DOSSIERSOLUTIONS

Databehandleravtale

Databehandleravtale

Det er [dato] inngått følgende databehandleravtale («Avtalen») mellom:

mellom

RADØY kommune
Org.nr: 954748634
Behandlingsansvarlig

og

Dossier Solutions AS
(Org.nr. 981 594 118)
Databehandler

Denne avtale er signert elektronisk, og hver av partene beholder hver sin kopi.

Dossier AS

.....
Even Harket, COO

Radøy kommune 14.09.2018

Grete Algrøy Herøy.
kommunalsjef helse og omsorg
for rådmann Jarle Landås

(A) Kommunen er Behandlingsansvarlig

(B) Dossier Solutions AS, org.nr. 981 594 118, Rådhusgata 30B, 0151 OSLO, er Databehandler (heretter benevnt «Dossier»)

(C) Kommunen og Dossier Solutions AS benevnes samlet «Partene» og separat som «Part».

1. Avtalens bakgrunn og omfang

1.1 Kommunen har tatt i bruk kompetansesystemet Dossier som er en IKT-løsning der Leger i Spesialisering Del I (LIS1), leder, veileder og supervisør, i Kommunen, skal kunne registrere oppnåelse av læringsmål, ref Forskrift om spesialistutdanning og spesialistgodkjenning for leger og tannleger (Spesialistforskriften). IKT-løsningen er utviklet i samarbeid mellom helseregionene og Helsedirektoratet og er basert på samme IKT-løsning for oppfølging av LIS i helseregionene. Bruken av IKT-løsningen innebærer at Dossier i en rolle som databehandler, på vegne av KOMMUNENs ansatte leger i spesialisering, behandler personopplysninger som angitt i punkt 2 under.

1.2 For de personopplysninger som behandles, er Dossier databehandler i relasjon til personopplysninger som behandles på vegne av KOMMUNEN og dennes ansatte.

1.3 De personopplysninger som behandles av Dossier omfatter de kategorier av personopplysninger og de kategorier av registrerte personer som er angitt i punkt 2 under, og behandlingen skal kun skje i henhold til de formål med behandlingen som er angitt der.

1.4 Ved "personopplysning" forstås enhver form for informasjon om en identifisert eller identifiserbar fysisk person, jf. artikkel 4(1) i Forordning (EU) 2016/679 av 27. april 2016 («Personvernforordningen»). Behandlingen som foregår etter denne Avtalen og i og med gjennomføringen av Tjenesteavtalen, skal skje i henhold til Gjeldende personvernrett, Personopplysningsloven inkludert Personvernforordningen, nasjonale særregler og forskrifter for personvern som er relevant for KOMMUNEN eller Dossier. «Gjeldende personvernrett» inkluderer bindende veiledninger, avgjørelser eller vedtak fra myndigheter, domstoler eller andre relevante organer.

2. Behandling av personopplysninger. Formål med behandlingen.

2.1 Dossier leverer tjenester («Tjenester») til KOMMUNEN som innebærer behandling av personopplysninger som normalt inngår i et personalregister. Dossier skal levere de Tjenester som er spesifisert i Vedlegg C. Dossier skal ikke behandle personopplysninger på annen måte enn det som er nødvendig for leveransen av de Tjenester som Dossier leverer til KOMMUNEN og skal ikke benytte personopplysningene til noe annet formål, med mindre annet formål er skriftlig avtalt i Vedlegg A til denne Avtalen eller inntatt i andre skriftlige instrukser fra KOMMUNEN. KOMMUNEN bestemmer formålene og virkemidlene for all behandling av personopplysninger som foretas av Dossier. Instruksen fra KOMMUNEN knyttet til behandlingen kan endres i Avtalens løpetid.

2.2 Rammene for Dossier's behandling av personopplysninger på vegne av KOMMUNEN følger denne Avtalen mellom partene, og er oppgitt i Vedlegg A-C til denne avtalen.

3. Dossier's plikter

3.1 Dossiers innestår for at den behandling av personopplysninger som gjøres på KOMMUNENs vegne til enhver tid skal være i tråd med Gjeldende personvernrett og eventuelle pålegg fra kompetente offentlige myndigheter.

3.2 I den grad det følger en plikt til dette i henhold til GDPR artikkel 30, skal Dossier, utover innholdet av denne Avtalen, løpende føre protokoll over sin behandling av personopplysninger i henhold til GDPR artikkel 30.

Dossier plikter til enhver tid å gi KOMMUNEN tilgang til slik protokoll samt sin øvrige sikkerhetsdokumentasjon og bistå KOMMUNEN å ivareta KOMMUNENs ansvar etter Gjeldende Personvernrett og pålegg fra offentlige myndigheter.

3.3 Dossier skal på forespørsel bistå ved utarbeidelse av konsekvensutredning etter GDPR artikkel 35.

3.4 Dossier skal kun behandle personopplysningene etter KOMMUNENs konkrete og dokumenterte instrukser og i henhold til formålet og rammene som er avtalt med KOMMUNEN. Dataene skal ikke benyttes i andre sammenhenger enn angitt i denne Avtalen, herunder overføre personopplysningene til et tredjeland eller en internasjonal organisasjon, med mindre Dossier er forpliktet til dette etter Gjeldende Personvernrett. I så fall skal Dossier skriftlig gi KOMMUNEN beskjed om denne juridiske forpliktelsen forut for at behandlingen påbegynnes, med mindre gjeldende lovgivning forbyr slik beskjed.

3.5 Dossier skal ikke gjennomføre overføring av personopplysninger til et tredjeland eller til internasjonale organisasjoner, uten at KOMMUNEN har gitt sin skriftlige tillatelse til dette. Dersom overføring av KOMMUNEN personopplysninger skal skjer til et tredjeland, skal Dossier bistå KOMMUNEN i å sørge for lovlig overføringsgrunnlag.

3.6 Hvis Dossier skjønner at en instruks fra KOMMUNEN er i strid med Gjeldende Personvernrett i lovgivningen i en medlemsstat skal Dossier omgående orientere KOMMUNEN skriftlig om dette.

3.7 Dossier kan ikke utlevere personopplysninger til andre eksterne parter uten at dette fremgår av Avtalen, eller annen lovlig grunnlag inkludert avtale eller samtykke til dette fra KOMMUNEN. Dossier skal løpende bistå KOMMUNEN med å oppfylle forpliktelser etter Gjeldende Personvernrett, herunder, men ikke begrenset til, KOMMUNENs forpliktelser til å svare på forespørsler om innsyn, korrigering, begrensning av behandling og sletting av personopplysninger fra sine brukere og ansatte, samt retten til å få oversendt kopi av de personopplysninger som behandles.

3.8 Dossier skal opprettholde et sikkerhetsnivå for behandlingen av personopplysningene som er tilstrekkelig i forhold til risikoen ved Behandlingen. Dossier skal beskytte personopplysningene fra ødeleggelse, endring, ikke-autorisert utlevering, eller ikke-autorisert tilgang. Dossier skal treffe de nødvendige tekniske og organisatoriske sikkerhetstiltak for å hindre at personopplysningene som behandles;

(i) utilsiktet eller ulovlig tilintetgjøres, tapes eller endres,

(ii) videregis eller gjøres tilgjengelige uten autorisasjon eller

(iii) for øvrig behandles i strid med lovgivningen, herunder personvernforordningen.

3.9 Dossier skal videre overholde de krav til sikkerhetstiltak som direkte forplikter Dossier, herunder lovmessige krav til sikkerhetstiltak i det land Dossier er etablert eller det land behandlingen skjer. Vedlegg B til databehandleravtalen angir videre KOMMUNENS krav til sikkerhet, i henhold til Norm for informasjonssikkerhet.

3.10 Dossier plikter å gjennomføre årlige sikkerhetsrevisjoner av informasjonssystemet de benytter i ledd av arbeidet de utfører på vegne av KOMMUNEN og som er relevant for denne avtalen. Resultatet av denne sikkerhetsrevisjonen skal gjøres tilgjengelig for KOMMUNEN på forespørsel. KOMMUNEN har rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette hos Dossier. Dossier plikter å gi nødvendig bistand til dette og skal, snarest mulig besvare konkrete spørsmål fra KOMMUNEN samt dokumentere sin etterlevelse av denne Avtalen.

3.11 Dersom den Registrerte, myndigheter eller andre ber om informasjon fra Dossier vedrørende Behandlingen av Personopplysninger i medhold av denne Avtalen, skal Dossier henvise forespørselen til KOMMUNEN. Dossier skal ikke, uten forutgående instruksjoner fra KOMMUNEN, overføre eller på annen måte utlevere Personopplysninger eller annen informasjon knyttet til Behandlingen av Personopplysninger til en tredjepart. Leverandøren skal uten unødig forsinkelse skriftlig orientere KOMMUNEN om;

(i) enhver forespørsel fra en myndighet om utlevering av personopplysninger omfattet av Avtalen er forbudt i henhold til EU-retten eller lovgivningen i en medlemsstat,

(ii) Ved Sikkerhetsbrudd som involverer Personopplysninger skal Leverandøren skriftlig varsle KOMMUNEN uten ugrunnet opphold etter at Leverandøren har fått kunnskap om Sikkerhetsbruddet. Varselet skal som et minimum:

- Beskrive typen Sikkerhetsbrudd, herunder, hvis mulig, kategoriene av og omtrentlig antall Registrerte og personopplysningsposter som er berørt;
- Inneholde navnet og kontaktopplysningene til vedkommende som kan kontaktes for mer informasjon;
- Beskrive sannsynlige konsekvenser av Sikkerhetsbruddet;
- Beskrive de tiltak som er tatt eller foreslås tatt av den Behandlingsansvarlige for å håndtere Sikkerhetsbruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av Sikkerhetsbruddet.

Kontaktpunkt for varsling av Sikkerhetsbrudd bør avtales.

(iii) Enhver anmodning om innsyn i personopplysningene mottatt direkte fra den registrerte eller fra tredjemann.

3.12 Fysiske plassering av servere, servicesentre mv., som inngår i utførelse av databehandlingen er gitt i Vedlegg A.

Dossier forplikter seg til å gi skriftlig varsel til KOMMUNEN minst 1 måned forut for endringer av den fysiske plassering.

4. Bruk av underleverandør

4.1 Dossier kan kun benytte underleverandør til behandling av personopplysninger omfattet av Avtalen, når underleverandøren har gitt tilstrekkelige garantier for at den vil gjennomføre tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i Gjeldende personvernrett og vern av den registrertes rettigheter. De(n) underleverandør som benyttes ved oppstart av Avtalen, er angitt i Vedlegg A. Databehandleren skal informere Behandlingsansvarlige om eventuelle planer om tilsetning eller utskiftning av underleverandører.

4.2 Dossier skal forut for bruk av en underleverandør inngå en skriftlig avtale med underleverandøren, hvor underleverandøren som minimum pålegges de samme forpliktelser som Leverandøren har påtatt seg ved Avtalen, herunder plikt til å gjennomføre passende tekniske og organisatoriske tiltak til sikring av at behandlingen oppfyller kravene i personvernforordningen.

4.2 Dossier hefter fullt ut overfor KOMMUNEN for underleverandørens oppfyllelse av sine personvernforpliktelser.

5. Fortrolighet

5.1 Dossier skal holde personopplysningene fortrolige.

5.2 Dossier skal ikke formidle personopplysningene til noen eller ta kopi av personopplysningene, med mindre dette er absolutt nødvendig for å ivareta Dossier sine forpliktelser overfor KOMMUNEN etter Avtalen og forutsatt at den som personopplysningene overlates til er kjent med opplysningenes fortrolige karakter og har lovet å holde personopplysningene fortrolige i overensstemmelse med Avtalen.

5.3 Bestemmelsene om fortrolighet i Avtalen skal gjelde for enhver av Dossier sine medarbeidere og Dossier står inne for at medarbeiderne overholder Avtalen.

5.4 Dossier skal begrense tilgangen til personopplysningene til de medarbeidere som må ha adgang til personopplysninger for å kunne oppfylle Dossier sine forpliktelser overfor KOMMUNEN.

5.5 Dossier sine forpliktelser etter dette punkt 5 består uten tidsbegrensning og uansett om Partenes samarbeid for øvrig måtte være opphørt.

5.6 KOMMUNEN skal behandle opplysninger som mottas fra Dossier fortrolig, og må ikke uberettiget utnytte eller videregi de fortrolige opplysningene. Fortrolig informasjon, inkludert konkurransesensitiv informasjon, skal ikke tilflyte noen andre enn de som har behov for tilgang til slik informasjon for å oppfylle kravene i denne Avtalen, og aldri til tredjemenn.

6. Endringer og overdragelser

6.1 Partene kan til enhver tid avtale å endre Avtalen. Endringer skal være skriftlige.

6.2 Dossier skal ikke overdra sine rettigheter og forpliktelser i henhold til Avtalen uten KOMMUNENs forutgående skriftlige samtykke.

6.3 Dersom Dossier er av den oppfatning at behandlingen etter KOMMUNENs instruks er i strid med Gjeldende Personvernrett, skal Dossier søke å melde ifra til KOMMUNEN slik at KOMMUNEN kan endre instruksen.

7. Varighet og opphør av Avtalen

7.1 Avtalen trer i kraft ved begge Parters underskrift og er gjeldende inntil den sies opp eller oppheves av en av Partene.

7.2 Uansett Avtalens formelle avtaleperiode skal Avtalen gjelde så lenge Dossier behandler personopplysninger for KOMMUNEN.

7.3 I tilfelle opphør av Avtalen, uansett det juridiske grunnlaget for oppsigelsen, skal Dossier yte nødvendige overgangstjenester til KOMMUNEN i henhold til Vedlegg B. Etter opphør av Avtalen skal Dossier, etter KOMMUNENs valg, enten slette eller tilbakelevere personopplysningene til KOMMUNEN. Tilbakelevering av personopplysninger vil skje på maskinlesbart format.

8. Rangordning

8.1 I tilfelle uoverensstemmelser mellom bestemmelsene i Avtalen og bestemmelsene i andre skriftlige eller muntlige avtaler inngått mellom Partene, skal bestemmelsene i Avtalen ha forrang. Bestemmelsene i punkt 3 kan ikke brukes i det omfang det er fastsatt strengere forpliktelser for Dossier ved annen avtale mellom Partene. I tillegg har avtalen ikke anvendelse i det omfang det er fastsatt strengere forpliktelser for Dossier og/eller underleverandører ved bruk av Kommisjonens standardkontrakter til overføring av personopplysninger til tredjeland.

***

Vedlegg A: Instruks for behandling

Rammene for Dossier's behandling av personopplysninger på vegne av KOMMUNEN er:

1.1 Karakteren av databehandlingen

Behandlingsaktiviteter er oversikt over LIS 1 utdannelsens læringsmål samt registrering og lagring av læringsaktiviteter for å dokumentere oppfyllelse av læringsmålene.

1.2 Kategorier av registrerte personer

LIS1, leder, veileder og supervisør.

1.3 Kategorier av personopplysninger

Dossier Information Security Management System (ISMS) kategoriserer data på følgende måte:

Level	Definition
Confidential	Should only be made available to the appropriate member in Dossier Solutions. Information Classifies as Confidential should never leave the company premises, or be shared digitally outside the organisations.
Internal	Only accessible to members of Dossier Solutions, Internal Documents that needs to be shared with Partners, need CISO/COO approval.
Public	Can be disclosed to any member of the public.

Data som behandles under denne avtalen er kategorisert som følger:

Datagruppe	Beskrivelse	Klassifisering
Brukerdata	Data som identifiserer brukeren basert på HelseID og forutsetter at brukeren har et HPR-nummer. Registrering er LIS1 eller basert på forespørsel fra LIS1	Confidential
Læringsmål	Læringsmål som beskriver krav til innhold i utdanningen til en LIS1	Confidential
Læringsaktiviteter	Læringsaktiviteter, med registrering av informasjon om tilhørende status, som dokumenterer innfrielse av ett eller flere læringsmål.	Confidential

1.4 Særlige kategorier av personopplysninger

Dossier behandler ingen særlige kategorier av personopplysninger.

1.5 Lokasjon for databehandler

Rådhusgata 30 B, 0151 Oslo, Norge.

1.6 Lokasjon for Underleverandør

Evry Norge AS, Postboks 639, 2810 Gjøvik

Org-nr: 934 382 404

Drift/infrastruktur inkludert lagring og sikkerhetskopier av database.

1.7 Produktforbedring

Dossier har, under denne avtalen, rett til å kartlegge bruksmønstre og karakteristika i løsningen for produktforbedring og videreutvikling av løsningen.

Kartleggingen vil ikke innebære behandling av personopplysninger. Dossier forbeholder seg alle rettigheter til kunnskapen som følger av en slik avlesning og analyse av data.

1.8 Uttrekk av data for Helsedirektoratet

Data som behandles under denne Databehandleravtalen på nærmere avtalt frekvens oversendes til HDIR for deres rapporteringer og analyser i forbindelse med HDIR's forskriftsfestede ansvar for oppfølging av helhet og kvalitet i utdanningen (ref. Forskrift om spesialistutdanning og spesialistgodkjenning for leger og tannleger). Datatyper som overføres er de samme som helseregionene overfører til HDIR.

1.9 Meddelelser

Henvendelser fra KOMMUNEN til Dossier kan gjøres på www.liskommune.no.

Vedlegg B – Detaljerte krav til informasjonssikkerhet

Nr	Tema	Krav
1	Norm for informasjonssikkerhet i helse- og omsorgssektoren	Databehandler skal følge relevante krav i Norm for informasjonssikkerhet (se faktaark 6b, og hvilke krav som er angitt for databehandler)
2	ISMS / styringssystem	Databehandler skal ha et styringssystem for informasjonssikkerhet som sikrer at databehandleren på en systematisk og dokumentert måte iverksetter og følger opp informasjonssikkerhet i virksomheten i tråd med relevante krav akseptabel risiko. Styringssystemet skal være basert på anerkjente standarder.
3	Sikkerhetsrevisjon	Databehandler skal gjennomføre interne revisjoner av informasjonssikkerhet jevnlig. Dokumentasjonen skal være tilgjengelig for Behandlingsansvarlig. Behandlingsansvarlig har adgang til å gjennomføre sikkerhetsrevisjoner av informasjonssikkerhet hos databehandler. Revisjon skal varsles minimum 14 dager før. Behandlingsansvarlig kan også benytte tredje part for gjennomføring av sikkerhetsrevisjon hos databehandler. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig. Retten til revisjon inkluderer testing av tekniske, organisatoriske og fysiske sikkerhetstiltak.
4	Sikring av data	Databehandler skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet.
5	Fjernaksess	Kravene i Normens fjernaksessveileder skal følges.
6	Tilgangsstyring	I utgangspunktet skal ikke Databehandler ha tilgang til innholdet i Behandlingsansvarliges data, med mindre dette er nødvendig for å oppfylle forpliktelsen Databehandler har. I slike tilfeller skal kun personell hos Databehandler med tjenstlig behov ha tilgang. Tilgang skal logges, og det skal vises til en begrunnelse for tilgang. For brukere med privilegerte tilganger, uavhengig om dette gir direkte tilgang til Behandlingsansvarliges data, skal denne brukeren være personlig, strengt begrenset og kontrollert, og med tilhørende nødvendige sikkerhetstiltak.
7	Autentisering	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Databehandler skal ha etablert passordpolicy. Behandlingsansvarlig kan stille spesifikke krav til autentisering, f.eks. at sterk autentisering skal benyttes.
8	Tiltak mot digitale angrep	Databehandler skal implementere tiltak mot digitale angrep som f.eks. tjenestenektangrep og skadelig kode.
9	Logging og sporbarhet	Databehandler skal implementere logging som viser tilgang til Behandlinganansvarliges data, og hvilke operasjoner som Databehandler har utført på dataene. Loggene skal sikres mot uautorisert innsyn, endring og

Nr	Tema	Krav
		sletting. Oppbevaringstid skal bestemmes ut fra formålet med loggingen.
10	Redundans og skalering	Databehandler skal ha en infrastruktur som sikrer kapasitet og oppetid i tråd med avtalt tjenestenivå gjennom tiltak som redundans og skalering.
11	Testdata	Behandlingsansvarliges data skal ikke benyttes for testformål uten at det er avtalt skriftlig med Behandlingsansvarlig. Eventuell anonymisering skal skje på instruks fra Behandlingsansvarlig. I tilfeller der Behandlingsansvarliges data benyttes til test etter avtale, skal disse sikres på samme måte som produksjonsdata. Der det benyttes produksjonsdata til testformål, skal disse slettes etter at test er utført.
12	Sletting og tilbakelevering	Databehandler skal ha rutiner og tekniske løsninger som sikres at alle Behandlingsansvarliges data slettes eller leveres tilbake på instruks fra Behandlingsansvarlig, eller ved opphør av databehandleravtale. Dette omfatter også data lagret på backupmedia og logger.
13	Lagringstid	Lagring av opplysninger skal bestemmes av Behandlingsansvarlig ut fra formålet med behandlingen. Når formålet med behandlingen er oppnådd skal opplysningene slettes i henhold til punkt nr. 12 i dette vedlegget.
14	Backup og restore	Databehandler skal ha forsvarlige backup- og restorerutiner som testes regelmessig.
15	Kryptering ved lagring	Data skal krypteres ved lagring hvis Behandlingsansvarlig stiller krav om dette.
16	Kryptering i kommunikasjon	Data skal alltid krypteres i kommunikasjon i hht NSM spesifikasjoner.
17	Adgangskontroll	Databehandler skal ha tilstrekkelig fysisk sikring hvor Behandlingsansvarliges data er tilgjengelig.
18	Sikkerhetsarkitektur	Databehandler skal separere data som tilhører forskjellige kunder. Databehandlers egne data skal separeres fra kundenes data. Databehandler skal ha rutiner som sikrer at Behandlingsansvarliges data ikke overføres til andre virksomheter uten at dette er godkjent av Behandlingsansvarlig.
19	Autorisasjonsregister	Databehandler skal til enhver tid ha et oppdatert autorisasjonsregister for personell som er autorisert for tilgang til Behandlingsansvarliges informasjon og tjenester.

Vedlegg C – Beskrivelse av tjenestene

LIS1 har tilgang til Dossier Kompetanseportal funksjonalitet som beskrevet på websiden: www.liskommune.no.

Kompetansportalen tilgjengeliggjøres som en tjeneste Software as a service (SaaS) der Dossier står for all drift og hardware, og LIS1 trenger kun å ha nettleser og nettilgang for å bruke applikasjonen. SaaS-installasjonene har alltid siste tilgjengelige versjon.

Driftstjenestene baserer seg på ITIL (IT Infrastructure Library). Rammeverket ivaretar og beskriver nødvendige prosedyrer, rutiner og rollebeskrivelser for å utøve sikre leveranser av driftstjenester, blant annet:

- Servere er plassert i sikrede serverrom med adgang kun for autorisert personell
- Backup-rutiner
- Redundant strøm og kjøling
- Tilgang inn fra Internett via redundante linjer og brannmur
- Applikasjonen aksesseres via kryptert forbindelse (https)