M-02-3 Databehandleravtale – databehandler/underleverandør av Helse Vest IKT AS

mellom

Helse Vest IKT AS, org.nr. 987 601 787
(databehandler)

og

DIPS AS
(underleverandør til databehandler), org. nr. 979 543 883

System: DIPS Interactor Sky

i henhold til personvernforordningen art 28 nr. 2 og nr.4 vedrørende bruk av databehandlere/underleverandører av Helse Vest IKT AS

1. Avtalens hensikt og formål

Denne avtalen (Databehandleravtalen) regulerer Helse Vest IKT AS bruk av underleverandører ved behandling av helse –og personopplysninger som skjer på vegne av Behandlingsansvarlig, heretter kalt Dataansvarlig, jf. personvernforordningen art 28 nr. 2.

Formålet med denne avtalen er å regulere underleverandørens behandling av personopplysninger på vegne av Dataansvarlig. Videre skal den regulere partenes rettigheter og plikter ved behandling av personopplysninger, jf. personvernforordningen art 28 nr.3.

Formålet med systemet/løsningen er:

Tilby funksjoner og tjenester for bestilling av og henvisning til medisinske tjenester hos spesialisthelsetjenesten, fra primærhelsetjenesten. DIPS Interactor integrerer fagsystemer som benyttes av aktørene i helsesektoren gjennom bruk av tradisjonell meldingsbasert samhandling kombinert med interaktive tjenester. Overordnet består produktet av løsninger for tjenesteyter, for bestiller (rekvirent, henviser) og sentrale komponenter i Norsk Helsenett. Komponentene for bestiller og tjenesteyter er godt integrert med fagsystemene de benytter. En viktig funksjon i DIPS Interactor er dynamiske tjenestetilbud som gjør det mulig for en tjenesteyter å definere rammene for den elektroniske samhandlingen på en dynamisk måte; presentere hvilke medisinske tjenester som finnes, informere rekvirentene om hvilken medisinsk kontekst disse bør benyttes, koble til kliniske problemstillinger osv.

Videre beskrivelse av løsning og utstyr fremgår av SSA-L.

Databehandleravtalen skal sikre at personopplysninger, som definert i gjeldende personvernregelverk ikke brukes urettmessig og at konfidensialitet, integritet, tilgjengelighet og robusthet ivaretas. Avtalen skal videre sikre at partene ivaretar vern av den registrertes rettigheter i henhold til personvernregelverket.

Underleverandøren skal oppfylle de plikter som fremgår av denne Databehandleravtalen samt å følge de instrukser Databehandler gir på vegne av Dataansvarlig.

2. Bakgrunn og nærmere om partene

Dataansvarlig har inngått avtale med Databehandleren/Helse Vest IKT AS som innebærer at Databehandler/Helse Vest IKT AS kan inngå avtaler med underleverandører i forbindelse med utvikling og drift av IT som en tjeneste til Dataansvarlig.

Av denne avtalen fremkommer det at Dataansvarlig skal på forespørsel kunne be Databehandler om å få seg forelagt avtalen som inngås mellom Helse Vest IKT AS og underleverandøren.

Dataansvarlig: Virksomheter/helseforetak som har inngått databehandleravtale med Helse Vest IKT AS. (Hvilke Dataansvarlige som bruker løsningen som omtales av denne avtalen fremkommer av konfigurasjonsdatabasen/Systemlisten som vedlikeholdes av Databehandler).

Databehandler: Helse Vest IKT AS.

Annen databehandler (Heretter kalt Underleverandør): DIPS AS

Dersom Underleverandøren benytter andre underleverandører er dette omtalt i punkt 8 og Vedlegg 3.

3. Forholdet til andre avtaler

Denne avtalen supplerer andre avtaler som er inngått mellom Databehandler og underleverandør.

Når det gjelder informasjonssikkerhet og personvern ved databehandling av person- og helseopplysninger skal bestemmelsene i denne Databehandleravtalen ha forrang fremfor bestemmelser i andre avtaler, med mindre alternative bestemmelser gir et sterkere vern av opplysningene enn bestemmelsene her.

4. Beskrivelse av behandling av personopplysninger

Denne Databehandleravtalen kommer til anvendelse ved behandling av personopplysninger som Underleverandøren utfører i henhold til «Avtale om løpende tjenestekjøp over internett», avtalt mellom Underleverandøren og Databehandler, signert 06.05.2022 med påfølgende endringsbilag (heretter kalt SSA-L), og etter Databehandlers instrukser på vegne av Dataansvarlig.

Underleverandøren skal bare behandle personopplysninger i den grad det er nødvendig med henblikk på de oppgaver Underleverandøren er pålagt ved SSA-L.

Formålet med og varigheten av behandlingen er nærmere beskrevet i vedlegg 1. Videre beskrives selve behandlingen som utføres, hvilke helse- og personopplysninger som skal behandles, kategorier av de registrerte og behandlingens art i vedlegg 1. Eventuelt senere endringer skal fremgå av vedlegg 1.

5. Omfang for behandling av helse- og personopplysninger

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

Dataansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i helse- og personopplysningene som behandles hos Databehandleren og Underleverandør. Tilgangen og innsynet må imidlertid skje via Databehandleren.

6. Dataansvarliges plikter

Dataansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen, relevant helselovgivning og annen særlovgivning, samt denne avtalen.

7. Underleverandørens plikter

7.1. Generelt

Underleverandøren forplikter seg til å behandle helse- og personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Databehandlerens dokumenterte instruksjoner og andre gjeldende avtaler mellom partene, samt «Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten» "Normen". Underleverandør skal ikke ved forsettlig eller grov uaktsom handling eller unnlatelse, sette Dataansvarlig i en slik situasjon at Dataansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Underleverandør skal ikke:

a. behandle helse- og personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen med vedlegg;
b. behandle helse- og personopplysninger utover det som er nødvendig for at Underleverandøren til enhver tid kan oppfylle gjeldende avtaler omtalt i punkt 4;
c. utlevere, overlate eller overføre helse- og personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Databehandler;
d. samle inn fra eller overføre helse- og personopplysninger til en tredjepart;
e. behandle helse- og personopplysninger de får tilgang eller adgang til gjennom oppdraget fra Databehandler på annen måte enn hva som er angitt i denne Avtalen med vedlegg.
f. gjøre kjent personopplysninger for noen tredjepart hvis dette ikke er godkjent av Databehandler eller loven krever det. Hvis en offentlig myndighet eller tilsynsmyndighet krever tilgang til personopplysninger, skal Underleverandør varsle Databehandler før utleveringen med mindre dette er forbudt ved lov. Underleverandør krever at alt ens personell som er autorisert for å behandle Dataansvarliges personopplysninger, forplikter seg til konfidensialitet og ikke behandler Dataansvarliges

personopplysninger for noe annet formål, unntatt på instruksjon fra Databehandler eller gjeldende lov krever det.

Underleverandør forplikter seg, uten kompensasjon eller annet vederlag enn det Underleverandør har krav på etter SSA-L til å:

a. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Dataansvarlig;

b. gi Databehandler tilgang til og innsyn i helse- og personopplysninger som behandles hos Underleverandør;

c. føre og vedlikeholde en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;

d. treffe alle rimelige tiltak for å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;

e. følge etablerte rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer fra Databehandler;

f. påse at samtlige personer som av underleverandør gis tilgang til personopplysninger som behandles på vegne av Dataansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;

g. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Underleverandørs løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;

h. gi Databehandler nødvendig bistand slik at Databehandler og Dataansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;

i. samarbeide med og bistå Databehandler ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;

j. omgående underrette Databehandler dersom Underleverandør mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;

k. bistå Databehandler for å sikre Dataansvarliges overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

7.2 Tekniske, organisatoriske og sikkerhetsmessige tiltak

Underleverandøren 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.

Underleverandør forplikter seg, uten kompensasjon eller annet vederlag enn det Underleverandør har krav på etter SSA-L til å:

a. 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, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av helse- og personopplysninger som ikke er i overensstemmelse med denne Avtalen, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;

b. ha gode og hensiktsmessige internkontrollrutiner;

c. ha rutiner for autorisasjon og styring som sikrer at bare de av Underleverandørs medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring

av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre oppdraget;

d. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse. På forespørsel, skal Underleverandør gi Databehandler tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av helse- og personopplysninger;

e. 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 Underleverandør;

f. ved mistanke om eller konstatering av avvik, omgående varsle Databehandler. 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;

g. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;

h. omgående varsle Databehandler ved uautorisert utlevering av personopplysninger;

i. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Dataansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;

j. bistå Databehandler med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs.:
   - sikkerhet ved behandlingen;
   - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
   - underretning av den registrerte om brudd på personopplysningssikkerheten;

k. i forbindelse med sikkerhetsrevisjon som utføres av Databehandler eller en tredjepart utpekt av Databehandler, framlegge interne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;

l. varsle Databehandler om alle kjente forhold eller forhold som databehandler burde ha vært kjent med som medfører endring i risikobildet;

m. innhente godkjenning av Databehandler før gjennomføring av enhver endring av databehandlingen hos Underleverandør som har eller kan ha betydning for informasjonssikkerheten.

Nærmere krav til Underleverandørs informasjonssikkerhet er angitt i **Vedlegg 2** (hvis relevant).

Ved brudd på denne Avtalen eller på bestemmelsene i personopplysningslovgivningen, helselovgivningen eller annen relevant lovgivning kan Databehandler, på vegne av Dataansvarlig, kreve endringer i behandlingsmåten eller pålegge Underleverandør å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Underleverandør skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Databehandler, der Databehandler kan dele dette videre til aktuell Dataansvarlig.

8. Underleverandørens bruk av annen databehandler

Dersom Underleverandøren benytter annen databehandler eller andre som normalt ikke er ansatt hos Underleverandøren, må det inngås avtale med denne virksomheten (annen databehandler) hvor de pålegges tilsvarende plikter som gjør at Underleverandøren kan oppfylle sine forpliktelser i forhold til Databehandler.

Underleverandøren plikter å føre oversikt over sine underleverandører/andre databehandlere (se vedlegg 3) og skriftlig informere Databehandleren om eventuelle påtenkte endringer vedrørende supplering eller bytte av

underleverandør før endringen gjennomføres. Dette må varsles i god tid slik at Databehandleren gis mulighet til å motsette seg endringen. På tidspunktet for inngåelse av denne Databehandleravtalen har Databehandler godkjent at Underleverandøren benytter de underleverandører som fremkommer av vedlegg 3.

9. Overføring av personopplysninger til utlandet

Ingen helse- og personopplysninger som behandles under denne databehandleravtalen skal føres ut av EØS/EU, med mindre det er særskilt avtalt med de Databehandler. I tillegg skal helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b). Eventuelle unntak som innebærer overføring til utlandet skal godkjennes eksplisitt av Dataansvarlig før behandlingen starter.

Databehandler bekrefter at ingen av underleverandørene overfører helse- og personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer/databehandleringer som er angitt i Vedlegg 1 B for underleverandørene i Vedlegg 3. Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Dataansvarlig på forhånd. Ved overføring av helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Databehandler gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Dataansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Dataansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Dataansvarliges egen risikovurdering.

10. Taushetsplikt

Underleverandøren har taushetsplikt vedrørende dokumentasjon og personopplysninger som Underleverandøren får tilgang til under Databehandleravtalen. Underleverandøren skal påse at alt personell er kjent med og forpliktet av taushetsplikten under denne Databehandleravtalen.

Denne bestemmelsen gjelder også etter opphør av Databehandleravtalen.

11. Innsyn, verifikasjon og revisjon

Databehandler kan til enhver tid kreve innsyn i og verifikasjon av Underleverandørs behandling av personopplysninger tilhørende Dataansvarlig, herunder innsyn i og verifikasjon av dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Underleverandørs system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Underleverandør på vegne av Dataansvarlig, og øvrige innsynsrettigheter nedfelt i lov. Hvis Dataansvarlig ber Databehandler om innsyn skal Databehandler kunne gjøre generell informasjon fra revisjonen (Revisjonens mål, problemstillinger, omfang, revisjonskriterier og metoder) tilgjengelig for den Dataansvarlige og andre dataansvarlige som Databehandler har databehandleravtale med og som benytter samme tjeneste hos Underleverandør. Underleverandør skal på forhånd godkjenne hvilken informasjon som kan gjøres tilgjengelig for andre dataansvarlige, og nekting av samtykke skal bare kunne skje dersom det foreligger saklig grunn for dette.

Ved ønske om revisjon skal Databehandler gi Underleverandør varsel i rimelig tid og tidspunkt og plan for revisjon avtales.

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

Underleverandør skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Underleverandøren eller dennes underleverandører skal korrigeres uten kostnad for Databehandler/Dataansvarlig, Underleverandøren skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

12. Varighet og opphør

Denne Databehandleravtalen gjelder så lenge Underleverandøren behandler personopplysninger på vegne av Dataansvarlig. Denne avtalen skal signeres før underleverandør begynner å behandle personopplysninger.

Ved brudd på denne Databehandleravtalen eller gjeldende personvernregelverk, kan Databehandler kreve at Underleverandøren stanser videre behandling av personopplysninger med umiddelbar virkning.

Ved opphør av Databehandleravtalen plikter Underleverandøren (og dennes godkjente underleverandører, jf. punkt 8) å ugjenkallelig slette samtlige dokumenter og elektroniske data som Underleverandøren måtte ha i sin besittelse i egenskap av Underleverandør.

Underleverandøren har ingen rett til å beholde kopier av opplysninger i noe som helst format.

Underleverandøren må fremlegge skriftlig dokumentasjon på at sletting og/eller destruksjon har funnet sted i henhold til Databehandleravtalen innen rimelig tid etter opphør av denne, og må bekrefte at Underleverandøren ikke har beholdt noen kopi, utskrift eller annen gjengivelse av noen som helst del av materialet, uansett bruk av medium.

Underleverandøren plikter å sjekke og dokumentere at ovennevnte krav også er overholdt av eventuelle godkjente underleverandører.

13. Avtalebrudd(mislighold) og erstatning for økonomiske utlegg

Avtalebrudd foreligger dersom en part ikke oppfyller sine forpliktelser etter denne Databehandleravtalen, og dette ikke skyldes forhold som den andre parten har ansvaret eller risikoen for. Den som vil påberope seg avtalebrudd må meddele dette til den annen part med skriftlig begrunnelse, uten ugrunnet opphold etter at det aktuelle forholdet ble kjent.

Vesentlig mislighold av denne Databehandleravtalen skal ansees som vesentlig mislighold også av SSA-L, og Databehandler kan da etter å ha gitt Underdatabehandler skriftlig varsel og rimelig frist til å bringe forholdet i orden, heve SSA-L med øyeblikkelig virkning i den utstrekning også SSA-L heves.

Ved eventuelt krav fra Databehandler eller Dataansvarlig for dekning av erstatning som noen av disse må yte som følge av Underdatabehandler eller Underleverandør eller tap og utgifter for annet mislighold under Databehandleravtalen, skal kravet ansees som erstatning etter SSA-L og erstatningsbegrensningen i SSA-L kommer til anvendelse mellom partene.

14. Rettsvalg og verneting

Dette er nærmere regulert i SSA-L.

Riktig verneting er Bergen tingrett med mindre annet fremgår av Tjenesteavtalen mellom partene.

15. Undertegning

Denne avtalen undertegnes i to eksemplarer og partene beholder ett hver.

Oslo, 1/6-22	Oslo 1/6-22
Sted og dato	Sted og dato
Helse Vest IKT AS Ole Jørgen Kirkeluten	DIPS AS Kolbjørn Haarr

Administrerende direktør	Adm.dir.

VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER

Tabellene oppdateres fortløpende og dateres.

24.05.2021

A. Formålet med og varigheten av behandlingen

Formålet med og varigheten av behandling av helse- og personopplysninger er:

Underdatabehandler vil Behandle og ha tilgang til Personopplysninger i forbindelse med service, support, vedlikehold, oppgradering og bistand til databehandler på leveranse av sky-basert programvare, Interactor Sky, og moduler fra Underdatabehandler i henhold til SSA-L.

Behandlingen er ikke tidsbegrenset, og varer frem til opphør av SSA-L, men behandling av data om enkeltpasienter kan tidsbegrenses – bestemt av Dataansvarlig.

Dato (fra/til)	Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen
24.05.2022	Tjenester avtalt i SSA-L	Formålet med behandling av helse- og personopplysninger er å tilby, drifte, utføre support og vedlikehold på Interactor Sky.	I avtaleperioden
24.05.2022	Brukerstøtte	Ulike typer konsulenttjenester utført på forespørsel fra Dataansvarlig og/eller Databehandler.	I avtaleperioden

B. Behandling av helse- og personopplysninger

Det følger av personvernforordningen art 4 nr.2 at med «behandling» menes: «*enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring*»

Følgende behandlinger av personopplysninger omfattes av Avtalen:

Helse- og personopplysninger i Interactor Sky: Innsamling, registrering, lagring, tilpasning eller endring, organisering, tilgjengeliggjøring, bruk, gjenfinning, utlevering, både i form av utlevering til EPJ, men også i forbindelse med «overføring» knyttet til servicearbeid, feilsøk, sletting eller tilintetgjøring.

Databehandling	Nærmere beskrivelse av databehandlingsaktiviteter	Lokasjon av system og sted for databehandlingsaktivitet
Tilgang til lagrede personopplysninger for feilretting	Leverandøren har behov for tilgang til lagrede personopplysninger for feilsøking og feilretting	Lokasjon for lagring: Sopra Sterias datasenter i Oslo, Norge. Sted for databehandlingsaktivitet: Ansatte hos Underdatabehandler og dennes underleverandør i Norge. I noen tilfeller kan det bli aktuelt at Underdatabehandlers underleverandørs ansatte i Polen og Spania behandler data.
Tilgang til lagrede personopplysninger for support oppdatering	Leverandøren har behov for tilgang til lagrede personopplysninger for oppdatering	Som over
Tilgang til lagrede personopplysninger for konfigurasjon	Leverandøren har behov for tilgang til lagrede personopplysninger for konfigurasjon. Leverandøren kan utføre konfigurasjonsendringer på oppdrag fra databehandler eller dataansvarlig	Som over
Innsamling	Systemet inkluderer integrasjon med brukerens EPJ system. I denne integrasjonen samles opplysninger som pasientinformasjon og brukerinformasjon (se Kapittel C i dette vedlegget), nødvendig for at Interactor skal kunne gjøre sin jobb.	Som over
Registrering	Systemet inkluderer skjermbilder der brukeren registrerer nødvendige opplysninger om hvilke tjenester som skal bestilles og relevante kliniske opplysninger forbundet med disse (se Kapittel C i dette vedlegget).	Som over

Databehandling	Nærmere beskrivelse av databehandlingsaktiviteter	Lokasjon av system og sted for databehandlingsaktivitet
Organisering	Reigstrerte data organiseres etter spesifikasjon for rekvisisjonsmeldinger før disse returneres til brukerens EPJ system som ferdige rekvisisjonsmeldinger.	Som over
Lagring	Registrerte data lagres i systemets database. Lagringstid begrenses.	Som over
Tilpasning eller endring	Lagrede opplysninger kan endres eller kompletteres etter gitte regler i systemet. For eksempel ved etterrekvirering av enkelte tjenester.	Som over
Gjenfinning	Lagrede opplysninger kan gjenfinnes i forbindelse med historisk visning av tidligere rekvisisjoner for aktuell pasient. Disse kan også benyttes som utgangspunkt for nye bestillinger gjennom kopifunksjoner.	Som over
Sletting eller tilintetgjøring	Data slettes når avtalt og angitt lagringstid passeres, eller dersom dette instrueres fra den registrerte, Dataansvarlig eller Databehandler.	Som over
Utlevering/Overføring	Systemet leverer ut rekvisisjonsmeldinger basert på integrert informasjon fra brukerens EPJ og registrert informasjon fra brukeren. Utleveringen skjer til brukerens elektroniske pasientjournal, integrert med Interactor. Overføring kan i andre sammenhenger skje ved at servicepersonell ser data i forbindelse med feilsøk, feilretting eller brukerstøtte.	Som over

C. Typer av opplysninger

Følgende helse- og personopplysninger behandles:

Personopplysninger
Behandlingen omfatter følgende typer personopplysninger: Navn, fødselsdato, personnummer, adresse, e-post adresse, telefonnummer, organisasjonstilhørighet, offentlige identifikatorer som HPR nummer og adresseringsinformasjon som HER id med tilhørende informasjon fra adresseregisteret (NHN-AR).

Helseopplysninger (ikke uttømmende liste)
Behandlingen omfatter for kategorien registrerte *Pasienter* i tillegg helseopplysninger i form av bestilte/henviste medisinske tjenester og kliniske opplysninger oppgitt av rekvirent/henviser i den forbindelse

D. Kategorier av registrerte

Følgende kategorier av personer behandles det opplysninger om (registrerte):

Kategorier av registrerte		
Pasienter	Helsepersonell ved brukerstedene (brukere av systemet), som er involvert i eller aktuell for å utføre helsetjenester.	Ansatte hos leverandør som er drift- og servicepersonell for systemet. Ansatte hos leverandørs underleverandørsom er drift- og servicepersonell for systemet.

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET FOR DATABEHANDLER OG UNDERLEVERANDØRER (ANNEN DATABEHANDLER)

Krav til informasjonssikkerhet er lik for Databehandler og Underleverandør (annen Databehandler).

24.05.2021

Nr.	Tema	Krav
1.	Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren	Databehandler og Underleverandør skal følge relevante krav i Norm for informasjonssikkerhet og personvern, inkludert vedlegget «Oversikt over Normens krav».
2.	Sikring av data	Databehandler og Underleverandør skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet. Mekanismene spesifiseres i pt. 4, 5 og 6 under.
3.	Autentisering	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Databehandler og Underleverandør skal ha etablert passordpolicy.
4.	Logging og sporbarhet	Dersom løsning ligger hos Helse Vest IKT er kravet at all tilgang skal gå igjennom VPN (Bomgar-løsningen). All behandingsaktivitet blir logget og er sporbar. Dersom løsning ligger hos/overføres Underleverandør skal Underleverandør skal sikre at all tilgang til og forsøk på tilgang til data kan dokumenteres. Logger skal sikres mot endring, og skal kunne forevises på etterspørsel.
5.	Tilgjengelighet, redundans og skalering	Underleverandør skal sikre at tjenesten er tilgjengelig iht. krav i kontrakt/SLA, inkludert beskyttelse mot tjenestenektangrep, programvare-, nettverks- og maskinvarefeil, og andre hendelser som kan gi redusert tilgjengelighet.

6.	Testdata	All testing skal avtales med Helse Vest IKT. Ved bruk av personopplysninger ved test skal det alltid tas utgangspunkt i bl.a. det grunnleggende personvernprinsippet i personvernforordningen art 5 b) «dataminimering». Det skal kun brukes adekvate og relevante personopplysninger og det skal begrenset til det som er nødvendig for formålet for behandlingen/testen. Testdata i Interactor Sky akkumuleres over tid gjennom bruk av testlegekontor og testintegrasjoner hos Databehandler og Dataansvarlig. Det forutsettes at testdata ikke er reelle helse- og personopplysninger, men enten anonyme eller syntetiske data. Underdatabehandlers testsystem er beskyttet på samme nivå som produksjonssystem.
7.	Sletting og tilbakelevering	Underleverandør skal ha rutiner som skal kunne vises på forespørsel fra databehandler på vegne av Dataansvarlig.
8.	Lagringstid	Underleverandør skal sørge for at data slettes iht. avtalens krav om lagringstid, og at data er tilgjengelige inntil avtalt tidspunkt for sletting.
9.	Backup og restore	Helse Vest IKT Det gjøres nødvendige sikkerhetskopier av data i løsningen for å muliggjøre restore etter eventuelle alvorlige driftsforstyrrelser for å minimere datatap.
10.	Kryptering ved lagring	Lagrede data i systemets databaser er kryptert med TDE – Transparent data encryption.
11.	Kryptering i kommunikasjon	Underdatabehandler bruker standard krypteringsmekanismer (TLS 1.2/VPN).
12.	Prosess for håndtering av det eksterne trusselbildet	HelseCert er det nasjonale beskyttelsesprogrammet for helsesektoren i Norge. (Cert=Computer emergency response Team). De bidrar med kompetanse om trusler, kommer med varsler og verktøy for å håndtere trusler.

		Underdatabehandler er med i Norsk Helsenetts HelseCert-program, med skanning av alle våre eksponerte tjenester, ser etter sårbarheter og melder fra ved funn. Underdatabehandler har en rekke interne sikkerhetstiltak for testing, analysering og synliggjøring av skadelig kode (basert på IPS/IDS-teknologi). Systemlogger fra systemet eksporteres rutinemessig til og analyseres av Security Operation Centre (SOC) for raskest mulig oppdagelse av alvorlige trusler og hendelser.

VEDLEGG 3 – UNDERLEVERANDØRER

Tabellene oppdateres fortløpende.

Her listes opp hvilke underleverandører som benyttes av Databehandlers underleverandør – se eksempler nedenfor-fylles kun ut når underleverandøren benytter andre underleverandører.

24.05.2021

Navn på underleverandør	Leveranseområde	Stedlig plassering
Sopra Steria AS, Org.nr. 910 909 088, PB 1172 Sentrum, 0107 Oslo, Norge	Leverer teknisk infrastruktur og kjøremiljø (plattform), inkl. drift av dette, for Interactor Sky. Med i dette er support, feilsøk og feilretting tilknyttet infrastruktur og plattform.	Norge
Sopra Steria Polska Sp z o o, 140234577ss (REGON) 522184829 (DUNS), Uniwersytecka 13 40-007 Katowice, Poland	Mulig innsyn i data gjennom fjernaksess i feilsøk, feilretting og support.	Polen
Sopra Steria España S.A.U., s A-79329108 (N.I.F), Avenida de Manoteras, num. 48 Edificio B, 6a planta 28050 MADRID, SPAIN	Mulig innsyn i data gjennom fjernaksess i feilsøk, feilretting og support.	Spania