

Vedlegg 11 – SSA-L

Databehandleravtale

I henhold til personopplysningsloven og forskrift om behandling av personopplysninger

Mellom

Indre Fosen kommune på vegne av kommunene

Indre fosen, Osen, Ørland og Åfjord

Behandlingsansvarlig

og

ACOS AS

Org.nr. 922 017 433

Databehandler

(til sammen kalt «**Partene**»)

1. Databehandleravtalens hensikt

Databehandleravtalens («**Avtalen**») hensikt er å regulere rettigheter og plikter etter Lov av 15. juni 2018 nr. 38 (heretter kalt personopplysningsloven), forskrift av 15. juni 2018 nr. 876 (forskrift om behandling av personopplysninger) og senere lovgivning som erstatter disse.

Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende. Avtalen regulerer Databehandlers behandling av personopplysninger på vegne av den Behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

Avtalen inngår som en del av Partenes anskaffelses- og vedlikeholdsavtale på ACOS programvare (heretter «**Hovedavtalen**»).

2. Formål, art og omfang

Det henvises til vedlegg 1 for beskrivelse av formål, art og omfang av behandling av personopplysninger.

Det er få begrensninger i programvare for hvilke kategorier av registrerte og type personopplysninger Behandlingsansvarlig kan behandle. Programvare har fritekstfelt og mulighet for arkivering av vedlegg. Det er Behandlingsansvarlig sitt ansvar å utdype kategorier av registrerte og typer personopplysninger i vedlegg 1.

3. Behandlingsansvarliges plikter og rettigheter

Den Behandlingsansvarlige er ansvarlig for å selv behandle personopplysninger i samsvar med personvernforordningen og personopplysningsloven (jf. artikkel 24), denne Avtalen og Hovedavtalen.

Behandlingsansvarlig er ansvarlig for, og skal etablere rutiner i egen virksomhet for blant annet å:

- ivareta de Registrertes rett til informasjon, innsyn og til å få opplysningene slettet eller korrigert
- gjennomføre løpende sletting av personopplysninger i tråd med lovpålagte krav
- melde fra om sikkerhetsbrudd til tilsynsmyndigheter og de registrerte.

Den Behandlingsansvarlige har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen (jf. personvernforordningen artikkel 4 nr. 7).

Den Behandlingsansvarlige har rett til å si opp Avtalen dersom Databehandleren ikke lenger oppfyller lovens krav etter personvernforordningen artikkel 28 nr. 1.

Behandlingsansvarlig skal ved forespørsel om brukerstøtte skjerme personopplysninger som ikke er nødvendig for bistanden.

Behandlingsansvarlig skal følge prinsippet om dataminimering ved sin behandling av personopplysninger.

Behandlingsansvarlig skal straks melde fra til Databehandler om forhold som vil kunne medføre behov for endringer i den måten Databehandler behandler opplysningene på, herunder endringer i hvilke kategorier personopplysninger som inngår i behandlingen og kategorier registrerte, jf. denne Avtalen punkt. 2 og vedlegg 1.

All bistand fra Databehandler iverksatt etter forespørsel fra Behandlingsansvarlig (inkl. ev. utgifter til 3. part) vil faktureres i henhold til Databehandlers ordinære timesatser.

4. Databehandlers plikter

Databehandler skal følge de rutiner og instruks for behandlingen som Behandlingsansvarlig til enhver tid har bestemt skal gjelde. Databehandleren skal kun behandle personopplysninger etter dokumenterte instruks fra den Behandlingsansvarlige.

Databehandleren må omgående underrette den Behandlingsansvarlige dersom Databehandleren mener en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger eller nasjonal rett (jf. artikkel 28 punkt 3 siste ledd).

Databehandleren plikter å overholde den til enhver tid gjeldende personvernlovgivning.

Databehandler skal sikre at kun ansatte hos Databehandler som har tjenstlige behov for tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig, kan gis slik tilgang.

Dersom Behandlingsansvarlig har lagt opp til at det kun er personlige brukere som skal ha tilgang vil Databehandler følge dette. I slike tilfeller må Behandlingsansvarlig selv holde oversikt over hvem hos Databehandler som har gyldig tilgang.

Behandlingsansvarlig kan utføre kontrollsjekk av tilganger hos Databehandler ved behov.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør. Alle ansatte og autoriserte personer hos Databehandler er underlagt taushetsplikt. Dokumentasjon vises ved anmodning.

Behandling av anmodninger som gjelder de registrertes rettigheter er Behandlingsansvarlig sitt ansvar. Dette gjennomføres i programvaren. Databehandler plikter likevel å bistå den Behandlingsansvarlige (ved hjelp av egnede tekniske og organisatoriske tiltak) å oppfylle plikten til å svare på anmodninger fra registrerte om utøvelse av deres rettigheter.

Databehandleren har en plikt til å bistå den Behandlingsansvarlige med å overholde de forpliktelsene etter personvernforordningen artikkel 32-36 som er relevante i avtaleforholdet.

Databehandler skal ikke levere ut personopplysninger uten den Behandlingsansvarliges uttrykkelige forhåndstillatelse eller det foreligger en lovpålagt plikt til slik utlevering. Som

utlevering etter denne bestemmelse regnes ikke at autorisert personell hos Databehandler, eller dennes underleverandører, gis tilgang til opplysningene.

Databehandler skal ikke ha rettigheter til, eller eierskap over personopplysninger som Databehandler får tilgang til som ledd i oppfyllelse av avtaler.

Databehandler skal ikke overføre personopplysninger til land utenfor EU/EØS (Tredjeland) eller Norge der særlover begrenser dette, uten etter instruksjon fra Behandlingsansvarlig.

5. Bruk av underleverandør

Databehandleren har den Behandlingsansvarliges generelle godkjenning til å bruke andre databehandlere («underleverandører»). Databehandleren må likevel underrette den Behandlingsansvarlige ved eventuelle planer om å skifte ut eller bruke nye underleverandører. Den Behandlingsansvarlige vil motta en slik underretning i god tid før endringen trer i kraft.

Behandlingsansvarlig har rett til å nekte godkjenning av nye underleverandører, og vil i så fall ikke få tilgang til tjenesten den aktuelle underleverandør er tilknyttet.

Samtlige som på vegne av Databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

De underleverandører som den Behandlingsansvarlige har godkjent på tidspunktet for inngåelsen av denne Avtalen fremgår av vedlegg 2.

6. Sikkerhet

Databehandler skal bistå slik at Behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift. Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter personvernforordningen artikkel 32. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle kravene etter personvernforordningen artikkel 28 og denne bestemmelse. Dokumentasjonen skal være tilgjengelig på Behandlingsansvarliges forespørsel.

Avviksmelding etter personvernforordningens artikkel 33 skal skje ved at Databehandler melder avviket til Behandlingsansvarlig uten ugrunnet opphold og senest innen 42 timer etter at Databehandler har fått kunnskap om avviket. Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet. Avviksmeldingen skal inneholde nødvendig informasjon for at Behandlingsansvarlig kan varsle tilsynsmyndigheten, og de registrerte hvis relevant.

7. Sikkerhetsrevisjoner

Databehandler skal årlig gjennomføre sikkerhetsrevisjon av systemer og utstyr som benyttes ved Behandling av Personopplysninger på vegne av Behandlingsansvarlig. Databehandler skal på forespørsel gi Behandlingsansvarlig tilgang til all informasjon som er nødvendig for:

- a) å påvise at Behandlingen skjer i samsvar med Avtalen og Behandlingsansvarliges instruksjer, og

- b) at Behandlingsansvarlig skal kunne oppfylle sine lovpålagte forpliktelser.

Databehandleren må muliggjøre og bidra til revisjoner (slik som inspeksjoner) som gjennomføres av den Behandlingsansvarlige eller en annen inspektør, på fullmakt fra den Behandlingsansvarlige. Revisjonen kan omfatte gjennomgang av organisering, rutiner, sikkerhetstiltak, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Eventuell gjennomføring av revisjon avtales alltid mellom Partene.

8. Avtalens varighet

Avtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

Ved brudd på denne Avtale, dokumenterte instruksjoner fra Behandlingsansvarlig eller personvernlovgivningen kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Avtalen løper parallelt med, og utløper på samme dato som, inngått i Hovedavtalen mellom Databehandler og Behandlingsansvarlig.

9. Ved opphør

Ved opphør av denne Avtalen plikter Databehandler å tilbakelevere alle dokumenter, inkl. kopier, som det har mottatt elektronisk eller fysisk og som inneholder Personopplysninger som omfattes av denne Databehandleravtalen.

Databehandler skal gi Behandlingsansvarlig kopi av alt innhold i databaser og lagringsmedier lignende, som inneholder personopplysninger som er omfattet av denne Databehandleravtalen.

Databehandler skal deretter slette alle Personopplysninger som omfattes av denne Avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Dette skal gjøres i det format som Behandlingsansvarlig bestemmer, så langt dette formatet er tilgjengelig for Databehandler.

Databehandler skal sende skriftlig bekreftelse til Behandlingsansvarlig på at denne bestemmelsen er overholdt innen 30 dager etter avtalens opphør.

10. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til de kontaktpersoner som er definert i Hovedavtalen mellom partene.

11. Lovvalg og verneting

Avtalen er underlagt norsk rett og Partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av Avtalen.

Vedlegg 1 til Databehandleravtale

Oversikt over behandling av personopplysninger

Følgende behandling av personopplysningene kan forekomme:

- I. Arkivering av personopplysninger gjennom drift av ACOS programvare.
- II. Databehandler vil kunne få innsyn i personopplysninger gjennom drift-, brukerstøtte- og vedlikeholdsyttelse på programvare.

Formålet med behandlingen av personopplysninger er å:

- I. være en arkivinstans for Behandlingsansvarlig. Selve behandlingen av personopplysninger, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse blir gjort av Behandlingsansvarlig i programvaren.
- II. holde programvare oppdatert, og bistå kunden med teknisk og funksjonell hjelp. Herunder de tjenester og systemer som er beskrevet i hovedavtalen eller på et senere tidspunkt bestilt av Behandlingsansvarlig.
- III. oppfylle de øvrige forpliktelsene som tilkommer Databehandler etter Hovedavtalen.

2. Programvare som dekkes av avtale

Programvare	I - Avtale gjelder for drift av:	II - Avtale gjelder for brukerstøtte og vedlikehold av
ACOS WebSak m/undermoduler	x	x

3. Behandlingen omfatter

Behandlingen vil kunne omfatte følgende kategorier av registrerte hos

Behandlingsansvarlige, både nåværende og tidligere:

- ansatte, politikere, leverandører og samarbeidspartnere
- Tjenestemottakere, herunder innbyggere og elever

Behandlingen vil kunne omfatte følgende kategorier av personopplysninger:

- navn, telefonnummer, adresse, e-post, bilder, IP-adresser, søknadsinfo, informasjon om saksbehandling og tjenester etterspurt/utført, bruker- og søkerinformasjon, fødselsdato, fødselsnummer, logininformasjon,.
- For WebSak vil det være personopplysninger i henhold til arkivloven

Eventuelt andre kategorier av personopplysninger fylles ut av Behandlingsansvarlig i et eget vedlegg og legges ved denne Avtalen.

Vedlegg 2 til Databehandleravtale Underleverandører

Vedlikeholds- og brukerstøtteytelser

Databehandler benytter ikke underleverandører for å yte vedlikeholds- og brukerstøtteytelser på programvaren.

Driftsytelser

Databehandler benytter **Visolit Norway AS** som underleverandør ved drift av programvare og programvaremoduler. Visolit benytter underleverandører knyttet til den enkelte tjeneste som definert i Visolits Tjenestekatalog. Underleverandør holder til i Norge, og lagrer all informasjon i ACOS-sonen i Norge. Det er etablert en egen ACOS-sone i underleverandørens driftssenter, slik at Behandlingsansvarlig etter denne Avtalen kan benytte ACOS programvare som en driftet tjeneste. Eksempel på driftssenter som benyttes er Green Mountain Data Centre og Microsoft Azure datasenter Region Norway.

Underleverandør er ISO27001 sertifisert i samsvar med krav om rutiner for bevaring av informasjonssikkerhet i personopplysningsloven artikkel 32.

Tilsvarende Databehandleravtale som denne er inngått mellom ACOS AS og underleverandør. ACOS vil være kontaktpunkt for spørsmål til drift av programvare.