

Databehandleravtale

Parter:

Databehandler	Behandlingsansvarlig
ASPIT AS Steinsrudvegen 1 3840 Seljord Org.nr: 983 439 977	Indre Fosen Kommune Andre sagmo Org.nr: 974777029

1. Om Avtalen

Denne databehandleravtalen (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Behandlingsansvarlig og Databehandler (heretter omtalt som "partene") etter:

- Lov av 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven);
- Forskrift av 15. juni 2018 nr. 876 om behandling av personopplysninger (personopplysningsforskriften);
- EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen");
- Lov om helseregistre og behandling av helseopplysninger av 20. juni 2014 nr. 43 (helseregisterloven);
- Lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20.juni 2014 nr. 42 (pasientjournalloven); og
- Enhver lov, forskrift eller annet regelverk som erstatter disse.

Ved motstrid mellom Avtalens regulering og de rammer som følger av personopplysningslovgivningen eller relevant helselovgivingen, viker Avtalens regulering.

2. Definisjoner

Begrepene "personopplysninger", "behandling", "behandlingsansvarlig", "databehandler", "brudd på opplysningssikkerhet" og "helseopplysninger" skal forstås slik de er definert i personvernforordningen artikkel 4, helseregisterloven § 2 og pasientjournalloven § 2 som gjeldende.

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

3. Avtalens bakgrunn og formål

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

Formålet med Avtalen er å sikre at helse- og personopplysningene ikke brukes urettmessig eller kommer uberettigede i hende.

Behandlingens art og formål

Avtalen gjelder levering av Online pasientjournalssystem fra ASPIT. Databehandlers formål er begrenset til å lagre opplysningene og å gjøre dem tilgjengelige utelukkende for behandlingsansvarlig. Databehandler er ansvarlig for drift, oppdatering og vedlikehold av programvaren, samt daglig sikkerhetskopiering av data.

Behandlingsansvarlig er eier av innholdet i sin database og er alene ansvarlig for innsamling, registrering, korrigerings, sletting, utlevering og bruk av helse- og personopplysninger.

Kategorier av registrerte:

Ansatte, pasienter, pårørende, kunder, kontakter og samarbeidspartnere.

Kategorier av personopplysninger:

Kontaktopplysninger, pasientjournaler, kartotekopplysninger, samt alle kategorier av helse- og personopplysninger som Behandlingsansvarlig trenger for å utøve sitt virke.

4. Rammene for behandling av helse- og personopplysninger

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

5. Behandlingsansvarliges plikter

Behandlingsansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen, relevant helselovgivning og annen

særlovgivning. Behandlingsansvarlig skal følge de sikkerhetsrutiner som måtte pålegges fra Databehandler i forbindelse med bruken av Online pasientjournalssystem fra ASPIT.

Databehandler forutsetter at Behandlingsansvarlig har et forsvarlig sikkerhetsnivå på lokalt utstyr, og følger Norm for informasjonssikkerhet i helse - omsorgs - og sosialsektoren (Normen).

Det er Behandlingsansvarliges ansvar å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte i sin database.

6. Databehandlers plikter

Generelt

Databehandler forplikter seg til å behandle helse- og personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen og "Norm for informasjonssikkerhet i helse- og omsorgstjenesten". Databehandler skal ikke ved noen handling eller unnlatelse, sette Behandlingsansvarlig i en slik situasjon at Behandlingsansvarlig bryter noen bestemmelse i gjeldende lov og regelverk. Databehandler må omgående underrette Behandlingsansvarlig dersom Databehandler mener noen handling eller unnlatelse er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger eller annen lovgivning.

Databehandler skal ikke:

- I. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til avtalen;
- II. utlevere, overlate eller overføre helse- og personopplysninger i noen form med mindre Behandlingsansvarlig har godkjent dette skriftlig.
- III. bruke andre databehandlere, med mindre Behandlingsansvarlig på forhånd har godkjent dette skriftlig.

Databehandler skal:

- I. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;
- II. gi Behandlingsansvarlig nødvendig bistand til å oppfylle plikten til å svare på anmodninger fra registrerte om utøvelsen av deres rettigheter idet det tas hensyn til behandlingens art og den informasjon som er tilgjengelig for Databehandler.
- III. pålegge eventuelle andre databehandlere de samme forpliktelsene som er fastsatt i denne databehandleravtalen gjennom en skriftlig avtale. Dersom den andre databehandleren ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, har Databehandler det fulle ansvaret ovenfor Behandlingsansvarlige.

Tekniske, organisatoriske og sikkerhetsmessige tiltak

Databehandler plikter å treffe og gjennomføre alle nødvendige og adekvate planlagte og systematiske tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er tilfredsstillende informasjonssikkerhet ved behandling av helse- og personopplysninger. Databehandler er ansvarlig for at tekniske løsninger og rutiner hos Databehandler til enhver tid er i henhold til offentlige krav med hensyn til behandling av sensitive personopplysninger.

Databehandleren skal:

- I. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av helse- og personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovgivningens bestemmelser;
- II. ha gode og hensiktsmessige internkontrollrutiner;
- III. ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av avtalen får slik tilgang.
- IV. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten blant annet rutiner for avviksmelding, og skal på forespørsel gi Behandlingsansvarlig tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av helse- og personopplysninger;
- V. avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på opplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;
- VI. ha på plass rutiner og systematiske tiltak for oppfølging av avvik, herunder tiltak for gjenoppretting av normal tilstand, fjerning av årsaken til avviket og hindre gjentakelse.
- VII. ved mistanke om eller konstatering av avvik, omgående varsle Behandlingsansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket.

7. Overføring av personopplysninger til utlandet

Ingen av helse- og personopplysningene som behandles under denne Avtalen skal føres ut av Norge, alle helse- og personopplysninger er plassert på servere i Norge.

8. Taushetsplikt

Databehandlers ansatte, er underlagt taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle personopplysningene forplikter seg til å behandle opplysningene fortrolig. Databehandler skal påse at alle som behandler personopplysninger under Avtalen er kjent med taushetsplikten.

Ansatte skal ha undertegnet taushetserklæring. Taushetsplikten gjelder også etter Avtalens opphør.

9. Innsyn, verifikasjon og revisjon

Behandlingsansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Databehandlers behandling av personopplysninger tilhørende Behandlingsansvarlig. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Databehandler på vegne av Behandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov.

Databehandler gjennomfører årlige sikkerhetsrevisjoner for systemer som omfattes av denne avtalen.

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

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

10. Avtalens varighet

Behandlingen er ikke tidsbegrenset og varer inntil avtalen sies opp av en av partene. Avtalen er løpende uten bindingstid eller oppsigelsestid for Behandlingsansvarlig. Behandlingsansvarlig kan si opp avtalen og betaler da ut den måned man står i ved oppsigelse. Dersom Behandlingsansvarlig ønsker kundeforholdet gjenopprettet innen 6 mnd etter oppsigelse tilkommer det gebyr på gjenoppstart av abonnement.

Databehandler kan si opp avtalen med 6 måneders varsel.

Ved opphør av denne avtalen skal alle data leveres Behandlingsansvarlig og deretter slettes forsvarlig hos Databehandler.

11. Teknisk omfang og leveransenivå

Online pasientjournalssystem fra ASPIT leveres som en fjerndriftet applikasjon der brukerne kobler seg til ved bruk av Citrix-klient på lokal pc/Mac. Behandlingsansvarlig er selv ansvarlig for at lokalt utstyr som pc/Mac, skriver og lignende fungerer etter hensikten. Behandlingsansvarlig er også ansvarlig for sin tilknytning til Internett.

Databehandler tar sikkerhetskopi av dataene hver natt utenom natt til mandag til egen lagringsenhet for rask gjenoppretting. I tillegg kopieres sikkerhetskopi ut av hus til en annen enhet på annen geografisk lokasjon for å sikre rask gjenoppretting ved katastrofe. På ekstern lokasjon oppbevares også versjonshistorikk etter GFS-prinsippet som sikrer historikk på data. All håndtering av sikkerhetskopi skjer kryptert for å sikre dataenes integritet og konfidensialitet.

Online pasientjournalssystem fra ASPIT tilfredsstiller Nivå 4 Høyt som er Normens høyeste sikkerhetsnivå for autentisering. Tjenesten benytter autentisering med brukernavn/passord og smartkort med pinkode fra buypass eller BankID og BankID på mobil. Tjenesten tilfredsstiller med dette også Datatilsynets retningslinjer for autentisering mot datasystem inneholdende sensitive personopplysninger.

Online pasientjournalssystem fra ASPIT leveres med en garantert tilgjengelighet på 99,5% målt over ett år i kjernetiden som er definert fra kl 08.00 til 16.00 på virkedager. Løsningen vil normalt være tilgjengelig til enhver tid, men kan utenfor kjernetiden tas midlertidig ned for vedlikehold. Slikt vedlikehold skal om mulig meldes Behandlingsansvarlig i forkant.

Databehandler benytter ikke underleverandører for leveransen av Online pasientjournalssystem.

Databehandler er ikke ansvarlig for forsinkelser eller mislighold av sine forpliktelser når disse skyldes omstendigheter utenfor Databehandlers rimelige kontroll.

12. Lovvalg og verneting

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

13. Betingelser

Databehandler kan med 3 måneders varsel gjøre endringer i avtalens priser. Mindre løpende justeringer ihht konsumprisindeks eller annen markedsendring kan foretas uten varslings.

Tilgang til Online-tjenesten forutsetter at Behandlingsansvarlig har brukerlisenser og et gyldig abonnement til programvaren.

Behandlingsansvarlig må varsle Databehandler om endringer i brukertilganger slik at det til enhver tid er samsvar mellom brukere hos Behandlingsansvarlig og brukertilganger i programmet.

Databehandler står for drift av Online-tjenesten og fakturerer for dette.

ASPIT AS
(Databehandler)

(Behandlingsansvarlig)



Dagligleder

Navn, tittel, sted/dato

Navn, tittel, sted/dato

Signatur sertifikat

Dokument navn:

Databehandleravtale

Unikt dokument Id:

3bdce341-15fc-4fa0-8508-30a00852

Dokument fingeravtrykk:

da0fb960e9edf816114dd3cc495d0bf904b3f6969ec29126b2cc2f5141a1b5f62d
26e6fc429bbf6b039814ac8450b8490e18fbcf88a1df6d3893ae921e44e64e

Undertegnede



Andre sagmo

Indre Fosen Kommune

Epost: andre.sagmo@indrefosen.kommune.no

Enhet: Chrome 80.0 on Windows 10 (desktop)

IP adresse: 185.49.197.109

IP Lokasjon: Rissa, Trøndelag, Norway

Signert med BankID : Sagmo, Andre
(19651006)

Tillitsfullt tidsstempelt:
2020-10-23 07:30:52 UTC

Dette dokumentet ble gjennomført av alle parter på:

2020-10-23 07:30:52 UTC



Revisjonslogg

Tillitsfullt tidsstemplet

2020-10-23 07:30:52 UTC

2020-10-23 07:30:44 UTC

2020-10-22 13:30:39 UTC

2020-10-22 13:30:19 UTC

2020-10-22 13:29:20 UTC

2020-10-22 13:29:05 UTC

2020-10-22 12:46:55 UTC

2020-10-22 12:46:55 UTC

2020-10-22 12:46:54 UTC

2020-10-22 12:46:42 UTC

2020-10-22 12:46:26 UTC

Hendelse med innsamlede revisjonsdato

Dokument ble signert av Andre sagmo (andre.sagmo@indrefosen.kommune.no)
Enhet: Chrome 80.0 on Windows 10 (desktop)
IP adresse: 185.49.197.109 - IP Lokasjon: Rissa, Trøndelag, Norway

Dokument ble godkjent via eid:bankid-no av Andre sagmo
(andre.sagmo@indrefosen.kommune.no)
Enhet: Microsoft Edge 80.0.361.69 on Windows 10 Unknown (desktop)
IP adresse: 185.49.197.109 - IP Lokasjon: Rissa, Trøndelag, Norway

Dokument ble gjennomgått av Andreas Fossan (andreas@fosenikt.no)
Enhet: Chrome 86.0 on Windows 10 (desktop)
IP adresse: 82.194.217.1 - IP Lokasjon: Rissa, Trøndelag, Norway

Dokument ble åpnet av Andreas Fossan (andreas@fosenikt.no)
Enhet: Chrome 86.0 on Windows 10 (desktop)
IP adresse: 82.194.217.1 - IP Lokasjon: Rissa, Trøndelag, Norway

Dokument ble gjennomgått av Andre sagmo
(andre.sagmo@indrefosen.kommune.no)
Enhet: Chrome 80.0 on Windows 10 (desktop)
IP adresse: 185.49.197.109 - IP Lokasjon: Rissa, Trøndelag, Norway

Dokument ble åpnet av Andre sagmo (andre.sagmo@indrefosen.kommune.no)
Enhet: Chrome 80.0 on Windows 10 (desktop)
IP adresse: 185.49.197.109 - IP Lokasjon: Rissa, Trøndelag, Norway

Dokument ble sendt til Bettina vangen
(bettina.vangen@indrefosen.kommune.no)

Dokument ble sendt til Andreas Fossan (andreas@fosenikt.no)

Dokument ble sendt til Andre sagmo (andre.sagmo@indrefosen.kommune.no)

Dokument ble forseglet av Steinar Andersen (steinar@aspit.no)

Dokument ble opprettet av Steinar Andersen (steinar@aspit.no)
IP adresse: 85.222.150.8 - IP Lokasjon: Paris, Île-de-France, France

