Databehandleravtale

I henhold til ny personvernlov, jf. personvernforordningen art. 28 nr. 3,

inngås databehandleravtale

mellom

_____ (Kunde),

Organisasjonsnummer:_____ (Orgnr)
Behandlingsansvarlig

Og

CompuGroup Medical Norway AS (CGM)
Databehandler

_____	_____
Sted og dato	Sted og dato
_____	_____
Signatur Kunden	Signatur CompuGroup Medical Norway AS
_____	_____
Blokkbokstaver	Blokkbokstaver

Databehandleravtale

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter lov av 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven), forskrift av 15. juni 2018 nr. 876(personopplysningsforskriften), lov av 20.juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger (helseregisterloven), lov av 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) og EUs personvernforordning (forordning 2016/679), samlet benevnt «Regelverket». 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 og art

Formålet med behandlingen, varigheten av behandlingen, behandlingens art, de typer personopplysninger som skal behandles og kategorier av registrerte følger av vedlegg til denne avtalen.

Databehandler leverer et elektronisk journalsystem til behandlingsansvarlig i henhold til leveranseavtalen (Hovedavtalen) mellom partene.

3. Behandlingsansvarliges rettigheter og plikter

Behandlingsansvarlig skal etterleve de forpliktelser som følger av Regelverket og denne avtalen. Herunder at de aktuelle personopplysningene kan behandles, sørge for at det foreligger et tilstrekkelig hjemmelsgrunnlag, ha ansvaret for at overføringer av personopplysninger til Databehandler lovlig kan skje og gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med punkt 3.

Behandlingsansvarlige har en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen.

4. Databehandlers plikter

Databehandler forplikter seg til å behandle helse- og personopplysninger i samsvar med Regelverket, denne Avtalen samt "Norm for informasjonssikkerhet i helse- og omsorgstjenesten". Databehandler skal kun behandle personopplysningene etter instruks fra Behandlingsansvarlig, herunder ikke overføre personopplysninger til land utenfor EU/EØS (tredjeland), uten etter skriftlig og dokumenterbar instruks fra Behandlingsansvarlig, jf. forordningen art. 28 (3) bokstav a. Videre skal Databehandler omgående underrette Behandlingsansvarlig om en instruks er i strid med Regelverket, jf. forordningen art. 28 andre avsnitt.

Databehandleren skal sikre at kun autoriserte personer har tilgang til opplysningene og at databehandleren fratar tilgangen dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder for den personen.

Databehandler skal sikre at personer som er autorisert til å behandle personopplysninger, har forpliktet seg til å behandle opplysningene fortrolig, eller er underlagt en egnet lovfestet taushetserklæring, jf. forordningen art. 28 (3) bokstav b. Plikten til konfidensialitet gjelder også etter at databehandleroppdraget er fullført.

Databehandler skal treffe tiltak som er nødvendige for å oppnå et sikkerhetsnivå som står i forhold til den relevante risiko ved behandlingen, jf. forordningen art. 32.

Databehandler skal etterkomme pålegg fra den Behandlingsansvarlige om å slette eller tilbakelevere personopplysninger etter at tjenestene knyttet til behandlingen er avsluttet, med mindre det foreligger lovkrav om at opplysningen fortsatt skal lagres, jf. forordningen art. 28 (3) bokstav g.

Databehandler skal gjøre tilgjengelig informasjon som er nødvendig for å påvise at forpliktelsene ovenfor er oppfylt for den Behandlingsansvarlige, samt muliggjøre og bidra til revisjoner og inspeksjoner som gjennomføres av den Behandlingsansvarlige eller annen på dennes vegne, jf. forordningen art. 28 (3) bokstav h.

Databehandler skal bistå den Behandlingsansvarlige med å svare på anmodninger som de registrerte inngir i samsvar med forordringens kapittel III.

Databehandler skal sikre at all behandling av personopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabelt risikonivå og i samsvar med risikovurdering utført av Databehandler.

Databehandleren definerer sikkerhetsmål, -strategi, -organisering og ansvar i samsvar med Regelverket og følger opp dette ved bruk av et internkontrollsystem.

Databehandler plikter å gi Behandlingsansvarlig tilgang til sin relevante sikkerhetsdokumentasjon og bistå slik at Behandlingsansvarlig kan ivareta sitt eget ansvar etter Regelverket.

Databehandler plikter å sørge for at samtlige personer hos seg som gis tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig er kjent med denne avtalen og er underlagt avtalens bestemmelser.

5. Bruk av underleverandør

Behandlingsansvarlig tillater at Databehandler benytter seg av underleverandører for oppfyllelse av forpliktelsene under denne avtalen. Behandlingsansvarlig har samtykket til bruk av de underleverandører som er angitt i vedlegg 1.

Databehandler skal sikre at underleverandører er undergitt tilsvarende forpliktelser som Databehandleren under denne avtalen.

Databehandler skal varsle Behandlingsansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Dersom Behandlingsansvarlig ikke har noen innvendinger mot dette innen [ti (10)] dager fra mottak av varslet, antas Behandlingsansvarlig for å ha godtatt endringene av underleverandører.

Tilgang til personopplysninger for andre eksterne tredjeparter enn Databehandlers underleverandører, krever konkret avtale mellom partene utover denne avtalen.

6. Overføring til tredjeland

Databehandleren skal ikke overføre Personopplysninger til et land utenfor EØS-området, som ikke er ansett for å gi tilstrekkelig beskyttelse i henhold til Gjeldende Personvernlovgivning ("Tredjeland"), uten skriftlig forhåndssamtykke fra Behandlingsansvarlig. Behandlingsansvarlig har samtykket til overføring til land hvor underleverandørene som er angitt i Vedlegg 1 er lokalisert.

Dersom Behandlingsansvarlig har gitt skriftlig samtykke til overføring av Personopplysninger til et Tredjeland, plikter Databehandleren på forespørsel fra Behandlingsansvarlig å inngå EUs standardkontrakt for overføring av

Personopplysninger til tredjeland (2010/87/EU) eller andre bestemmelser som erstatter 2010/87/EU-bestemmelsene.

Databehandleren kan også benytte EU-US Privacy Shield eller andre instrumenter som utgjør et rettslig grunnlag for overføringen i henhold til Gjeldende Personvernlovgivning. For å unngå tvil, understrekes det at overføring på grunnlag av EU-US Privacy Shield og andre instrumenter forutsetter skriftlig forhåndsgodkjennelse fra Behandlingsansvarlig.

Hvis Databehandler ønsker å overføre Personopplysninger til et Tredjeland som ikke er angitt i Vedlegg 1 skal Databehandler skriftlig varsle Behandlingsansvarlig om dette senest 3 måneder før overføringen finner sted. Behandlingsansvarlig skal svare på henvendelsen fra Databehandler senest innen 1 måned. Hvis Behandlingsansvarlig ikke samtykker til overføringen, og Databehandleren ikke med rimelighet kan tilby et annet alternativ, har Behandlingsansvarlig rett til å si opp Avtalen.

7. Sikkerhet

Databehandler skal ha en tilfredsstillende teknisk og fysisk sikring på den løsningen som benyttes.

Databehandler skal ha klare rutiner for logging av feil og avvik som er av betydning og som er omfattet av denne avtalen. Dersom det avdekkes slike feil eller avvik, skal Databehandler så snart som mulig varsle Behandlingsansvarlig om dette.

Behandlingsansvarlig kan revidere Databehandlers personopplysningssikkerhet ved bruk av en tredjepart godkjent av Databehandler. Revisjonen kan omfatte gjennomgang av rutiner, stikkprøver, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Slike revisjoner kan kun gjøres etter skriftlig forhåndsvarsel fra Behandlingsansvarlig. De som utfører revisjon må forholde seg til Databehandlers rimelige instrukser ved adgang til Databehandlers lokaler, og for øvrig akseptere Databehandlers saklige behov for konfidensialitet. Revisjoner skal skje på en effektiv måte og skal i minst mulig utstrekning forstyrre Databehandlers arbeid.

Databehandler skal etablere tiltak og rutiner for å avdekke avvik fra personvernsikkerhet og andre sikkerhetsbrudd, samt ha rutiner og iverksette tiltak for å følge opp og rette avvik. Databehandler plikter å bistå Behandlingsansvarlig med oppfølgingen av avvik, samt fremskaffe den nødvendige informasjon om avviket som følger av Regelverket.

Eventuelle avvik skal skriftlig meldes til Behandlingsansvarlig uten ugrunnet opphold og senest innen 48 timer etter at Databehandler fikk mistanke om avviket, selv om Databehandler ikke har all påkrevet informasjon tilgjengelig. Melding til Behandlingsansvarlig om eventuelle avvik skal ikke utsettes i påvente av undersøkelser rundt årsak, omfang og konsekvens. Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til avviket.

8. Type personopplysninger

De registrerte er hovedsakelig pasienter, kunder og ansatte hos den behandlingsansvarlige.

Mer informasjon i vedlegg til denne avtalen.

9. Avtalens varighet

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

Ved brudd på denne avtale eller personopplysningsloven kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

10. Avslutning av databehandleravtale

Ved opphør av denne avtalen plikter Databehandler å slette eller destruere alle dokumenter og data, som inneholder opplysninger som omfattes av avtalen. Denne slettingen/destrueringen skal utføres etter gjeldende lovbestemmelser. Dette gjelder også for eventuelle sikkerhetskopier.

Databehandler skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør. Behandlingsansvarlig skal motta en skriftlig bekreftelse på dette.

Vedlegg 1: Oversikt over Databehandlers underleverandører

Selskap	Rolle	Org. nr.	Leveranseområde	Adresse
DIPS ASA	Leverandør av Journal Pluss (Dips Communicator)	979 543 883	Software support og service	Jernbaneveien 85 8006 Bodø, Norge
CompuGroup Medical SE	Drift og infrastruktur CGM nettverk og CGM hosting		Driftstjenester	Maria Trost 21 56070 Koblenz, Tyskland
Link Mobility	Leverandør av SMS tjenester via produktet «ePortal»	992 434 643	SMS leveranse	Langkaia 1 0150 Oslo, Norge
Puzzel	SMS varsling for bestemte kundegrupper	916 938 705	SMS varsling	Fredrik Selmers vei 3 0663 Oslo, Norge
CompuGroup Medical Denmark AS	Drift og infrastruktur, CGM Medical Cloud		Driftstjenester	Olof Palmes Allé 8200 Aarhus N, Danmark
MedRave*	Leverer medisinsk utsyr, produkter med integrasjon til EPJ	914 183 162	Software support og service	Rådhusgata 30B 0151 Oslo, Norge
Unisoft*	Leverer produkter med integrasjon til EPJ, som for eksempel Triage og Lims-in-a-box	830 517 502	Software support og service	Hedrumsveien 1674 3282 Kvelde, Norge
Imatis DNV*	Leverer produkter med integrasjon til EPJ, som for eksempel Imatis Visit og Imatis Flow	963 310 439	Software support og service	Storgata 159, 3915 Porsgrunn, Norge

***Gjelder kunder som har produkter fra underleverandøren.**

Vedlegg 2: CGMs behandling av personopplysninger

Dette vedlegget gir en oversikt over personopplysningene som databehandleren kan behandle innenfor rammen av hovedavtalen, og som kan tilordnes behandlingsansvarlig.

Vedlegget inneholder også informasjon om for eksempel formål, behandlingsaktiviteter, steder for behandling og datasikkerhet knyttet til databehandlers behandling av personlig informasjon.

Formål

Oppfylle databehandlers forpliktelser i henhold til hovedavtalen.

Som en del av Hovedavtalen vil Databehandler kunne behandle Behandlingsansvarliges databaser, legge inn nye versjoner og rettelser av systemet, foreta uttrekk av data, feilsøking og feilretting, samt andre typer tilhørende supportaktiviteter og endringer som er ønsket fra Behandlingsansvarliges side. Databehandler vil i denne forbindelse kunne behandle personopplysninger.

Generelle bemerkninger om personlige data i databehandlers system

Databehandler har de generelle rettighetene til systemene databehandler gir til behandlingsansvarlig, med eventuelle avvik som oppstår i hovedavtalen.

Databehandlers utgangspunkt er at alle data som registreres i systemet av behandlingsansvarlig, eller av noen som opptrer på vegne av behandlingsanvarlig, for eksempel data om ansatte eller pasienter, tilhører behandlingsansvarlig og faller under behandlingsansvarliges ansvar.

At den behandlingsansvarlige registrerer data i et eller flere av databehandlers systemer vil ikke automatisk bety at databehandler faktisk behandler data, noe databehandler kun vil være i de tilfeller hvor databehandler faktisk behandler personopplysningene det gjelder.

Databehandler utfører behandling av data på vegne av kunder i henhold til hovedavtalen hovedsakelig der hvor databehandler utfører driftstekniske oppgaver, kommuniserer personlige data til og fra andre systemer, samt i de tilfeller hvor personopplysninger forekommer i forbindelse med support eller konsulentoppdrag (for eksempel migrering, registrering av data på vegne av behandlingsansvarlig, endring av data på vegne av behandlingsansvarlig).

Behandlingsansvarlig er alltid ansvarlig for å sikre at innhenting og registrering av data, informasjon til den registrerte, sletterutiner og andre lovmessige forpliktelser vedrørende innhenting og behandling av personlige data er innført i henhold til relevante lover og regler.

Databehandler er alene ansvarlig for å sikre at databehandlingen utført av databehandler under vilkårene beskrevet i hovedavtalen utføres i henhold til denne avtalen.

Databehandleravtale

Kategorier av registrerte

Alle kategorier av registrerte som behandlingsansvarlig kan komme til å registrere, består primært av:

Pasienter/studenter/ansatte/brukere eller andre som bruker eller har rettigheter til å bruke kundens tjenester, mottagere av helsetjenester, slektninger eller andre kontakter, ansatte (brukere) av kunden, konsulenter/ansatte fra underleverandører, helsepersonell eller andre som ikke er ansatt av kunden, men har annen tilknytning til pasienter (sendere/mottagere av pasientkommunikasjon fra andre leverandører av helsetjenester, alle ansatte i undervisningsinstitusjoner, ansatte i offentlig forvaltning/adminstrasjon eller tilsvarende).

Datakategorier

For ansatte/konsulenter hos behandlingsansvarlig (vær oppmerksom på at ikke alle data gjelder for alle ansatte/konsulenter)

Navn og kontaktinformasjon, personnummer eller tilsvarende, stilling, tittel, spesialitet, identifikasjonsnumre (for eksempel HER-id, HPR-nummer, RSH, rekvirentkoder), log-in informasjon og lignende informasjon.

For pasienter/mottagere av helsebehandling (vær oppmerksom på at ikke alle data gjelder for alle pasienter/mottagere av helsebehandling)

Navn og kontaktinformasjon, personnummer eller tilsvarende, kjønn, medisinsk og helseinformasjon, betaling og forsikringsinformasjon, avtaler, opprinnelsesland, morsmål, familiesituasjon/status, familierelasjoner, samtykkedata, informasjon om skole/klasse og arbeidssituasjon. Vær oppmerksom på at dataene også kan inkludere notater i fritekst i journalen og andre deler av systemet (alle typer personlig informasjon kan være inkludert i disse tekstfeltene og det er ikke uvanlig å finne andre typer sensitive personlige data som ikke er medisinsk eller helsedata).

Andre registrerte personer (se under avsnittet «Kategorier av registrerte» ovenfor for typene personer dette kan gjelde for, vær oppmerksom på at ikke alle data gjelder for alle pasienter/mottagere av helsebehandling)

Navn og kontaktinformasjon, personnummer eller tilsvarende, yrke, stilling, arbeidssted, identifikasjonsnumre (for eksempel HER-id, HPR-nummer, RSH, rekvirentkoder), relasjon til/hendelse relatert til/kontakter/diskusjoner/notater/memoer inkludert/vedrørende pasient/mottager av helsebehandling og lignende data. Vær oppmerksom på at dataene også kan inkludere notater i fritekst i journalen og andre deler av systemet (alle typer personlig informasjon kan være inkludert i disse tekstfeltene og det er ikke uvanlig å finne andre typer sensitive personlige data som ikke er medisinsk eller helsedata).

Databehandleravtale

Behandlingsaktiviteter

Nedenfor er en liste over aktivitetene som kan utføres av databehandleren innenfor rammen av databehandling i henhold til hovedavtalen.

Lagring, behandling eller endring, innsamling, registrering, strukturering, produksjon, lesing, bruk, tilpassing eller aggregering, overføring, begrensning, sletting eller destruering, korreksjon eller feilsøking på vegne av behandlingsansvarlig basert på hva som er avtalt mellom databehandler og behandlingsansvarlig i hovedavtalen, samt er i samsvar med instruksjoner utstedt i spesielle tilfeller for databehandlers support, konsultasjon, utvikling eller driftsavdelinger eller ansatte tilhørende databehandler.

Plassering hvor personopplysninger skal behandles

For alle kunder;

Databehandling kan utføres av ansatte av databehandler ved firmaets norske kontorer, hos den behandlingsansvarlige dersom databehandlers ansatte utfører support eller konsulentarbeid på stedet, eller på stedet eller i lokaler tilhørende underleverandører.

Fysisk lagring for kunder som benytter CGM Hosting;

CGM Datasenter i Frankfurt, Tyskland.

Datasikkerhet

Beskyttelse av kundenes personopplysninger er en prioritet for databehandler. De grunnleggende prinsippene som ligger til grunn for databehandlers datasikkerhet er; tilgjengelighet, nøyaktighet, konfidensialitet og sporbarhet.

Mangler i datasikkerhet kan føre til forstyrrelse av viktige offentlige tjenester som tilbys av kundene og medføre en risiko for de registrertes rettigheter og friheter. Databehandler skal derfor følge disse retningslinjene for å sikre at de ovennevnte prinsippene er overholdt med hensyn til all personlig databehandling:

- Identifiser, risikostyr og tildel ansvar for persondatatilgang og ha relevante og balanserte sikkerhetstiltak for å beskytte slik data.
- Behandle datatilgjengelighet i samsvar med gjeldende lovgivning, policyer og retningslinjer og kundens instruksjoner.
- Utdanne og informere ansatte om datasikkerhet for å oppnå og opprettholde et godt treningsnivå og sørge for at passende datasikkerhetsforanstaltninger brukes.
- Designe, implementere og vedlikeholde prosedyrer og verktøy for overvåkning som sørger for datasikkerhet.
- Designe, implementere og vedlikeholde rutiner og verktøy for styring av brudd på personvernet.
- Kontrollere medarbeideres tilgang til data; det vil si at den rette informasjonen er tilgjengelig på rett sted og tidspunkt til en autorisert bruker.