Innlandet fylkeskommune

Styrende dokument, veg

Rev: 001

Dato: 01.01.2020

D2-D-Databehandleravtale

Xxxx «Kontraktsnavn» 20xx-20xx

<Elementsnr:>

Databehandleravtale

Databehandleravtale til driftskontrakt xxxx «Kontraktsnavn» (heretter «leveranseavtalen»)

datert xx.xx.xxxx, er inngått mellom

[Skriv her]

(heretter kalt databehandleren)

og

Innlandet fylkeskommune

(heretter kalt den behandlingsansvarlige)

Den behandlingsansvarlige og databehandleren blir i fellesskap omtalt som «partene».

Denne databehandleravtalen omfatter den generelle avtaleteksten og vedleggene som er angitt i kapittel 1.2 Vedlegg til databehandleravtalen.

Databehandleravtalens varighet er beskrevet i leveranseavtalen.

Sted og dato	[Behandlingsansvarliges navn her]	[Databehandlers navn her]
[Skriv sted og dato her]		
_____	_____	_____
	behandlingsansvarliges underskrift	databehandlers underskrift

Databehandleravtalen undertegnes i to eksemplarer, ett til hver part.

Innholdsfortegnelse

1 Generelle bestemmelser

1.1 Databehandleravtalens bakgrunn og formål

Formålet med databehandleravtalen er å regulere hvordan databehandleren bruker og sikrer personopplysninger som behandles på vegne av den behandlingsansvarlige i samsvar med de gjeldende kravene til behandling av personopplysninger. Dette blir gjort for å sikre at personopplysningene ikke brukes ulovlig, urettmessig, eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet. Kravene omfatter bestemmelsene i personopplysningsloven, med den innlemmede personvernforordningen, i tillegg til forskrifter til loven. Dette vil videre bli omtalt som «personvernregelverket».

Denne databehandleravtalen gjelder for all behandling av personopplysninger som databehandleren gjør for å oppfylle leveranseavtalen. Databehandleravtalen vil i tillegg gjelde for ytterligere behandling av personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne databehandleravtalens gyldighetsperiode, og som innebærer at databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige. Slike avtaler skal gå frem av *Vedlegg 104 – Endringer i oppdraget/tjenesten etter avtaleinngåelsen*.

Databehandleravtalen fritar ikke databehandleren for forpliktelser som er pålagt databehandleren direkte i personopplysningsloven eller annen lovgivning.

Hvis leveranseavtalen blir overdratt til andre parter, skal denne databehandleravtalen overdras på samme måte.

1.2 Vedlegg til Databehandleravtalen

Vedlegg	**Ja**	**Nei**
Vedlegg 101 – Endringer i den generelle avtaleteksten	☐	☒
Vedlegg 102 – Partenes avtaler om andre forhold	☐	☒
Vedlegg 103 – Vederlag og betalingsbetingelser	☐	☒
Vedlegg 104 – Endringer i oppdraget/tjenesten etter avtaleinngåelsen	☐	☒
Vedlegg 201 – Spesifisering av databehandleroppdraget	☒	
Vedlegg 401 – Krav til sikkerhet ved behandlingen	☒	
Vedlegg 402 – Underdatabehandler	☒	
Vedlegg 403 – Bistand til den behandlingsansvarlige	☒	☐
Vedlegg 404 – Brudd på personopplysningssikkerheten	☒	
Vedlegg 405 – Sletting og tilbakelevering	☒	
Vedlegg 406 - Prosedyre for tilsyn som foretas av den behandlingsansvarlige	☒	☐
Vedlegg 501 - Overføring av personopplysninger til Utlandet	☒	☐
Vedlegg 501B - Overføring av personopplysninger til Utlandet	☒	☐

1.3 Rangordning

Hvis det oppstår uenighet, skal disse prinsippene gjelde:

1. Ved motstrid mellom databehandleravtalens regulering og rammene som følger av personvernregelverket eller annen relevant lovgivning, viker databehandleravtalens regulering.
2. Databehandleravtalen har forrang ved eventuell motstrid med leveranseavtalens bestemmelser når det gjelder behandling av personopplysninger.
3. Den generelle avtaleteksten i databehandleravtalen går foran vedleggene.
4. I den grad det er klart og utvetydig hvilket punkt eller hvilke punkter som er endret, erstattet eller gjort tillegg til, skal disse motstridprinsippene gjelde:
   a) *Vedlegg 101 – Endringer i den generelle avtaleteksten* går foran den generelle avtaleteksten.
   b) Vedlegg 104 – Endringer i oppdraget/tjenesten etter avtaleinngåelsen går foran de øvrige vedleggene.

1.4 Forhandling eller endring av databehandleravtalen

Begge partene kan forhandle om databehandleravtalen hvis lovendringer eller uoverensstemmelser i databehandleravtalen gir anledning til dette.

Endringer til den generelle avtaleteksten skal samles i *Vedlegg 101 – Endringer i den generelle avtaleteksten*.

Hvis det oppstår endringer i det gjeldende lovverket, kommer en rettskraftig dom som gir en annen tolkning av personvernlovgivningen, eller blir gjort endringer i leveranseavtalen (eller senere skriftlige avtaler mellom partene) som krever endringer av denne databehandleravtalen, skal partene samarbeide for å oppdatere databehandleravtalen i tråd med endringene.

1.5 Partenes avtaler om andre forhold

Forhold som ikke er regulert i denne databehandleravtalen, følger de pliktene og rettighetene som er regulert i leveranseavtalen.

Hvis det finnes regulering av andre forhold som er knyttet til å oppfylle denne databehandleravtalen, følger dette av *Vedlegg 102 – Partenes avtaler om andre forhold*.

1.6 Meddelelser

Meddelelser, underretning, instrukser, varsler eller annen kommunikasjon mellom partene etter denne databehandleravtalen skal sendes skriftlig til kontaktperson for leveranseavtalen.

Dersom databehandleren blir kontaktet av tredjeparter, inkludert registrerte og tilsynsmyndigheter, skal databehandleren videreformidle henvendelsen til den behandlingsansvarlige snarest. Med mindre annet er skriftlig avtalt, og så langt det er mulig, skal den behandlingsansvarlige selv ha kontakten med tredjeparter.

Melding om brudd på personvernregelverket er regulert i *Vedlegg 404 – Brudd på personopplysningssikkerheten.*

1.7 Bestemmelser om vederlag og dekning av kostnader

Hvis partene har regulert eller avtalt vederlag eller lignende i forbindelse med databehandlerens bistand til den behandlingsansvarlige, vil dette gå frem av *Vedlegg 103 – Vederlag og betalingsbetingelser*.

1.8 Behandlingens varighet

Denne databehandleravtalen gjelder fra datoen den er signert, og til leveranseavtalen løper ut. Unntaket er hvis databehandlerens plikter etter leveranseavtalen opphører på et tidligere tidspunkt. Dersom leveranseavtalen forlenges, forlenges denne databehandleravtale tilsvarende, med mindre annet er skriftlig avtalt.

1.9 Mislighold

Dersom en avtalepart misligholder sine forpliktelser etter denne databehandleravtalen, skal anvendbare bestemmelser i leveranseavtalen gjelde.

Dersom det ikke finnes anvendbare bestemmelser om heving i leveranseavtalen, kan en av partene heve leveranseavtalen dersom den andre parten i vesentlig grad misligholder sine forpliktelser etter denne databehandleravtalen.

Når det skal vurderes om mislighold etter avsnittene ovenfor er vesentlig, kan den behandlingsansvarlige særlig ta hensyn til om databehandlerens mislighold knytter seg til bestemmelser om behandling av personopplysninger som er i strid med instruks fra den behandlingsansvarlige, om personopplysningssikkerhet, om bruk av underdatabehandler og om overføring av personopplysninger ut av EU/EØS. Denne oppramsingen er ikke uttømmende.

2 Databehandleroppdraget[1]

Databehandleroppdraget er spesifisert i *Vedlegg 201 – Spesifisering av databehandleroppdraget*. Spesifiseringen skal minst omfatte

- hensikten med og en beskrivelse av databehandleroppdraget
- behandlingens formål og art
- kategorier av registrerte og typen personopplysninger

[1] Artikkel 28 nr. 3 første avsnitt.

3 Den behandlingsansvarliges plikter og rettigheter[2]

3.1 Ansvar og råderett over personopplysningene

Den behandlingsansvarlige har ansvar for at det finnes rettslig grunnlag for den behandlingen som databehandleren er instruert til å gjøre.

Den behandlingsansvarlige er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernregelverket. Den behandlingsansvarlige skal til enhver tid ha full rettslig råderett over personopplysningene.

Med mindre annet er skriftlig avtalt eller følger av dokumentert instruks skal den behandlingsansvarlige

a) svare på henvendelser fra de registrerte om behandling av personopplysninger som er omfattet av denne databehandleravtalen
b) informere de registrerte i tråd med gjeldende regelverk for behandling av personopplysninger og ellers oppfylle pliktene sine når det gjelder de registrertes rettigheter
c) melde brudd på personopplysningssikkerheten til Datatilsynet og eventuelt til de registrerte, uten ugrunnet opphold i henhold til gjeldende regelverk for behandling av personopplysninger
d) samarbeide med tilsynsmyndigheter i tråd med gjeldende regelverk for behandling av personopplysninger

3.2 Rett og plikt til å bestemme formålet

Den behandlingsansvarlige har både rett og plikt til å bestemme hvilke formål og hvilke hjelpemidler som skal brukes i behandlingen.

3.3 Ansvar for å gi instrukser

Den behandlingsansvarlige skal gi databehandleren dokumenterte instrukser om hvordan personopplysningene skal behandles. Denne databehandleravtalen med vedlegg utgjør instruksen.

[2] Artikkel 28 nr. 3 første avsnitt.

4 Databehandlerens forpliktelser[3]

4.1 Krav til behandling av personopplysninger etter skriftlig instruks[4]

Databehandleren skal bare behandle personopplysninger etter dokumenterte instrukser fra den behandlingsansvarlige og følge alle de rutinene og instruksene for behandlingen som den behandlingsansvarlige til enhver tid har bestemt at skal gjelde.

Første ledd gjelder ikke dersom norsk lov pålegger databehandleren en konkret behandling av personopplysninger. I så fall skal databehandleren underrette den behandlingsansvarlige om dette før behandlingen settes i verk, med mindre loven forbyr slik underretning av hensyn til viktige samfunnsinteresser.

Mener databehandleren at en instruks fra den behandlingsansvarlige er i strid med personvernregelverket eller annen lovgivning, skal databehandleren umiddelbart underrette den behandlingsansvarlige om sin oppfatning.

4.2 Krav til fortrolig behandling av personopplysningene[5]

Databehandleren skal bare autorisere personer som av tjenstlige grunner må ha tilgang til personopplysningene.

Databehandleren skal sikre at bare autoriserte personer har tilgang til personopplysningene, og at tilgangen fratas dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder for personene.

Databehandleren skal til enhver tid ha en oppdatert oversikt over hvilke medarbeidere hos databehandleren og eventuelle underdatabehandlere og tredjeparter som har tilgang til personopplysningene som behandles. Denne oversikten skal på forespørsel legges frem for den behandlingsansvarlige innen rimelig tid.

Databehandleren skal sikre at personer som er autorisert til å behandle person-opplysningene, har forpliktet seg til å behandle opplysningene konfidensielt eller er underlagt en lovfestet taushetsplikt. Underdatabehandler(e) som på vegne av databehandleren utfører oppdrag der bruk av eller tilgang til personopplysningene inngår, skal være kjent med databehandlerens forpliktelser overfor den behandlingsansvarlige etter avtaler og lovverk, og skal påta seg å etterleve disse forpliktelsene. Databehandleren skal etter forespørsel fra den behandlingsansvarlige dokumentere at de autoriserte personene er underlagt slik

[3] Artikkel 28 nr. 3 første avsnitt.
[4] Artikkel 28 nr. 3 bokstav a.
[5] Artikkel 28 nr. 3 bokstav b)

konfidensialitet og taushetsplikt. Dokumentasjonen kan blant annet inneholde en beskrivelse av opplæringen og en taushetserklæring.

Taushetsplikten gjelder også etter at databehandleravtalen har opphørt.

4.3 Krav til sikkerhet ved behandlingen[6]

Databehandleren skal oppfylle alle krav til sikkerhetstiltak som stilles i personvern-regelverket. Dette inkluderer å sette i verk tiltak som kreves i henhold til personvernforordningens artikkel 32 for å sørge for å oppnå et passende sikkerhetsnivå ut fra personvernrisikoen. Databehandleren skal som et minimum sette i verk det sikkerhetsnivået og de sikkerhetstiltakene som er spesifisert nærmere i *Vedlegg 401 – Krav til sikkerhet ved behandlingen*.

Eventuelle nye krav til informasjonssikkerhet som måtte følge av endringer i personvern-regelverket, skal oppfylles. Databehandleren plikter å sette i verk eventuelle endringer, tillegg og annet som er nødvendig for å oppfylle nye krav, før endringene trer i kraft.

Databehandleren kan ikke endre avtalte informasjonssikkerhetstiltak uten at den behandlingsansvarlige er blitt skriftlig informert og skriftlig har godkjent endringen. Endringer kan bare nektes på saklig grunnlag.

Dersom databehandleren må endre informasjonssikkerhetstiltakene sine som følge av akutte endringer i trusselbildet, skal den behandlingsansvarlige varsles om dette uten ugrunnet opphold. Databehandleren skal skriftlig informere den behandlingsansvarlige om endringene som er gjort, og hvordan risiko-/trusselbildet er endret, innen det antallet virkedager fra endringen er gjort, som er angitt i *Vedlegg 401 – Krav til sikkerhet ved behandlingen*.

4.4 Bruk av annen databehandler (underdatabehandler)[7]

Databehandleren skal oppfylle betingelsene i personvernforordningen artikkel 28 nr. 2 og 4 ved bruk av underdatabehandler(e). Bruk av underdatabehandler skal ikke skje uten en generell eller spesifikk godkjenning fra den behandlingsansvarlige.

Nærmere betingelser for databehandlerens bruk av underdatabehandler og/eller eventuelle godkjenninger av spesifikke underdatabehandlere går frem av *Vedlegg 402 – Underdatabehandler*.

Dersom databehandleren benytter seg av underdatabehandlere, forblir databehandleren ansvarlig for deres behandling av personopplysningene. Dersom underdatabehandlerne ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, har databehandler det hele og fulle ansvaret overfor den behandlingsansvarlige. Underdatabehandler(e) har de

[6] Artikkel 28, nr. 3, bokstav c)
[7] Artikkel 28 nr. 3 bokstav d)

samme forpliktelsene som databehandleren med hensyn til vern av personopplysninger. Disse forpliktelsene er fastsatt i avtalen med underdatabehandleren.

Databehandleren skal garantere for at underdatabehandlere har bekreftet at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne databehandleravtalen oppfyller kravene i personvernregelverket.

Databehandleren er forpliktet til å sikre at databehandleravtalen med underdatabehandlere gir den behandlingsansvarlige rett til å tre inn i databehandleravtalen dersom databehandleren går konkurs. Dette skal sikre at databehandlerens rettigheter kan gjøres gjeldende – for eksempel instruksjon om sletting eller tilbakeføring av personopplysninger.

Den behandlingsansvarlige skal etter forespørsel få utlevert denne avtalen. Eventuelle kommersielle vilkår, for eksempel priser, som ikke påvirker sikkerhetsbestemmelsene i databehandleravtalen, trenger ikke utleveres.

4.5 Bistand til å ivareta de registrertes rettigheter[8]

Databehandleren plikter å bistå den behandlingsansvarlige, ved hjelp av passende tekniske og organisatoriske tiltak, med å oppfylle den behandlingsansvarliges forpliktelser til å besvare forespørsler om utøvelse av de registrertes rettigheter etter personvernforordningens kapittel III.

En detaljert beskrivelse av hvilken støtte databehandleren skal gi for at den registrerte får utøvd rettighetene sine, er gitt i *Vedlegg 403 – Bistand til behandlingsansvarlig*.

4.6 Støtte til at den behandlingsansvarlige kan oppfylle krav til informasjonssikkerhet[9]

Databehandleren plikter å støtte den behandlingsansvarlige med å sikre at forpliktelsene i henhold til artikkel 32–36 som er relevante i dette databehandleroppdraget, overholdes.

4.6.1 Bistand til sikkerhet ved behandling[10]

Databehandleren plikter å bistå den behandlingsansvarlige med å gjennomføre passende tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som passer til de risikoene som er forbundet med behandlingen.

[8] Artikkel 28 nr. 3 bokstav e.
[9] Artikkel 28 nr. 3 bokstav f.
[10] Artikkel 32 Sikkerhet ved behandlingen.

4.6.2 Bistand ved brudd på personopplysningssikkerheten[11]

All behandling av personopplysninger som er i strid med personvernregelverket, denne databehandleravtalen, de behandlingsansvarliges instrukser, og alle sikkerhetsbrudd, skal behandles som et brudd på personopplysningssikkerheten.

Databehandleren skal

a) avdekke, registrere, rapportere og rette opp avvik knyttet til informasjonssikkerhet, blant annet ved å loggføre og dokumentere alle forsøk på ikke-autorisert tilgang og andre brudd på personopplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos databehandleren.
b) uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes databehandleren eller vedkommendes underdatabehandler, skal korrigeres uten kostnad for den behandlingsansvarlige.
c) etter å ha fått kjennskap til et brudd på personopplysningssikkerheten uten ugrunnet opphold informere den behandlingsansvarlige
d) dokumentere alle avvik, inkludert de faktiske forholdene knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak, samt dokumentere overfor den behandlingsansvarlige at tiltak er utført
e) gi den behandlingsansvarlige alle nødvendige opplysninger for å kunne gi avviksmelding/melding om brudd på personopplysningssikkerheten til de aktuelle tilsynsmyndighetene og for å kunne besvare eventuelle spørsmål fra og etterleve eventuelle pålegg fra disse myndighetene. På samme måte skal det gis nødvendig opplysninger for å kunne gjennomføre varsling til de registrerte.

Hvem som skal informeres hos den behandlingsansvarlige, og hvordan, er opplyst i Vedlegg 404 – Brudd på personopplysningssikkerheten.

4.6.3 Bistand til å informere den registrerte om brudd[12]

Dersom bruddet medfører en risiko for den registrertes rettigheter og friheter, skal databehandleren gi den informasjonen som kreves for at den behandlingsansvarlige skal kunne gi en grundig beskrivelse av bruddet til tilsynsmyndigheten. Det samme gjelder for brudd som medfører at den behandlingsansvarlige må varsle den registrerte.

4.6.4 Bistand til vurdering av personvernkonsekvenser og forhåndsdrøftinger[13]

Dersom den behandlingsansvarlige skal foreta en vurdering av personvernkonsekvenser og eventuelt forhåndsdrøftinger, skal databehandleren gi den behandlingsansvarlige den informasjonen og den støtten som er nødvendig.

[11] Artikkel 33 Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten.
[12] Artikkel 34 Underretning av den registrerte om brudd på personopplysningssikkerheten.
[13] Artikkel 35 Vurdering av personvernkonsekvenser og artikkel 36 Forhåndsdrøftinger.

4.7 Sletting eller tilbakelevering[14]

Databehandleren skal, etter skriftlig instruksjon fra den behandlingsansvarlige, slette eller tilbakelevere alle personopplysninger til den behandlingsansvarlige etter at leveranseavtalen eller senere skriftlige avtaler mellom partene er opphørt.

Hvordan denne bestemmelsen skal gjennomføres i praksis, er beskrevet i *Vedlegg 405 – Sletting og tilbakelevering*.

4.8 Tilsyn og revisjon[15]

Databehandleren har plikt til å gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene som er fastsatt i artikkel 28, er oppfylt, og dessuten muliggjøre og bidra til revisjoner, inkludert inspeksjoner, som gjennomføres av den behandlingsansvarlige selv eller av en annen inspektør på fullmakt fra den behandlingsansvarlige. Dette omfatter også å gi tilgang til sikkerhetsdokumentasjon.

Databehandleren plikter å gjennomføre sikkerhetsrevisjoner i forbindelse med utbedring etter alvorlige hendelser, større endringer av betydning for informasjonssikkerheten og avdekking av nye alvorlige sårbarheter.

Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke oppfyller kravene ovenfor, skal dette behandles som avvik/brudd på personopplysningssikkerheten.

Avdekker revisjonen at databehandleren ikke oppfyller kravene i denne databehandleravtalen, plikter databehandleren å foreta nødvendige utbedringer umiddelbart.

Prosedyrer for eventuelle tilsyn i regi av den behandlingsansvarlige knyttet til databehandlerens eller underdatabehandlerens overholdelse av denne databehandleravtalen går frem av *Vedlegg 406 – Prosedyre for tilsyn som foretas av Behandlingsansvarlig*.

5 Overføring av personopplysninger til utlandet[16]

Alle overføringer av personopplysninger til land utenfor Norge skal spesifiseres i *Vedlegg 501 – Overføring av personopplysninger til utlandet*. Oversikten skal også inneholde en liste over ytterligere dokumentasjon som eventuelt kreves i hver enkelt overføring.

Databehandleren og eventuelle underdatabehandlere har et selvstendig ansvar for å sikre at overføringen av personopplysninger til tredjestater[17] er i samsvar med kapittel V i personvernforordningen.

Databehandleren og eventuelle underdatabehandlere skal ikke overføre personopplysninger til tredjestater eller la personer i tredjestater på noen måte få tilgang til personopplysninger uten at den behandlingsansvarlige på forhånd eksplisitt har godkjent dette skriftlig og gitt instruks om overføring eller tilgang. Det at den behandlingsansvarliges ansatte har

[14] Artikkel 28 nr. 3 bokstav g.
[15] Artikkel 28 nr. 3 bokstav h.
[16] Kapittel V (artikkel 44–50).
[17] Land utenfor EU/EØS.

fjerntilgang til virksomheter som holder til i EU/EØS, regnes ikke som overføring til tredjestater, men må være i overenstemmelse med kravene i personvernforordningen.

Bestemmelsene i avsnittet ovenfor gjelder ikke for godkjente tredjestater.

Bestemmelsene om overføring til tredjestater gjelder både der personopplysninger lagres på en server i tredjestat, og der serveren står i Norge, men personale i en tredjestat har tilgang til personopplysningene som databehandleren behandler på vegne av den behandlingsansvarlige. Det samme gjelder for innlogging via skytjenester[18].

Spørsmål om overføring til tredjestater skal tas opp med den behandlingsansvarlige. Frister og andre bestemmelser er spesifisert i *Vedlegg 501 - Overføring av personopplysninger til utlandet*.

[18] Skytjenester er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.

Vedlegg 101 – Endringer i den generelle avtaleteksten

Ingen endringer

Vedlegg 102 – Partenes avtaler om andre forhold

Erstatningsansvar

Partenes erstatningsansvar for skade som rammer den registrerte eller andre fysiske personer, og som skyldes brudd på personvernforordningen, personopplysningsloven med forskrifter eller annet regelverk som gjennomfører personvernforordningen, følger av bestemmelsene i personvernforordningen artikkel 82.

Dersom det ikke foreligger bestemmelser om erstatning i leveranseavtalen, har en avtalepart krav på å få dekket det økonomiske tapet han blir påført, som følge av at den andre avtaleparten misligholder sine forpliktelser etter denne databehandleravtalen.

Uavhengig av reguleringer i leveranseavtalen er avtalepartene hver for seg ansvarlige for overtredelsesgebyr som er ilagt i medhold av personvernforordning artikkel 83.

Lovvalg

Partenes rettigheter og plikter etter denne databehandleravtalen bestemmes i sin helhet av norsk rett.

Dersom en tvist ikke blir løst ved forhandlinger eller mekling, kan hver av partene forlange tvisten avgjort med endelig virkning ved norske domstoler.

Partene vedtar ved denne databehandleravtalen Hedmarken tingrett som verneting. Dette gjelder også etter opphør av databehandleravtalen.

Vedlegg 103 – Vederlag og betalingsbetingelser

Dekning av kostnader

Databehandlerens kostnader i forbindelse med denne databehandleravtalen er kostnader som inngår i tilbudssummen.

Ved revisjon og tilsyn skal hver avtalepart dekke sine egne kostnader. Dette gjelder med mindre et tilsyn avdekker avvik fra forpliktelsene etter denne databehandleravtale. I det tilfellet skal alle kostnadene forbundet med tilsynet dekkes av databehandleren, inkludert den behandlingsansvarliges og eksterne revisorers relevante kostnader.

Vedlegg 104 – Endringer i oppdraget/tjenesten etter avtaleinngåelsen

Det foreligger ikke konkrete planer om endringer i databehandleravtalen på utlysningstidspunktet. Dersom det gjøres endringer i driftskontrakten kan det være nødvendig å gjøre endringer/tilføyelser også i databehandleravtalen.

Vedlegg 201 – Spesifisering av databehandleroppdraget

Hensikt med og beskrivelse av databehandleroppdraget

Hensikten med databehandleroppdraget er å ivareta behandlingsansvarlig sin kontraktsoppfølging overfor driftsentreprenør. Driftsentreprenør (heretter databehandler) må benytte nødvendige registreringssystemer, og gi behandlingsansvarlig tilgang til disse, for å dokumentere gjennomføring og utførelse av oppgavene i driftskontrakten. Registreringssystemene omfatter dokumentasjon av både driftsentreprenørens og underentreprenørenes/underleverandørenes utførelse av de kontraktsfestede oppgavene, og innebærer blant annet at oppdragsgiver skal kunne kontrollere mengder, kilometer og andre målbare enheter.

Formål med behandlingen av personopplysningene

Formålet med behandlingen av personopplysningene er å kontrollere at driftsentreprenør disponerer ressursene han gjennom kontrakten har forpliktet seg til å stille til rådighet, og at driftsentreprenør ved hjelp av disse ressursene utfører arbeidet og oppgavene han i kontrakten har forpliktet seg til.

I tillegg til kontrollformålet, vil også dokumentasjonen for utførte mengder, kilometer og andre målbare enheter kunne brukes som datagrunnlag ved utlysning av nye driftskontrakter.

Kategorier av registrerte

Personopplysningene som behandles gjelder følgende kategorier av registrerte som er tilknyttet den behandlingsansvarlige: ansatte, utsendte arbeidstakere, eller innleide hos entreprenør, underentreprenører og underleverandører.

Type personopplysninger

Personopplysninger som behandles omfatter følgende:

Navn, fødselsdato, posisjonsdata, kjøretøyidentifikasjon, øvrige opplysninger som fremkommer av aktivitetsplaner for kontraktsoppfølgingen, mannskapsoversikt og oversikt over mannskapers godkjente prøver/eksamener for å dokumentere deres kompetanse.

Type behandling

Følgende behandlinger omfattes av databehandleravtalen:

Databehandler samler inn opplysninger som er nødvendige for behandlingsansvarlig sin kontraktsoppfølging ved innsyn i de kontraktsfestede registreringssystemene. Databehandler sletter personopplysningene etter nærmere avtale med behandlingsansvarlig.

Vedlegg 401 – Krav til sikkerhet ved behandlingen

Tekniske og organisatoriske tiltak[19]

Databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen ved behandlingen. Behandlingsansvarlig vil i det følgende angi minimumskrav.

Internkontroll

- Databehandleren skal ha et dokumentert og oppdatert internkontrollsystem for å ivareta informasjonssikkerheten.
- Databehandler skal ha dokumentert ansvar og oppgaver for informasjonssikkerhet, og ansvarsforholdene skal være gjort kjent i organisasjonen.
- Databehandleren skal dokumentere rutiner og sikkerhetstiltak. Dokumentasjonen skal være tilgjengelig på forespørsel fra den behandlingsansvarlige.
- Databehandleren må gi tilstrekkelig dokumentasjon på at behandlingsansvarliges krav er ivaretatt gjennom at den behandlingsansvarlige får tilgang til revisjonsrapporter.
- Databehandler gjennomfører og dokumenterer ledelsens gjennomgang av sikkerheten minimum årlig

Opplæring og informasjon til databehandlers ansatte

- Ansatte hos databehandleren skal ha opplæring i informasjonssikkerhet.
- Ansatte hos databehandleren skal ha informasjon om databehandleravtalen og formålet med den.
- Alle medarbeidere og autoriserte personer hos databehandler skal være informert om/få opplæring i sin eventuelle taushetsplikt for personopplysninger

Sikkerhetsrevisjoner

Generelle bestemmelser for sikkerhetsrevisjoner er gitt i kapittel 4.8 Tilsyn og revisjon.

- Databehandler skal bidra til at den behandlingsansvarlige eller en tredjepart med fullmakt skal ha tilgang til å gjennomføre tilsyn/ revisjon hos databehandler eller underleverandør

[19] Artikkel 32 nr. 1.

Risikovurdering[20]

Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene som er forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet. For å ivareta dette kravet skal følgende gjennomføres:

- Databehandleren skal dokumentere gjennomføring av risikovurderinger og når risikovurdering sist er gjennomført.
- Den behandlingsansvarlige skal få tilgang til gjennomførte risikovurderinger og status på håndtering av tiltak.

Avvikshåndtering

- Databehandleren skal sikre at avvik fra krav til informasjonssikkerhet registreres og rapporteres.
- Databehandler skal sikre at den behandlingsansvarlige varsles umiddelbart ved sikkerhetsbrudd.

Autorisering av tilgang til personopplysninger[21]

For denne databehandleravtalen er dette regulert i kapittel *4.2 Krav til fortrolig behandling av personopplysningene*.

- Databehandler skal bare utpeke og gi autoriserte personer tilgang til personopplysningene.
- Databehandler skal ha dokumenterte rutiner for autorisering og å sikre at ingen andre enn autoriserte har tilgang til personopplysningene.
- Databehandleren skal ha oversikt over tilganger og hvem som har innsyn i personopplysningene.

Taushetsplikt

Ved gjennomføringen av databehandleravtalen, gjelder reglene om taushetsplikt i forvaltningsloven. For databehandlere som ikke er omfattet av forvaltningsloven, gjelder forvaltningsloven § 13 tilsvarende.

[20] Artikkel 32 nr. 2
[21] Artikkel 32 nr. 4

Akutte endringer av informasjonssikkerhetstiltak

Må databehandleren endre informasjonssikkerhetstiltakene sine som følge av akutte endringer i trusselbildet, skal den behandlingsansvarlige varsles om dette skriftlig, med informasjon om endringene som er foretatt, og hvordan risiko/trusselbildet er endret.

Vedlegg 402 – Underdatabehandler

Bruk av underdatabehandler

Dersom en databehandler er en leverandør utenfor EU/EØS (tredjestat) stilles det i Personopplysningsloven særskilte krav til avtalene med disse.

Leverandøren kan bare bruke underdatabehandlere etter skriftlig godkjenning fra behandlingsansvarlig. Leverandøren må inngå databehandleravtaler med sine underleverandører iht. personvernlovgivningens krav.

Den behandlingsansvarlige har, da databehandleravtalen trådte i kraft, godkjent bruk av en underdatabehandler som følger av skjema 402-A, til en behandling som er beskrevet for den enkelte databehandler. Databehandleren kan ikke, uten samtykke fra den behandlingsansvarlige, bruke den enkelte underdatabehandler til annen behandling enn den som er avtalt.

Skifte av underdatabehandler

Databehandleren har, med mindre han er underlagt begrensninger i avtale eller annet regelverk, rett til å skifte ut eller hente inn underleverandører som nevnt i avsnittet ovenfor, i løpet av leveranseavtalens løpetid. Databehandleren skal i dette tilfellet varsle den behandlingsansvarlige senest 4 uker før ny underleverandør starter opp.

Den behandlingsansvarlige har deretter 2 uker til å fremme innsigelser mot den nye underleverandøren. Den behandlingsansvarlige kan i denne perioden motsette seg bruk av den nye underleverandøren dersom det foreligger saklig grunn eller en vurdering av personvernkonsekvenser (DPIA) tilsier det. I det tilfellet at den behandlingsansvarlige motsetter seg underleverandøren, må databehandleren avslutte underleverandørforholdet med underleverandøren.

Vedlegg 402-A – Underdatabehandler (Underleverandør)

Skjemaet skal fylles ut og signeres for hver underdatabehandler (underleverandør) som brukes

Skjema 402-A – Underdatabehandler	
Navn på underdatabehandler:	
Organisasjonsnummer:	

Gi en beskrivelse av underdatabehandlerens oppgaver og/eller tjenester for *databehandleren.* Det skal her også angis dersom det er flere kontraktsledd mellom underdatabehandleren og *databehandleren*, samt hvem underdatabehandleren i så fall står i kontraktsforhold **med**		
Gi en beskrivelse av underdatabehandlerens behandling av personopplysninger i forbindelse med oppfyllelse av leveranseavtalen og/eller databehandleravtalen. Behandlingens formål og art skal også gå frem.		
List opp stater hvor underdatabehandleren har personell som har tilgang til personopplysninger som er omfattet av databehandleravtalen. Dette omfatter plassering av eventuell server for skylagring og av sikkerhetskopier.		
Omfatter underdatabehandlerens behandling av personopplysninger underlagt særlige reguleringer etter EU-forordning 2016/679.	Personopplysninger uten særskilte reguleringer (kryss av)	☐
	Særlige kategorier personopplysninger etter EU-forordning 2016/679 artikkel 9 (kryss av)	☐
	Personopplysninger om straffedommer og lovovertredelser etter EU-forordning 2016/679 artikkel 10 (kryss av)	☐

Dato: Dato:

For databehandleren For den behandlingsansvarlige

_____ _____

Navn: Navn:

Tittel: Tittel:

Vedlegg 403 – Bistand til den behandlingsansvarlige

Dersom behandlingsansvarlig trenger bistand ved spørsmål om databehandlers sikring av personvern må databehandler bistå behandlingsansvarlig.

Kontaktpersoner ved bistand:

Hos den behandlingsansvarlige:	Hos databehandleren:
Ingebjørg Elisabeth Wikstrøm Jurist og personvernkoordinator i samferdselsavdelingen Telefonnr: 957 79718 E-post: ingebjorg.elisabeth.wikstrom@innlandetfylke.no	Navn Stilling Telefonnr. E-post

Vedlegg 404 – Brudd på personopplysningssikkerheten

Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige varsles slik:

Varslet skal være skriftlig, og skal sendes på epost til behandlingsansvarlig ved personvernkoordinator uten ugrunnet opphold. Kopi av varselet skal sendes til driftskontraktens byggeleder i Innlandet fylkeskommune.

Varselet om brudd på personopplysningssikkerheten skal som et minimum inneholde opplysninger som er angitt i personvernforordningens artikkel 33 nr. 3 og 4.

Kontaktpersoner ved brudd på personopplysningssikkerheten:

Hos den behandlingsansvarlige:	Hos databehandleren:
Navn: Ingebjørg Elisabeth Wikstrøm Stilling: Jurist og personvernkoordinator i samferdselsavdelingen Telefonnr: 957 79718 E-post: ingebjorg.elisabeth.wikstrom@innlandetfylke.no	Navn Stilling Telefonnr. E-post

Vedlegg 405 – Sletting og tilbakelevering

Alle data av betydning for vederlag/oppgjør, herunder personopplysninger fra GPS-logger, oppbevares i 1 år etter at sluttoppgjøret er ferdig. Deretter skal alle personopplysninger slettes.

Anonymiserte data om de utførte arbeidene/mengdene gjennom hele kontraktsperioden skal overleveres behandlingsansvarlig iht. driftskontrakten kap. C2-17.76.1.

Vedlegg 406 - Prosedyre for tilsyn som foretas av den behandlingsansvarlige

Den behandlingsansvarlige eller en representant for den behandlingsansvarlige, kan foreta et fysisk tilsyn i løpet av kontraktsperioden for å kontrollere overholdelsen av denne databehandleravtalen hos databehandleren.

Utover det mulige fysiske tilsynet kan det føres tilsyn med databehandleren når det etter den behandlingsansvarliges vurdering oppstår behov for det.

Den behandlingsansvarliges eventuelle utgifter i forbindelse med tilsyn hos databehandler dekkes av den behandlingsansvarlige selv. Databehandleren er forpliktet til å sette av de ressursene (hovedsakelig den tiden) som er nødvendig for at den behandlingsansvarlige skal få gjennomført tilsynet sitt.

Vedlegg 501 - Overføring av personopplysninger til utlandet

Dersom underdatabehandler er utenlandsk (utenfor Norge) eller bruker servere, skytjenester eller tjenester fra utenlandsk(e) leverandør(er) må databehandler fylle ut dette skjemaet:

Hva overføres og behandles	Til hvilken virksomhet	I hvilket land	Er landet (1) i EU/EØS, (2) en godkjent tredjestat utenom USA, (3) USA (sertifisert etter Privacy Shield, eller (4) tredjestat

Spørsmål om overføring til tredjestater skal tas opp med den behandlingsansvarlige senest ___45_____ dager før oppstart eller endring av slik behandling.

Databehandleren skal legge frem en risikovurdering for overføringen.

Vedlegg 501 B – Dokumentasjon av nødvendige garantier

Dette skjemaet brukes til å spesifisere ytterligere informasjon om overføring av personopplysninger til tredjestat eller til en internasjonal organisasjon. Det skal legges ved ett vedlegg pr overføring. Databehandler skal fylle ut dette skjemaet.

Hva overføres og behandles	Til hvilken virksomhet	I hvilket land	Er landet (1) i EU/EØS, (2) en godkjent tredjestat utenom USA, (3) USA (sertifisert etter Privacy Shield, eller (4) tredjestat

Oversikt over vedlegg som dokumenterer nødvendige garantier for overføring til tredjestater:

	Ja (vedlegg nr.)	Nei	Ikke relevant
Sertifisering etter Privacy Shield-avtalen			
Er dokumentasjon på slik sertifisering vedlagt?			---
Er dokumentasjon på at overføringen av person-opplysninger i samsvar med grunnkravene i personvernforordningens artikkel 5 vedlagt?			
Er dokumentasjon på at det er gjennomført risikovurdering (jf. artikkel 32) vedlagt?			
Bruk av andre «nødvendige garantier»			
Er det brukt standard personvernbestemmelser vedtatt av Europakommisjon (Standard Contractual Clauses)?			
Er det brukt bindende virksomhetsregler for et konsern eller en gruppe av foretak?			
Er det brukt godkjente atferdsnormer eller sertifiseringsmekanismer?			
Bruk av kontrakt/avtalevilkår som virksomheten har utformet selv			
Er kontrakt/avtalevilkår vedlagt?			
Er det vedlagt dokumentasjon på at kontrakten er godkjent av Datatilsynet, og at Personvernrådet har gitt sin tilslutning for å kunne overføre personopplysninger?			