DATABEHANDLERAVTALE

Mellom

JURIDISK NAVN	ORGANISASJONSNUMMER

(«**Behandlingsansvarlig**»)

og

PayEx Norge AS, org. nr. 979 315 503, 0106 Oslo [for egen regning og på vegne av andre selskaper i PayEx-konsernet som PayEx Sverige AB, 556735-5671 Stockholm («**Databehandler**»)

Partene har inngått avtale om PayEx MediPay i henhold med Rammeavtalen ("**Avtalen**"). Avtalen vil kunne omfatte behandling av Personopplysninger i henhold til EU-forordning 2016/679, som er implementert i norsk lovgivning ved personopplysningsloven (lov 15. juni 2018 nr. 38) og personopplysningsforskriften (forskrift 15. juni 2018 nr. 876) ("**Gjeldende Personvernlovgivning**").

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

Til denne avtale følger det to vedlegg:

1) Behandlingsansvarlig instruksjoner og formål

2) Godkjenning av underbehandlere

Denne hovedteksten og vedleggene utfyller hverandre. Hvis kontraktsdokumentene er motstridende på noen måte, gjelder hovedteksten før vedleggene

1. Avtalens formål

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 1 til denne Databehandleravtalen.

Begreper og definisjoner benyttet i Avtalen skal forstås på samme måte som i personopplysningsloven.

«Behandling»	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
«Personopplysninger»	enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som

	direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet
«Behandlingsansvarlig»	en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,
«Databehandler»	en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige,
«Brudd på personopplysningssikkerheten»	et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet
«PayEx-konsern»	PayEx Norge AS og dets konsernselskaper til enhver tid
«Gjeldende lovverk»	viser til lovgivning, forskrifter og råd fra tilsynsmyndigheter som er gjeldende for Behandlingsansvarlig fra tid til annen (for eksempel direktiv 95/46 / EF, personvernforordning EU 2016/679, personopplysningsloven) (eller lov som erstatter den) og Datatilsynets forskrifter og generelle råd)
«Underdatabehandler»	betyr tredjeparter som etter disse databehandlingsvilkår har fullmakt til å behandle personopplysninger for å levere deler av tjenestene og eventuell tilknyttet teknisk støtte

2. Databehandlers plikter

Databehandleren bekrefter at denne vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne Avtalen oppfyller kravene i personopplysningsloven og vern av den registrertes rettigheter, herunder innfrir alle kravene etter personvernforordningens artikkel 32. Se også ytterligere plikter i punkt 4.

Databehandleren skal kun behandle personopplysningene basert på dokumenterte instrukser fra den Behandlingsansvarlige. Databehandleren skal til enhver tid kunne dokumentere slike instrukser. Databehandler skal ikke behandle personopplysninger Databehandleren får tilgang til på annen måte enn det som er nødvendig for å utføre de oppdrag som Databehandler har for den Behandlingsansvarlige.

Databehandleren skal bistå den Behandlingsansvarlige i å svare på anmodninger fra registrerte hensyntatt behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak. Dette gjelder både anmodninger fra de registrerte om å utøve sine rettigheter etter personvernforordningens kapittel III samt bistå den Behandlingsansvarlige med å sikre overholdelse av forpliktelsene knyttet til personopplysningssikkerhet. Tilsvarende gjelder for bistand med vurdering av personvernkonsekvenser og forhåndsdrøftinger i personvernforordningens artikkel

32 til 36, hensyntatt behandlingens art og den informasjonen som er tilgjengelig for Databehandleren. Foreligger det godkjente adferdsnormer etter personvernforordningens artikkel 40 eller godkjent sertifiseringsordning etter artikkel 42, som Databehandleren har påtatt seg å overholde eller være sertifisert etter, plikter Databehandleren å etterkomme slike adferdsnormer eller sertifiseringskrav.

Databehandleren skal føre protokoll (logg) over behandlingsaktiviteter denne utfører på vegne av den Behandlingsansvarlige, som skal inneholde minimum den informasjon som er pålagt etter personvernforordningen artikkel 30 nr. 2.

Databehandleren skal gjøre tilgjengelig for den Behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i dette punkt 2 er oppfylt, samt muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av den Behandlingsansvarlige eller en annen inspektør på fullmakt fra den Behandlingsansvarlige. Den Behandlingsansvarlige har selv det direkte ansvaret for kontakt og kommunikasjon med aktuelle tilsynsmyndigheter, herunder Datatilsynet. Disse forpliktelser skal utføres uten kostnad for den Behandlingsansvarlige. På partens forespørsel skal inspektøren inngå en taushetsavtale om gjennomgangen. Revisjoner hos Databehandleren kan også utføres av tilsynsmyndighet avhengig av lovkrav eller andre økonomiske forskrifter.

Databehandleren har taushetsplikt om personopplysninger som vedkommende får tilgang til som en følge av Avtalen og behandling av personopplysningene, og skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. Denne bestemmelsen gjelder også etter Avtalens opphør.

Databehandleren skal ikke utlevere opplysninger eller informasjon som denne behandler for den Behandlingsansvarlige til tredjepart uten eksplisitt pålegg fra den Behandlingsansvarlige. Henvendelser til Databehandleren skal Databehandleren videreformidle til Behandlingsansvarlige så raskt som mulig.

Er Databehandleren av den oppfatning at en instruks fra den Behandlingsansvarlige er i strid med personvernforordningen, personopplysningsloven, eller annen regulering av behandling av personopplysninger, skal Databehandleren umiddelbart underrette den Behandlingsansvarlige om Databehandlerens oppfatning.

Databehandleren skal underrette Behandlingsansvarlig om forekomsten av mistenkt brudd på personopplysningssikkerheten eller hendelse som sannsynligvis vil utvikle seg til en slik hendelse, uten urimelig forsinkelse, men senest 24 timer etter å ha blitt oppmerksom om dette.

3. Bruk av underleverandør

Databehandleren skal kun benytte underleverandører til behandling av personopplysninger (underdatabehandler) som er skriftlig godkjent av den Behandlingsansvarlige og som har bekreftet å gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne Avtalen oppfyller kravene i personopplysningsloven og vern av den registrertes rettigheter.

Godkjente underdatabehandlere ved Avtalens inngåelse er spesifisert i vedlegg 1 til Avtalen.

Behandlingsansvarlig gir Databehandleren generell tillatelse til bruk av underdatabehandler for behandling av personopplysninger etter Avtalen. I tilfelle Databehandleren har planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere, skal Databehandleren underrette den Behandlingsansvarlige om planene og dermed gi den Behandlingsansvarlige muligheten til å motsette seg slike endringer.

Underdatabehandler skal pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i Avtalen i bindende avtale hvor underdatabehandler skal gi

tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller lovmessige krav. Dersom underdatabehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger og kravene i Avtalen, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser.

4. Sikkerhet og avvik

Databehandleren skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven med forskrifter og de punkter som er opplistet i vedlegg 1. Databehandleren skal kunne dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på den Behandlingsansvarliges forespørsel.

I tilfelle sikkerhets- eller personvernbrudd, skal Databehandleren varsle den Behandlingsansvarlige uten ugrunnet opphold. Melding om brudd skal minimum inneholde:

1. Beskrivelse av arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt,

2. navnet på og kontaktopplysningene til personvernrådgiveren eller et annet kontaktpunkt der mer informasjon kan innhentes,

3. beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,

4. beskrivelse av de tiltak som er truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Dersom ikke alle opplysninger kan gis i første melding, skal opplysningene gis suksessivt så snart de foreligger.

Den Behandlingsansvarlige har ansvaret for å sende melding til tilsynsmyndighet, og Databehandler skal ikke sende slik melding eller kontakte tilsynsmyndighet uten at den Behandlingsansvarlige har gitt instruks om dette.

5. Overføring til tredjeland

Personopplysninger skal kun overføres til land utenfor EU/EØS (tredjeland) etter instruks fra den Behandlingsansvarlige. Databehandleren skal altså ikke overføre eller la personer i tredjeland på noen måte få tilgang til personopplysninger uten at Behandlingsansvarlig har eksplisitt godkjent dette skriftlig og gitt instruks om overføring eller tilgang på forhånd. Samtykke og instruks må dekke hvilke land opplysningene skal kunne overføres til. Overføring til tredjeland forutsetter, selv med samtykke og instruks, at de krav til sikkerhet og vern av de registrertes rettigheter som følger av personopplysningsloven og annet regelverk er ivaretatt.

6. Avtalens varighet, pålegg om stans, plikter ved opphør/oppsigelse

Avtalen gjelder så lenge Databehandleren behandler eller har tilgang til personopplysninger på vegne av Behandlingsansvarlige etter Avtalen.

Ved brudd på denne Avtalen, personopplysningsloven eller annet relevant regelverk, kan Behandlingsansvarlig pålegge Databehandleren å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandleren skal, etter den Behandlingsansvarliges instruksjon, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og sletter eksisterende kopier, med mindre det er et lovmessig krav om at personopplysningene skal fortsatt lagres. Dette gjelder også for eventuelle sikkerhetskopier, men hvor det er tilstrekkelig med å overskrive etter de etablerte rutiner for sikkerhetskopiering.

Den Behandlingsansvarlige skal motta en skriftlig bekreftelse fra Databehandleren på at alle personopplysninger er returnert eller slettet i henhold til den Behandlingsansvarliges instruksjoner og at Databehandleren ikke har beholdt kopi, utskrifter eller andre former for personopplysninger i noen form.

Behandlingsansvarliges rett til kompensasjon i henhold til avsnitt nummer 2 i dette kapittel skal være begrenset til direkte skade og skal styres av ansvarsbestemmelsen i avtalen mellom partene. Dette gjelder også eventuelle overtredelser begått av Underdatabehandler. Behandlingsansvarlig skal ikke under noen omstendighet være ansvarlig for indirekte skader, for eksempel tap av fortjeneste, tap av inntekt, oppfyllelse forpliktelser overfor tredjepart, ansvar overfor tredjepart eller andre følgeskader. Denne ansvarsbegrensningen skal imidlertid ikke gjelde i tilfelle grov uaktsomhet eller forsett.

7. Erstatning og ansvar

Databehandler skal holde Behandlingsansvarlig skadesløs for skader, krav eller administrasjonsgebyr som oppstår mot Behandlingsansvarlig på grunn av Databehandlerens behandling av personopplysninger som er i strid med denne avtalen 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.

Hvis Databehandler mottar et krav om erstatning eller administrasjonsgebyr rettet mot ham som følge av brudd på gjeldende lov, skal Databehandleren informere Behandlingsansvarlig uten unødig forsinkelse. Databehandlerne må ta rimelige tiltak for å begrense skadevirkningene av hendelsen.

8. Øvrige plikter og rettigheter

Øvrige plikter og rettigheter følger av Hovedavtalen som gjelder mellom Databehandleren og Behandlingsansvarlige om tjenestene som nødvendiggjør behandling av personopplysninger og denne Avtale. De samme kontaktpersoner gjelder for Avtalen som etter Hovedavtalen.

Denne Avtalen skal ikke utvide Behandlingsansvarliges sanksjonsmuligheter, herunder erstatningsansvar for Databehandleren, utover det som følger av Hovedavtalen.

Ved eventuell overdragelse av Hovedavtalen til andre parter, skal denne Avtale overdras tilsvarende.

9. Lovvalg

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.

Databehandler	**Behandlingsansvarlig**
_____	_____
NAVN:	NAVN:
STED/DATO:	STED/DATO:

Avtalen er utstedt i to originale eksemplarer, hvor partene har mottatt hvert sitt. Avtalen må signeres av signaturberettiget hos begge parter.

Vedlegg 1

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

PayEx Sverige AB

- Postnord Strålfors AB - TERMINALVÄGEN 24, 171 73 Solna, corp ID 556102-9843
- EDI Solutions AB - Box 9169, 400 94 Göteborg, corp ID 556569,5789
- Swedbank AB - LANDSVÄGEN 40, 172 Sundbyberg, corp ID 502017-7753
- 21 Grams AB - LUMAPARKSVÄGEN 9, 120 31 Stockholm, corp. ID 556666-3729
- SpeedLedger AB - SPANNMÅLSGATAN 19, 411 05 Göteborg, corp ID 556398-4904
- PayEx Norge AS – Postboks 613 Sentrum, 0106 OSLO, corp ID 979 315 503

PayEx Norge AS

- Experian AS - Postboks 5275 Majorstua, 0303 OSLO, corp ID 881 917 122
- Evry Norge AS – Postboks 4, 1330 FORNEBU, corp ID 933 012 867
- Systempartner Norge AS, nå Concent AS – Postboks 1302, 3205 Sandefjord, corp. ID 971 052 554
- Nets Branch Norway, Haavard Martinsens vei 54, 0978 OSLO, corp ID 996 345 734
- LinkMobility AS – Langkaia 1, 0150 OSLO, corp ID 992 434 643
- Vipps AS – Postboks 9236 Grønland, 0134 OSLO, corp. ID 918 713 867

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.