikt på forespørsel fra den Behandlingsansvarlige.
- 5.5 Ved opphør av Databehandleravtalen plikter Databehandleren å avvikle alle tilganger til personopplysninger som behandles under avtalen.

6 Bistand til Behandlingsansvarlig

- 6.1 Databehandleren skal på forespørsel bistå Behandlingsansvarlig med oppfyllelse av de registrertes rettigheter etter personvernforordningens kapittel III gjennom egnede tekniske eller organisatoriske tiltak. Plikten til å bistå gjelder likevel bare i den utstrekning dette er mulig og hensiktsmessig sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.
- 6.2 Databehandler skal uten ugrunnet opphold videresende alle henvendelser som Databehandler eventuelt mottar fra den registrerte vedrørende den registrertes rettigheter i henhold til Gjeldende personvernregler til Behandlingsansvarlig. Slike henvendelser kan kun besvares av Databehandler når dette er skriftlig godkjent av Behandlingsansvarlig.
- 6.3 Databehandleren skal bistå den Behandlingsansvarlige med å overholde kravene til personopplysningssikkerhet i personvernforordningen artikkel 32-36, herunder yte bistand ved personvernkonsekvensvurdering og forhåndsdrøftinger med Datatilsynet, sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.



- 6.4 Hvis Databehandler på Behandlingsansvarliges forespørsel yter bistand som nevnt i punkt 6.1 eller 6.3, og bistanden går ut over det som er nødvendig for at Databehandleren skal oppfylle sine egne forpliktelser etter Gjeldende personvernregler, kan Databehandler kreve dekket sine dokumenterte kostnader knyttet til bistanden. Arbeid dekkes i henhold til prisbestemmelsene i Hovedavtalen.

7 Sikkerhet ved behandlingen

- 7.1 Databehandler skal iverksette egnede tekniske og organisatoriske tiltak for å oppnå et tilfredsstillende sikkerhetsnivå sett hen til behandlingens karakter og omfang, den tekniske utviklingen, implementeringskostnader og aktuelle risikoer for fysiske personers rettigheter og friheter. Databehandleren skal som minimum iverksette de tiltak som er spesifisert i Databehandleravtalens Bilag C.
- 7.2 Databehandleren skal foreta risikovurderinger for å sikre at et egnet sikkerhetsnivå opprettholdes til enhver tid. Databehandleren skal herunder sørge for jevnlig testing, analyse og vurdering av sikkerhetstiltakene, særlig med hensyn til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester, samt evne til raskt å gjenopprette tilgjengeligheten av personopplysningene ved hendelser.
- 7.3 Databehandler skal dokumentere risikovurderingen og sikkerhetstiltakene, og gjøre dem tilgjengelig for Behandlingsansvarlige på forespørsel, samt gi adgang til slik revisjon som er avtalt mellom partene, jf. Databehandleravtalens punkt 11.

8 Melding om brudd på personopplysningssikkerheten

- 8.1 Databehandler skal uten ugrunnet opphold skriftlig underrette den Behandlingsansvarlige om eventuelle brudd på personopplysningssikkerheten, samt for øvrig gi slik bistand og informasjon som er nødvendig for at den Behandlingsansvarlige skal kunne melde bruddet til tilsynsmyndigheter i tråd med Gjeldende personvernregelverk.
- 8.2 Underretning etter punkt 8.1 skal meddeles kontaktpunktet for Behandlingsansvarlig i henhold til Bilag C punkt C.9, og skal:
- beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
 - inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,
 - beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten, og
 - beskrive de tiltak som Databehandleren har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.



Informasjonen kan i den grad det det er nødvendig gis trinnvis uten ytterligere ugrunnet opphold.

- 8.3 Databehandler plikter å gjennomføre alle de tiltak som med rimelighet kan kreves for å utbedre og unngå tilsvarende brudd på personopplysningssikkerheten. Databehandler skal, så langt det er mulig, rådføre seg med Behandlingsansvarlig om de tiltak som skal gjennomføres, herunder vurdere Behandlingsansvarliges eventuelle forslag til tiltak.
- 8.4 Behandlingsansvarlig er ansvarlig for å underrette Datatilsynet og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandler skal ikke informere tredjeparter om brudd på personopplysningssikkerheten med mindre noe annet er påkrevd etter gjeldende rett eller det følger av uttrykkelig skriftlig instruks fra Behandlingsansvarlig.

9 Bruk av Underdatabehandler

- 9.1 Databehandler kan kun benytte Underdatabehandler etter forutgående generell eller spesifikk skriftlig tillatelse fra Behandlingsansvarlig i samsvar med Databehandleravtalens Bilag B. Oversikt over godkjente Underdatabehandlere fremgår av Databehandleravtalens Bilag B.
- 9.2 Dersom en Databehandler engasjerer en Underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Behandlingsansvarlige, plikter Databehandler å inngå skriftlig avtale med Underdatabehandleren som pålegger denne tilsvarende forpliktelser med hensyn til vern av personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen. Se punkt 9.7 med hensyn til bruk av standard tredjepartstjenester.
- 9.3 Databehandler skal kun engasjere Underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene etter Gjeldende personvernregler. Databehandler skal gjennomføre kontroller av Underdatabehandlere for å verifisere at tilfredsstillende tiltak er iverksatt. Databehandler skal kunne fremlegge rapporter fra slike kontroller for Behandlingsansvarlig på forespørsel.
- 9.4 Dersom Behandlingsansvarlig motsetter seg endringer i bruken av Underdatabehandlere etter Databehandleravtalens Bilag B punkt B.1 skal Partene i god tro forhandle med sikte på å enes om en rimelig løsning på hvordan videre levering av tjenestene under Hovedavtalen skal gjennomføres, herunder om fordeling av eventuelle kostnader mellom Partene. Endringen i bruk av Underdatabehandlere kan ikke gjennomføres før Partene har kommet til enighet.
- 9.5 Dersom Underdatabehandleren ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar på samme måte som om Databehandler selv sto for behandlingen.



- 9.6 Databehandler plikter å forelegge avtaler med Underdatabehandlere for Behandlingsansvarlig på forespørsel. Dette gjelder likevel bare de delene av avtalen som er relevant for behandlingen av personopplysningene og med de begrensninger som eventuelt måtte følge av lov eller forskrift. Rent kommersielle vilkår kan uansett ikke kreves fremlagt.
- 9.7 I den utstrekning Databehandleren benytter underleverandør som leverer standardiserte tredjepartstjenester som Behandlingsansvarlig uttrykkelig har akseptert at leveres på underleverandørens standardvilkår i henhold til Hovedavtalen, og som Databehandleren følger opp på Behandlingsansvarliges vegne, kan partene bli enige om at underleverandørens standard databehandleravtale legges til grunn og gjøres gjeldende direkte overfor Behandlingsansvarlig som et direkte databehandlerforhold (altså ikke som Underdatabehandler) forutsatt at den oppfyller kravene i Gjeldende personvernregler. Databehandleren skal følge opp databehandleravtalen med underleverandøren på vegne av Behandlingsansvarlig med mindre annet er avtalt i det enkelte tilfellet.
- ## 10 Overføring av personopplysninger til land utenfor EØS-området
- 10.1 Personopplysninger kan bare overføres til et land utenfor EØS-området ('Tredjestat') eller til internasjonal organisasjon hvis Behandlingsansvarlig skriftlig har godkjent slik overføring og vilkårene i punkt 10.3 er oppfylt. Som overføring regnes blant annet å:
- a) behandle personopplysningene i datasentre o.l. som er lokalisert i Tredjestat eller av personell som er lokalisert i Tredjestat (ved fjerntilgang);
 - b) overlate behandlingen av personopplysninger til Underdatabehandler i Tredjestat; eller
 - c) utlevere personopplysningene til en Behandlingsansvarlig i Tredjestat eller i en internasjonal organisasjon.
- 10.2 Databehandler kan likevel overføre personopplysninger dersom det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandler underrette Behandlingsansvarlig så langt dette er tillatt ved lov.
- 10.3 Overføring til Tredjestater eller internasjonale organisasjoner kan kun finne sted dersom det foreligger nødvendige garantier for et tilstrekkelig beskyttelsesnivå for personvern i henhold til Gjeldende personvernregler. Med mindre annet er avtalt mellom Partene kan slik overførsel kun finne sted med grunnlag i:
- a) en av EU-kommisjonens beslutninger om tilstrekkelig beskyttelsesnivå i henhold til personvernforordningen artikkel 45; eller
 - b) en Databehandleravtale som inkorporerer standard personvernbestemmelser som angitt i personvernforordningen artikkel 46 (2) (c) eller (d) (EU Model clauses); eller
 - c) bindende virksomhetsregler (Binding Corporate Rules) i henhold til personvernforordningen artikkel 47.



- 10.4 Den Behandlingsansvarliges eventuelle godkjenning av at personopplysninger overføres til en Tredjestat eller internasjonal organisasjon skal fremgå av Databehandleravtalens Bilag B.

11 Generelt om revisjon

- 11.1 Databehandler skal på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige, all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i personvernforordningen artikkel 28 og denne Databehandleravtalen er oppfylt.
- 11.2 Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved inspeksjoner fra aktuelle tilsynsmyndigheter. Den Behandlingsansvarliges tilsyn med eventuelle Underdatabehandler skal skje gjennom Databehandleren med mindre annet er særskilt avtalt. Nærmere rutiner for gjennomføring av revisjoner fremgår av bilag C punkt C.5.
- 11.3 Dersom en revisjon avdekker avvik fra forpliktelsene i Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler så snart som mulig utbedre avviket. Behandlingsansvarlig kan kreve at Databehandleren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Behandlingsansvarlig.
- 11.4 Hver av Partene dekker sine egne kostnader forbundet med en årlig revisjon. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandleren likevel dekke Behandlingsansvarliges rimelige kostnader forbundet med revisjonen.

12 Sletting og tilbakelevering av opplysninger

- 12.1 Ved opphør av denne Databehandleravtalen plikter Databehandler å tilbakelevere og slette alle personopplysninger som behandles på vegne av Behandlingsansvarlig under Databehandleravtalen i samsvar med bestemmelsene i Bilag C punkt C.6. Dette gjelder også eventuelle sikkerhetskopier.
- 12.2 Behandlingsansvarlig bestemmer hvordan en eventuell tilbakelevering av personopplysninger skal skje. Behandlingsansvarlig kan kreve tilbakelevering skjer på et strukturert og alminnelig anvendt maskinlesbart format. Behandlingsansvarlig skal dekke Databehandlerens dokumenterte kostnader til tilbakelevering med mindre dette er inkludert i vederlaget under Hovedavtalen.
- 12.3 Hvis det benyttes delt infrastruktur eller backup der direkte sletting ikke er teknisk mulig, skal Databehandler sørge for at personopplysningene gjøres utilgjengelige inntil de er overskrevet.



12.4 Databehandler skal bekrefte skriftlig overfor Behandlingsansvarlig at sletting eller utilgjengeliggjøring er foretatt og skal på forespørsel dokumentere hvordan det er gjennomført.

12.5 Nærmere bestemmelser om sletting og tilbakeleveringer fremgår av bilag C.

13 Mislighold og pålegg om stans

13.1 Ved brudd på Databehandleravtalen og/eller Gjeldende personvernregler, kan Behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge Databehandler å stoppe hele eller deler av behandlingen av opplysningene med øyeblikkelig virkning.

13.2 Dersom Databehandler ikke overholder sine plikter i henhold til denne Databehandleravtale og/eller Gjeldende personvernregler, vil dette anses som mislighold av Hovedavtalen, og de plikter, frister, sanksjoner og ansvarsbegrensninger som følger av Hovedavtalens regulering av Leverandørens mislighold kommer til anvendelse, med mindre annet er uttrykkelig avtalt mellom partene i Bilag E.

14 Varighet og opphør

14.1 Databehandleravtalen gjelder fra den er signert av begge Parter. Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig. Den gjelder også for eventuelle personopplysninger som måtte finnes hos Databehandler eller noen av dennes Underdatabehandler etter Hovedavtalens opphør.

14.2 Reglene om oppsigelse i Hovedavtalen gjelder tilsvarende for Databehandleravtalen, så langt det passer. Databehandleravtalen kan ikke sies opp så lenge Hovedavtalen består med mindre den avløses av en ny databehandleravtale.

15 Lovvalg og verneting

Avtalen er underlagt norsk rett. Tvister løses i samsvar med Hovedavtalens bestemmelser, herunder eventuelle bestemmelser om verneting.



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 – TROMS FYLKESKOMMUNE SIN RETNINGSLINJE FOR
LEVERANDØRSTYRING**

**BILAG E - ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST
OG ENDRINGER ETTER AVTALEINNGÅElsen**

A. OPPLYSNINGER OM BEHANDLINGEN

A.1. Hovedavtalen og formålet med behandlingen av personopplysninger

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige er knyttet til å levere tjenester som beskrevet i Hovedavtalen.

Med Hovedavtalen menes følgende avtale(r) inngått mellom partene:

<Sett inn navn og dato for inngåelse av den eller de underliggende tjenesteavtalen(e) som Databehandleravtalen er knyttet til.>

<Merknad: Hvis det er flere tjenesteavtaler som benytter samme databehandleravtale kan de angis samlet her eller det kan utarbeides et bilagssett for hver avtale, avhengig av om behandlingens art og omfang, og graden av ensartethet på den behandlingsansvarliges instruks, er slik at det mest hensiktsmessig beskrives samlet eller hver for seg.>

Behandlingen har følgende formål:

<Beskriv behandlingsformål, for eksempel:

- Analyse av brukertilfredshet i prosjekt X, som nærmere beskrevet i Hovedavtalens Bilag 1 (om SSA benyttes)
- Levering av skylagringstjenester som nærmere beskrevet i Hovedavtalens Bilag 1 (om SSA benyttes)
- Bruk av system X til innsamling og behandling av opplysninger om Behandlingsansvarliges ansatte>
- Bruk av system Y til håndtering av søknader om skoleskyss

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

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

<Beskriv hva behandlingen omfatter, for eksempel:

- Innsamling, lagring og analyse av brukertilfredshetsundersøkelser som beskrevet i Hovedavtalens Bilag 1
- Registrering, organisering og oppbevaring av personopplysninger i system X>
- Lagring av data, inkludert personopplysninger, i system Y

A.3. 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: <Angi type, f.eks. navn og kontaktinformasjon, utdanning, kommunikasjonspreferanser osv.>

A.4. Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

<Beskriv hvem behandlingen av personopplysninger omfatter, for eksempel: «Innbyggere i Troms fylkeskommune», "Brukere av skolefritidsordningen" eller "Ansatte og konsulenter i Troms fylkeskommune".

Dersom det behandles opplysninger om en særlig sårbar eller utsatt gruppe som f.eks. barn eller handikappede skal det oppføres særskilt.>

A.5. Varighet av behandlingen

Databehandlers behandling av personopplysninger under Hovedavtalen kan påbegynne når Databehandleravtalen har trådt i kraft. Behandlingen har følgende varighet (velg ett alternativ):

☐	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. databehandlerens bruk av underdatabehandlere



B. BETINGELSER FOR DATABEHANDLERENS BRUK OG ENDRING AV EVENTUELLE UNDERDATABEHANDLERE

B.1. Behandlingsansvarliges godkjenning av bruk av Underdatabehandlere

Ved inngåelse av Databehandleravtalen godkjenner Behandlingsansvarlig bruk av de Underdatabehandlere som er oppført i punkt 0. 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 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 godkjenning fra Behandlingsansvarlig. Underdatabehandleren kan ikke behandle personopplysninger under Hovedavtalen før slik godkjenning er gitt. Godkjenning kan ikke nektes uten saklig grunn.

<Merknad: Hvis Databehandler benytter underleverandør (tredjepart) som leverer standardiserte tredjepartstjenester (typisk skytjenester), og som oppfyller vilkårene i Databehandleravtalen punkt 9.7, slik at tredjepartens standard databehandleravtale kommer til anvendelse direkte overfor den behandlingsansvarlige, vil skifte av underleverandør hos tredjeparten følge bestemmelsene i tredjepartens databehandleravtale.>



B.2. Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere:

Navn	Org.nr.	Adresse	Beskrivelse av behandling	Behandlingssted	Kontaktinformasjon	Særlige kategorier personopplysninger
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	[Angi om det behandles særlige kategorier av personopplysninger]
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]	[Kontaktinformasjon]	

Databehandleren kan ikke bruke den enkelte Underdatabehandleren til en annen behandling enn avtalt eller la en annen Underdatabehandler utføre den beskrevne behandlingen i andre tilfeller enn det som følger av Bilag B, punkt B.1 om skifte av Underdatabehandler.



C. INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

C.1. Behandlingens omfang og formål

Personopplysningene skal utelukkende behandles i det omfang og for de formål som er beskrevet i

- Hovedavtalen
- Databehandleravtalen med bilag

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Databehandleravtalen, og kan ikke behandle disse til egne formål.

C.2. Sikkerhet ved behandlingen

C.2.1. Angivelse av sikkerhetsnivå

Ut fra en vurdering av omfanget av personopplysninger som blir behandlet, typen opplysninger og karakteren av behandlingen er det basert på en konkret risikovurdering fastsatt at behandlingen (velg ett alternativ):

- ☐ Krever et høyt sikkerhetsnivå. Begrunnelse:

<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:

<Vis til risikovurderingen som er gjort og skriv begrunnelse>

< F.eks.: Behandlingen omfatter bare opplysninger som er allment kjent som navn og adresse>

C.2.2. Styringssystem for informasjonssikkerhet

Databehandleren skal ha et egnet styringssystem for informasjonssikkerhet.

Databehandleren skal etablere og forvalte tilstrekkelige sikkerhetstiltak for å ivareta informasjonssikkerheten for behandling av personopplysningene, herunder (flere valg mulig):

- | | |
|--------------------------|---|
| ☐ | Sikkerhetskrav som beskrevet i Hovedavtalen: <i><sett inn henvisning til konkret regulering i Hovedavtalen></i> |
|--------------------------|---|

☐	Sikkerhetskrav som beskrevet nedenfor: <Sett inn beskrivelse av relevante sikkerhetskrav>
--------------------------	---

C.3. Dokumentasjon

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som fremkommer av Gjeldende personvernregler og Databehandleravtalen, herunder kravene til informasjonssikkerhet. Slik dokumentasjon skal oppbevares og ajourholdes så lenge Databehandleravtalen består, og gjøres tilgjengelig for Behandlingsansvarlig eller tilsynsmyndigheter på forespørsel.

C.4. Overføring av personopplysninger - Lokasjon for behandling og tilgang

Behandling av de personopplysninger som avtalen omfatter kan ikke uten den Behandlingsansvarliges forutgående skriftlige godkjenning utføres på eller med tilgang fra andre lokasjoner enn de som er angitt i Bilag B.2. Med lokasjon menes:

- Sted det er mulig å få tilgang til personopplysningene fra (aksessering)
- Sted hvor personopplysningene bearbeides (prosesserer)
- Sted hvor personopplysningene lagres

Begrensningen ovenfor gjelder ikke Databehandlerens mor-, søster- og datterselskaper som er etablert innenfor EØS-området. Databehandleren skal imidlertid på forespørsel fra den Behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles.

C.5. Rutiner for revisjon og tilsyn

For å kontrollere etterlevelse av Gjeldende personvernregler og Databehandleravtalen er det avtalt følgende (flere valg mulig):

☐	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: i. gjennomføres én gang årlig, ii. utføres i henhold til anerkjente attestasjonsstandarter, for eksempel ISAE 3402. iii. 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>

C.6. 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: <Angi hvordan og hvilket format som skal benyttes for tilbakelevering>



☐	<Sett inn eventuelle andre avtalte rutiner for sletting eller tilbakelevering>

C.7. 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.>

C.8. Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningsikkerheten eller endring i bruk av underdatabehandlere, skal følgende kanaler benyttes:

Hos Behandlingsansvarlig

Sikkerhetsbrudd:

Telefon: [Fyll ut]

E-post [Fyll ut]

Andre henvendelser:

Navn: [Fyll ut]

Stilling: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]

Hos Leverandøren

Sikkerhetsbrudd:

Telefon: [Fyll ut]

E-post [Fyll ut]

Andre henvendelser:

Navn: [Fyll ut]

Stilling: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]



D. TROMS FYLKESKOMMUNES RETNINGSLINJE FOR LEVERANDØRSTYRING

1. Innledning

Leverandørstyring handler om å evaluere, administrere og overvåke organisasjonens forhold til eksterne leverandører for å sikre at deres tjenester og produkter oppfyller etablerte standarder for kvalitet og sikkerhet. Retningslinjen skal sikre ivaretagelse av informasjon og personopplysninger som behandles av leverandører.

2. Omfang

Denne retningslinjen omfatter rammer og føringer for hvordan Troms fylkeskommune skal stille krav til fylkeskommunens leverandører om ivaretagelse av informasjonssikkerhet og personvern, og skal gi anbefalte sikkerhetskrav for anskaffelse og forvaltning.

Med leverandører mener vi også andre som er i leveransekjeden, herunder underleverandører eller andre tredjeparter.

3. Målsettinger

Sikre at leverandørene ivaretar informasjonssikkerheten og personvernet i henhold til inngåtte avtaler og gjeldende regelverk.

4. Krav til leverandører som behandler informasjon på vegne av Troms Fylkeskommune

Leverandøren har taushetsplikt om informasjonen leverandøren får tilgang til i kontraktsforholdet.

Dersom leverandøren skal behandle personopplysninger skal det inngås databehandleravtale.

Hvis leverandøren skal benytte Troms Fylkeskommune sine IKT-systemer skal IKT-reglementet for bruk av IKT-ressurser følges.

5. Avtaleregulering av leverandørene

Disse informasjonssikkerhetskravene handler om å sikre at relevante krav til informasjonssikkerhet og personvern er definert og avtalefestet. Dersom det er hensiktsmessig, så skal mer detaljerte krav for håndtering av informasjon, systemer, tilganger og IT-utstyr spesifiseres i egen avtale.

- *Standardavtaler.* Alle leverandører skal der det er mulig, reguleres med relevante standardavtaler. Kravene i standardavtalene skal også gjelde for leverandørenes underleverandører.
- *Sikkerhets- og personvernkrav.* Avtaleforholdet skal inkludere krav til informasjonssikkerhet og personvern. De samme kravene skal gjelde for leverandørens underleverandører.

Når en leverandør behandler personopplysninger på vegne av fylkeskommunen, skal det i tillegg etableres en databehandleravtale for å sikre at behandlingen skjer i tråd med personvernregelverket. Fylkeskommunen skal bruke standardiserte maler for slike avtaler, enten malen til [DFØ](#) eller [Datatilsynet](#).

- *Vurdering av tilstrekkelige garantier.* Når en leverandør behandler personopplysninger på vegne av fylkeskommunen, så er leverandøren etter personopplysningsloven en databehandler. Databehandlere skal stille tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven. Eksempler på garantier kan være at databehandleren har et sertifisert styringssystem for informasjonssikkerhet (ISO 27001), at de har et styringssystem for informasjonssikkerhet og personvern (ISO 27701), eller at de gjennom annen dokumentasjon kan demonstrere etterlevelse av lovverket.



6. Informasjonssikkerhetskrav til leverandører

6.1 Sikkerhetsrevisjon

Troms Fylkeskommune skal ha tilgang til å gjennomføre sikkerhetsrevisjon av løsning/leverandør. Dette inkluderer penetrasjonstesting og sårbarhetsskanning.

6.2 Risikostyring

Leverandøren skal ha en løpende prosess for fortløpende identifisere, vurdere og håndtere sårbarheter i tjenesten.

Leverandør bør være åpen om sine sikkerhetspraksiser og regelmessig rapportere sikkerhetsstatus og eventuelle hendelser.

6.3 Avslutning av avtale

Leverandøren skal yte bistand til Troms Fylkeskommune dersom fylkeskommunen ønsker å avslutte avtalen. Leverandøren skal legge til rette for at fylkeskommunens data blir overført til fylkeskommunen eller til tredjepart utpekt av fylkeskommunen.

Troms Fylkeskommune skal beholde eierskapet til fylkeskommunens data etter at kontrakten er avsluttet og til data er flyttet og/eller slettet fra tjenesten.

6.4 Beskyttelse av data under overføring

Data som overføres via nettverk skal sikres. Dette gjelder både data som overføres til og fra tjenesten, internt i tjenesten og data som utveksles med andre tjenester.

6.5 Beskyttelse av datasenter

Leverandør skal forhindre uautorisert tilgang til sine datasenter samt beskytte mot tyveri, skade, tap og at utstyr svikter for å sikre kontinuerlig drift.

6.6 Beskytte lagret informasjon

Leverandøren skal definere, velge, dimensjonere og implementere passende kryptografiske mekanismer støttet av en tilstrekkelig nøkkeladministrasjonsinfrastruktur for å sikre sikker drift av tjenestene. Det gjelder data i ro så vel som data i bevegelse (data in transit).

Leverandør skal sikre at det finnes pålitelige sikkerhetskopiering og evne til gjenoppretting for å beskytte data mot tap eller skade.

6.7 Separasjon mellom kunder

Leverandøren må skille Troms Fylkeskommune sine tjenester og data fra andre kunder hos leverandøren.

6.8 Backup

Leverandør skal sørge for tilfredsstillende backup av data slik at data kan gjenskapes (restores) raskt og effektivt ved behov.

6.9 Sletting av data

Leverandøren må kunne dokumentere hvordan man sletter data og hvordan man sikrer at slettede data ikke kommer på avveie eller kan gjenskapes.

6.10 Tilgjengelighet

Tjenesten skal være tilgjengelig for Troms Fylkeskommune når fylkeskommunen har behov for tjenesten. Leverandøren skal kunne garantere oppetid og dokumentere historisk oppetid/tilgjengelighet.

6.11 Endringshåndtering

Leverandøren skal ha prosess for å håndtere endringer for å sikre at endringer som kan påvirke sikkerheten identifiseres og håndteres, og at uautoriserte endringer kan oppdages.

6.12 Sporbarhet

Alle relevante handlinger som utføres av leverandøren skal logges. Loggen skal ikke kunne manipuleres. Troms Fylkeskommune skal få tilgang til loggene på forespørsel.



6.13 Tilgangskontroll/autentisering

Løsningen skal ha en robust tilgangskontroll som sikrer at rett person får tilgang til rett informasjon og rette funksjoner i løsningen. Autentisering utelukkende basert på brukernavn og passord anses ikke som forsvarlig.

Dersom det er relevant for tjenesten skal leverandør skal tilby verktøy for administrasjon av Troms Fylkeskommune sine brukere og deres tilganger og ha tilstrekkelig støtte for bruk av eksterne identitetstilbydere slik som bla Microsoft Entra ID.

6.14 Sikkerhetsovervåking

Leverandøren skal ha tilstrekkelig sikkerhetsovervåking av tjenesten, rutiner for varslings ved hendelser, samt evne til å håndtere sikkerhetshendelser raskt og effektivt.

Leverandør skal på forespørsel gi Troms Fylkeskommune tilgang til revisjonsrapporter for vurdering av sikkerhetsovervåkingen, vurdering av tilgangsstyringen til systemer og komponenter for leverandørens egne administratorer og hvilke prosedyrer og rutiner de har for varslings.

Sikkerhetslogger skal gjøres tilgjengelig for Troms Fylkeskommunes på forespørsel.

7. Ansvar

- Ansvarlig for styringssystem for informasjonssikkerhet og personvern (INFODOK) eier denne retningslinjen.
Systemeiere er ansvarlige for at systemer som driftes av leverandører er avtaleregulert, og at relevante sikkerhetskrav er inkludert i avtalene.
- Se også dokumentet [Roller og ansvar - Informasjonssikkerhet og personvern](#)

8. Resultat

Lavere risiko for sikkerhetsbrudd som følge av at leverandørene ivaretar informasjonssikkerheten innenfor de rammene kommunen har satt.

1. Referanser

- ISO 27002:2022 5.19 «Informasjonssikkerhet i leverandørforhold»
- ISO 27002:2022 5.20 «Håndtering av informasjonssikkerhet i leverandøravtaler»
- ISO 27002:2022 5.21 «Håndtering av informasjonssikkerhet i IKT-leveransekjeden»
- ISO 27002:2022 5.22 «Overvåking, gjennomgang og endringshåndtering av leverandørtjenester»
- NIS2 artikkel 21 nr 2 bokstav d «Supply chain security»



E. ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER ETTER AVTALEINNGÅELEN

Tilleggspunkt til kapittel 8

Dersom bruddet medfører at den behandlingsansvarlige må varsle de registrerte (jf. artikkel 34), må databehandleren gi den behandlingsansvarlige informasjonen som kreves for at den behandlingsansvarlige kan ivareta plikten til å gi slik underretning på en tydelig måte, og i tråd med artikkel 33 nr. 3 bokstav b), c) og d).

Tillegg til kapittel 14 punkt 2 (14.2)

Behandlingsansvarlig har likevel rett til å si opp avtalen dersom databehandleren ikke lenger oppfyller lovens krav etter artikkel 28 nr. 1.