Instruksjoner for databehandling

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 behandlingsanvarlig, 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.

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 undervisininginstitusjoner, ansatte i offentlig forvaltning/adminstrasjon eller tilsvarende).

Data kategorier

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).

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 på Lysaker, 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 tjenster 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 vedlikeholder 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.