

Databehandleravtale

I henhold til personopplysningslovens § 13, jf. § 15 og personopplysningsforskriftens kapittel 2, og senere lovgivning som erstatter disse, herunder EUs personvernsforordning 2016/679 ved ny personopplysningslov som gjennomfører denne i Norge.

mellom

Nord-Odal kommune

behandlingsansvarlig

og

ACOS AS
databehandler

1. Databehandleravtalens hensikt

Databehandleravtalens (avtalen) hensikt er å regulere rettigheter og plikter etter Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven), forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften) og senere lovgivning som erstatter disse, herunder EUs personvernforordning 2016/679 ved ny personopplysningslov som gjennomfører denne i Norge (heretter kalt personopplysningsloven).

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

2. Formål, art og omfang

Følgende behandling av personopplysningene kan forekomme:

- I. Arkivering av personopplysninger og andre sensitive opplysninger gjennom drift av ACOS programvare.
- II. Databehandler vil også kunne få innsyn i personopplysninger gjennom brukerstøtte- og vedlikeholdsytelse på programvare.

Se vedlegg 1 for hvilken programvare som er omfattet av hvilken behandling.

Formålet med behandlingen av personopplysninger:

- I. ved drift av programvare, 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. ved brukerstøtte- og vedlikeholdsytelse av programvare, kan databehandler få innsyn i personopplysninger i programvare som en konsekvens av bistand hos behandlingsansvarlig. Formålet med ytelsene er å holde programvare oppdatert, og bistå kunden med teknisk og funksjonell hjelp.

Behandlingen vil kunne omfatte følgende kategorier av registrerte hos behandlingsansvarlige:

- ansatte
- innbyggere, herunder: elever og lignende
- Leverandører

Behandlingen vil kunne omfatte følgende kategorier av personopplysninger:

- navn, telefonnummer, adresse, e-post, bilder, IP-adresser, søknadsinfo, informasjon om saksbehandling, dybdeopplysninger om person, fødselsdato, fødselsnummer, logininformasjon, tjenester utført, helseinformasjon, sensitiv informasjon og underliggende informasjon.

Det er få begrensninger for hvilke kategorier av personopplysninger og registrerte behandlingsansvarlig kan behandle. Programvare har fritekstfelt og mulighet for arkivering

av vedlegg. Hvis kategorier nevnt ovenfor ikke er utfyllende, er det behandlingsansvarlig sitt ansvar å utdype kategorier av registrerte og personopplysninger i vedlegg 1.

3. Behandlingsansvarliges plikter og rettigheter

Den behandlingsansvarlige er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven (jf. artikkel 24), denne Databehandleravtalen og andre avtaler inngått mellom partene.

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. artikkel 4 nr. 7).

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

Behandlingsansvarlig har ved forespørsel om brukerstøtte en plikt til å skjerme personopplysninger som ikke er nødvendig for bistanden.

Behandlingsansvarlig skal følge prinsippet om dataminimering ved 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 Databehandleravtalen punkt. 2 og vedlegg 1.

All bistand iverksatt av behandlingsansvarlig, inkl. ev. utgifter til 3. part, vil faktureres i henhold til Databehandlers ordinære timesatser.

4. Databehandlers plikter

Databehandler skal følge de rutiner og instruksjoner for behandlingen som behandlingsansvarlig til enhver tid har bestemt skal gjelde. Databehandleren skal kun behandle personopplysninger etter dokumenterte instruksjoner 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 bokstav 3 siste ledd).

Databehandler skal sikre at kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes 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 artikkel 32-36 som er relevante i avtaleforholdet.

Databehandler skal ikke levere ut Personopplysningene 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. Databehandleren må likevel underrette den behandlingsansvarlige ved eventuelle planer om å skifte ut eller bruke nye databehandlere. 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.

Databehandler benytter Telecomputing Norway AS som underleverandør ved drift. TeleComputing benytter underleverandører knyttet til den enkelte tjeneste som definert i TeleComputings Tjenestekatalog.

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.

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.

ACOS vil være kontraktsansvarlig og kontaktpunkt for spørsmål til drift av programvare.

6. Sikkerhet

Databehandler skal bistå til at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift. Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter artikkel 32 ved ny personopplysningslov. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel.

Avviksmelding etter personopplysningslovens artikkel 33 skal skje ved at databehandler melder avviket til behandlingsansvarlig. 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 denne Databehandleravtalen og Behandlingsansvarliges instruksjoner, 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 rutiner, 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 personopplysningsloven 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 statens standard avtaler og andre kontrakter inngått mellom databehandler og behandlingsansvarlig.

9. Ved opphør

Ved opphør av denne Databehandleravtalen 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 Databehandleravtalen. 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 driftsavtalen mellom partene.

11. Lovvalg og vernetting

Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som vernetting. Dette gjelder også etter opphør av avtalen.

Vedlegg 1 til databehandleravtale

Oversikt over behandling av personopplysninger

1.a Drift av programvare

Formålet med behandlingen av personopplysninger ved drift av programvare er å 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.

1.b Brukerstøtte og vedlikehold av programvare

Formålet med behandlingen av personopplysninger ved brukerstøtte- og vedlikeholdsyttelse av programvare er at databehandler kan få innsyn i personopplysninger i programvare som en konsekvens av bistand hos behandlingsansvarlig. Formålet med ytelsene er å holde programvare oppdatert, og bistå kunden med teknisk og funksjonell hjelp. Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang.

2. Programvare som dekkes av avtale

Programvare	1a - Avtale gjelder for drift av:	1.b - Avtale gjelder for brukerstøtte og vedlikehold av
ACOS WebSak med undermoduler		x
- Geointegrasjon pakke 2	x	x
ACOS innsyn	x	x
ACOS CMS		
ACOS Interact og e-skjema	x	x

3. Behandlingen omfatter

Behandlingen vil kunne omfatte følgende kategorier av registrerte hos behandlingsansvarlige:

- ansatte
- innbyggere, herunder: pasienter, elever og lignende
- kunder/medlemmer

Behandlingen vil kunne omfatte følgende kategorier av personopplysninger:

- navn, telefonnummer, adresse, e-post, bilder, IP-adresser, søknadsinfo, informasjon om saksbehandling, dybdeopplysninger om person, fødselsdato, logininformasjon, tjenester utført, sensitiv og konfidensiell informasjon og annen informasjon i henhold til arkivloven.
- For Skjema vil kommunen selv etterspørre personopplysninger i skjemafelt.
- For Innsyn vil det være personopplysninger som ikke er unntatt offentlighet.
- Eventuelt annet (fylles ut av behandlingsansvarlig i et eget vedlegg og legges ved denne avtalen)

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

Behandlingsansvarlig

Databehandler

Sognfua 31.7.18

Sted og dato

Straume 28.06.2018

Sted og dato

Trine J. Hansen
Navn: *Trine J. Hansen*

Stilling: *Ass. Rådgiver*

Anne Gro Hellsten
Navn: Anne Gro Hellsten

Stilling: Markedsdirektør