DATABEHANDLERAVTALE

mellom

[Kunde]
(heretter kalt **"Behandlingsansvarlig"**)

og

PayEx Norge AS, org nr
(heretter kalt **"Databehandler"**)

Vedrørende Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig

1 Bakgrunn

Partene har inngått avtale om PayEx MediPay i henhold med Rammeavtalen ("**Avtalen**"). Avtalen vil kunne omfatte behandling av Personopplysninger i henhold til EU Direktiv 95/46/EF av 24. oktober 1995, som er implementert i norsk lovgivning ved personopplysningsloven (lov 14. april 2000 nr. 31) og personopplysningsforskriften (forskrift 15. desember 2000 nr. 1265) og den nye norske personopplysningsloven som implementerer EU-forordning 2016/679 fra tidspunktet denne trer i kraft ("**Gjeldende Personvernlovgivning**").

Denne avtalen ("**Databehandleravtalen**") regulerer **Databehandlers** behandling av Personopplysninger på vegne av **Behandlingsansvarlig** og Databehandlers ansvar for informasjonssikkerhet etter Gjeldende Personvernlovgivning.

Begreper som er skrevet med stor forbokstav skal ha samme betydning som fastsatt i Gjeldende Personvernlovgivning med mindre annet er eksplisitt uttalt.

2 Beskrivelse av behandlingen

Denne Databehandleravtalen gjelder all behandling av Personopplysninger som Databehandler utfører på vegne av den Behandlingsansvarlige på grunnlag av Avtalen. Databehandleren kan bare behandle de kategorier av Personopplysninger som er forutsatt i Avtalen og i den grad det er nødvendig for å oppfylle Avtalen.

Formålene med Behandlingen, kategorier av Personopplysninger og berørte Registrerte er angitt i vedlegg D1 til denne Databehandleravtalen.

3 Behandlingsansvarliges plikter

Behandlingsansvarlig er ansvarlig for at det foreligger et rettslig grunnlag for Behandling av Personopplysninger i tilknytning til Avtalen og i henhold til denne Databehandleravtalen.

4 Databehandlers plikter

4.1 Etterlevelse av krav i lov og forskrift

I avtaleperioden for Databehandleravtalen skal Databehandler overholde Gjeldende Personvernlovgivning.

Databehandler skal ikke ved uaktsom eller forsettlig handling eller unnlatelse sette den Behandlingsansvarlige i en situasjon der Behandlingsansvarlig misligholder Gjeldende Personvernlovgivning.

Databehandler skal samarbeide med og yte bistand til den Behandlingsansvarlige for å sikre at Behandlingsansvarlig overholder sine forpliktelser i henhold til Gjeldende Personvernlovgivning.

Databehandler skal overholde de til enhver tid gjeldende instrukser og rutiner for behandling av Personopplysninger som Behandlingsansvarlig har vedtatt.

4.2 Begrensninger vedrørende bruk

Databehandler skal ikke behandle Personopplysninger utover det som kreves for oppfyllelse av sine forpliktelser overfor Behandlingsansvarlig i henhold til Avtalen.

Databehandler skal påse at Personopplysninger ikke gis til utenforstående med mindre Behandlingsansvarlig har pålagt slik utlevering eller Databehandler er forpliktet til dette i medhold av lov.

Databehandler skal ikke ha rettigheter til eller eierskap over Personopplysninger som Databehandler får tilgang til som ledd i oppfyllelse av Avtalen.

Databehandler skal påse at Personopplysninger som behandles på vegne av Behandlingsansvarlig holdes fysisk eller logisk atskilt fra andre data som Databehandler behandler.

4.3 Informasjonssikkerhet

Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen, jf. Gjeldende Personvernlovgivning.

En liste over minimumskrav til sikkerhet som får anvendelse for Databehandler, samt forpliktelser knyttet til dokumentasjon av tiltakene, er angitt i Vedlegg D1.

4.4 Avvik

Enhver Behandling av Personopplysninger som er i strid med sikkerhetskrav eller andre krav fastsatt i denne Databehandleravtalen, Behandlingsansvarliges instrukser eller Gjeldende Personvernlovgivning, inkludert Brudd på Personopplysningssikkerheten og ethvert annet sikkerhetsbrudd, skal behandles som et avvik.

Databehandler skal 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.

Databehandler skal umiddelbart eller så snart som mulig etter å ha blitt oppmerksom på det, rapportere avvik til den Behandlingsansvarlige. Rapporten skal omfatte den informasjonen som er påkrevet i henhold til Gjeldende Personvernlovgivning. Databehandler skal også gi Behandlingsansvarlig den bistand som er nødvendig for at Behandlingsansvarlig kan oppfylle kravene til å rapportere Brudd på Personopplysningssikkerheten til Datatilsynet og Registrerte, og for å kunne besvare spørsmål fra datatilsynsmyndigheter og berørte Registrerte.

4.5 Varslingsforpliktelser

Databehandler skal uten unødig opphold etter å ha blitt oppmerksom på det aktuelle forholdet, skriftlig varsle Behandlingsansvarlig i et tilfelle hvor:

i. Databehandleren er av den oppfatning at Behandlingsansvarliges instrukser til Databehandler er i strid med Gjeldende Personvernlovgivning;
ii. Det har oppstått en situasjon som vesentlig hindrer Databehandlerens nåtidige eller fremtidige evne til å behandle personopplysninger i tråd med denne Databehandleravtalen;
iii. Databehandler har mottatt krav om utlevering av Personopplysninger som behandles under denne Databehandleravtalen fra myndigheter. Databehandler er ikke forpliktet til å varsle dersom det i henhold til preseptorisk lovgivning er forbudt å varsle.

iv. Databehandler mottar en henvendelse fra en registrert som ønsker å utøve sine rettigheter i medhold av Gjeldende Personvernlovgivning;
v. Databehandler planlegger å gjøre endringer i de tjenestene som leveres som får følger for måten Personopplysninger behandles på, for eksempel ny og endret funksjonalitet;
vi. Det har oppstått et avvik, som foreskrevet i pkt. 4.4.

Databehandler skal i alle tilfeller uten unødig opphold skriftlig varsle Behandlingsansvarlig dersom Databehandleren ikke etterlever sine forpliktelser etter Gjeldende Personvernlovgivning og/eller denne Databehandleravtalen. Behandlingsansvarlig kan etter å ha mottatt slikt varsel, enten suspendere Databehandlers rett til å behandle Personopplysninger under Avtalen til Databehandleren igjen kan demonstrere etterlevelse, eller si opp Avtalen med 10 dagers skriftlig varsel.

4.6 Sikkerhetsrevisjon

Databehandleren skal hvert år, for egen kostnad, innhente en revisjonsrapport fra autorisert tredjepart som gjennomgår Databehandlerens etterlevelse av informasjonssikkerhetskrav under denne Databehandleravtalen og Avtalen. Rapporten skal omfatte, men ikke være begrenset til, en vurdering av Databehandlers oppfyllelse av sikkerhetsrelaterte plikter som er fastsatt i denne Databehandleravtalen (jf. pkt. 4.3 og Vedlegg D1) og Databehandlers bruk av underleverandører (jf. pkt. 4.8). Rapporten skal være basert på anerkjente bransjestandarder for slike rapporter. Rapporten skal videresendes til Behandlingsansvarlig senest 1 måned etter at den er foreligger.

Hvis revisjonen avdekker brudd på Databehandlers forpliktelser i henhold til Databehandleravtalen, skal dette bli håndtert som et avvik, jf. pkt. 4.4.

Denne bestemmelsen er ikke til hinder for at Behandlingsansvarlig kan utøve sine revisjonsrettigheter under Avtalen (dersom Avtalen inneholder en slik rett).

4.7 Overføring til utlandet

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 D1 pkt. e) 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 D1 pkt. e), 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.

4.8 Bruk av underleverandører

Behandlingsansvarlig har samtykket til bruk av de underleverandører som er angitt i vedlegg D1 pkt. e). Hvis Databehandler ønsker å engasjere en ny underleverandør eller gjøre andre endringer i listen over underleverandører som skal Behandle Personopplysninger under Avtalen, skal Databehandler skriftlig varsle Behandlingsansvarlig om endringen minimum 3 måneder før den iverksettes. Behandlingsansvarlig skal svare på henvendelsen fra Databehandler senest 1 måned etter at skriftlig varsel er mottatt om endringen aksepteres eller ikke. Hvis Behandlingsansvarlig ikke aksepterer endringen, og Databehandler ikke med rimelighet kan tilby et annet alternativ, kan Behandlingsansvarlig si opp Avtalen med umiddelbar virkning.

Dersom Behandlingsansvarlig har samtykket til at Databehandleren kan benytte underleverandører for å Behandle Personopplysninger under Avtalen, skal Databehandleren inngå avtale med den aktuelle underleverandøren hvor underleverandøren pålegges de samme plikter som Databehandleren er pålagt i denne Databehandleravtalen. Databehandleren er fullt ut ansvarlig overfor Behandlingsansvarlig for handlinger eller unnlatelser begått av en underleverandør.

4.9 Konfidensialitet

Databehandleren, inkludert dennes underleverandører, påtar seg å ivareta taushet om Personopplysninger som behandles på vegne den Behandlingsansvarlige i henhold til Avtalen og denne Databehandleravtalen. Taushetsplikten omfatter også annen informasjon av betydning for informasjonssikkerheten.

Databehandler skal påse at alle personer som på en eller annen måte er involvert ved Behandlingen av Personopplysninger, inkludert godkjente underleverandører, er klar over og forpliktet til å overholde taushetsplikten.

Taushetsplikten skal også gjelde etter utløpet av denne Databehandleravtalen.

5 Skadesløsholdelse

Hvis Behandlingsansvarlig blir holdt ansvarlig for et brudd på Gjeldende Personvernlovgivning og/eller denne Databehandleravtalen som er forårsaket av Databehandler og/eller dennes underleverandører, skal Databehandler holde Behandlingsansvarlig skadesløs for enhver kostnad, avgift, administrativ bot, skade, utgift og/eller direkte tap som har oppstått, forutsatt at:

a) Behandlingsansvarlig varsler Databehandler om kravet innen rimelig tid,
b) Databehandleren gis kontroll over den rettslige prosessen og forhandlinger knyttet til en potensiell avgjørelse av kravet; og
c) Behandlingsansvarlig samarbeider med Databehandler i prosessen som knytter seg til forsvaret og avgjørelsen av kravet på Databehandlerens kostnad.

Databehandler skal ha bevisbyrden med hensyn til å godtgjøre at Databehandler på ingen måte er ansvarlig for bruddet på Gjeldende Personvernlovgivning og/eller denne Databehandleravtalen.

6 Varighet og opphør av Databehandleravtalen

Denne Databehandleravtalen gjelder fra den dato begge parter har signert Databehandleravtalen og frem til opphør av Avtalen, bortsett fra eventuelle vilkår som i henhold til denne Databehandleravtalen eller Avtalen skal fortsette å ha virkning etter opphør.

Ved opphør av Databehandleravtalen skal Databehandler, inkludert eventuelle underleverandører, tilbakelevere alle Personopplysninger og andre opplysninger som Databehandleren eller dennes godkjente underleverandører i henhold til pkt. 4.8 har fått tilgang til i henhold til Avtalen. Opplysningene skal bli tilbakelevert i et standardisert format og medium sammen med nødvendige instruksjoner for å fasilitere den Behandlingsansvarliges videre bruk av opplysningene.

Såfremt det er gjennomførbart, kan Behandlingsansvarlig kreve at Personopplysninger og andre opplysninger i stedet overføres til en ny databehandler. Dersom dette innebærer en større kostnad for Databehandler enn å overføre til Behandlingsansvarlig, skal Behandlingsansvarlig betale merkostnadene. Databehandler skal på forespørsel fra Behandlingsansvarlig dokumentere kostnadene.

Som et alternativ til tilbakelevering eller overføring, kan Behandlingsansvarlig bestemme at alle eller deler av opplysningene skal ugjenkallelig slettes av Databehandleren og eventuelle underleverandører etter mottak av skriftlig instruks fra den Behandlingsansvarlige. Databehandleren og eventuelle underleverandører har ingen rett til å beholde kopier av opplysninger i noe som helst format.

Den Behandlingsansvarlige skal motta en skriftlig erklæring fra Databehandleren om at samtlige opplysninger enten er tilbakelevert eller slettet i samsvar med eventuell instruks fra den Behandlingsansvarlige, og at Databehandleren og eventuelle underleverandører ikke har beholdt noen kopi, utskrift eller annen fremstilling av opplysninger på noe som helst medium.

7 Lovvalg og tvisteløsning

Partenes rettigheter og plikter etter denne Databehandleravtalen bestemmes i sin helhet etter norsk rett.

Oslo tingrett vedtas som eksklusivt verneting.

Partene kan som alternativ til domstolsbehandling avtale at tvisten avgjøres med endelig virkning ved voldgift.

VEDLEGG D1
Dette vedlegget representerer Behandlingsansvarliges ytterligere instruksjoner til Databehandler i tilknytning til Databehandlers Behandling av Personopplysninger for Behandlingsansvarlig, og er en integrert del av Databehandleravtalen.

a) Behandlingens formål og karakter

Databehandler skal levere (i) PayEx Checkout med betalingsmåten Kortbetalinger (ii) PosPay Betalingssystem, (iii) Rapporteringsservice, og (iii) Vipps, samt (iv) betalingsmåten PayEx Faktura til Behandlingsansvarlig som angitt i Rammeavtalen. Databehandleren vil behandle Personopplysninger for følgende formål:

- Opplysninger brukes av Databehandler for forenkling av betalingsprosessen, ved at kundeopplysninger overføres til PayEx Checkout
- Opplysninger brukes av Databehandler for å oppfylle lovmessige og forretningsmessige krav til identifisering i forbindelse med kredittsjekk, scoring, betaling, fakturering, purring og inkasso.

b) Kategorier av registrerte

- Kunder av Behandlingsansvarlig (pasienter)

c) Kategorier av Personopplysninger

- Kunder av Behandlingsansvarlig: personnummer, navn, adresse, epost, mobilnummer, transaksjonsbeløp, fakturagebyr

d) Spesielle opplysningskategorier

- Helseopplysninger om ansatte: Nei.

e) Underleverandører, inkludert geografisk plassering av Behandlingen

- EDI Solutions AB, Box 9169, 400 94 Göteborg, 556569-5789, Gøteborg, Sverige
- Basefarm AS, Nydalen Allé 37a, 0403 Oslo, Norge

f) Særlige sikkerhetstiltak som får anvendelse for Databehandler

Databehandler skal ha på plass sikkerhetstiltak som er adekvate sett i forhold til den risikoen Behandlingen av Personopplysninger på vegne av Behandlingsansvarlig representerer. Dette inkluderer, blant annet, følgende tiltak og rutiner:

- Etablere en sikkerhetsorganisasjon med klare ansvarsområder
- Kunne vise til en sikkerhetsstrategi

- Kunne dokumentere at krav til personvern og konfidensialitet er oppfylt med hensyn til de ansatte, hos underleverandører og andre mottakere av Personopplysninger

- Etablere tilgangskontroll til systemer og data for å sikre at bare ansatte med et arbeidsrelatert behov for tilgang til Personopplysninger har tilgang

- Etablere tilgangskontroll til bygninger og utstyr for å sørge for at bare ansatte med et arbeidsrelatert behov for tilgang, har tilgang

- Benytte verktøy for virusbeskyttelse, spam-filtre og brannmurer når dette er nødvendig eller påkrevet

- Logge alle kritiske systemoperasjoner

- Kryptere kommunikasjon dersom det er nødvendig eller påkrevet. Helseopplysninger og andre Personopplysninger som krever særskilt beskyttelse under Gjeldende Personvernlovgivning skal alltid krypteres

- Etablere prosedyrer for sletting og anonymisering av Personopplysninger;

- Etablere prosedyrer for lagring og avhendelse av datamedium

- Ha systemer for backup/gjenopprettingsprosess for alle kritiske systemer og gjenopprettingstester

- Lære opp ansatte om informasjonssikkerhet og personvern

- Leverandørstyring vedrørende informasjonssikkerhetskrav

Databehandler skal kunne dokumentere tiltakene som er opplistet ovenfor så langt Gjeldende Personvernlovgivning krever dette. Dokumentasjonen skal være tilgjengelig for Behandlingsansvarlig på forespørsel.

Listen over sikkerhetstiltak skal ikke anses som uttømmende.