GLOOKO STANDARDKONTRAKTBESTEMMELSER

AFDELING I

Bestemmelse 1

Formål og anvendelsesområde

(a) Formålet med disse standardkontraktbestemmelser (herefter Bestemmelserne) er at sikre overholdelse af artikel 28, stk. 3 og 4, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

(b) De dataansvarlige og databehandlerne, der er opført i Bilag I, har accepteret disse Bestemmelser for at sikre overholdelse af artikel 28, stk. 3 og 4, i forordning (EU) 2016/679 og artikel 29, stk. 3 og 4, i forordning (EU) 2018/1725.

(c) Disse Bestemmelser finder anvendelse, hvis kravene i Hovedaftalen er opfyldt og til behandling af personoplysninger som anført i Bilag II.

(d) Bilag I-IV er en integrerende del af Bestemmelserne.

(e) Disse Bestemmelser berører ikke de forpligtelser, som den dataansvarlige er underlagt i henhold til forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725.

(f) Disse Bestemmelser sikrer ikke i sig selv, at forpligtelserne vedrørende internationale overførsler i henhold til kapitel V i forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725 overholdes.

Bestemmelse 2

Bestemmelsernes uforanderlighed

(a) Parterne forpligter sig til ikke at ændre Bestemmelserne, bortset fra at tilføje oplysninger til bilagene eller ajourføre oplysninger i dem.

(b) Dette forhindrer ikke parterne i at medtage de standardkontraktbestemmelser, der er fastsat i disse Bestemmelser, i en bredere kontrakt eller i at tilføje andre Bestemmelser eller yderligere garantier, forudsat at de ikke direkte eller indirekte er i strid med Bestemmelserne eller indskrænker de registreredes grundlæggende rettigheder eller frihedsrettigheder.

Bestemmelse 3

Fortolkning

(a) Hvor disse Bestemmelser anvender de udtryk, der er defineret i henholdsvis forordning (EU) 2016/679 eller forordning (EU) 2018/1725, har disse udtryk samme betydning som i nævnte forordning.

(b) Disse Bestemmelser skal læses og fortolkes i lyset af bestemmelserne i henholdsvis forordning (EU) 2016/679 eller forordning (EU) 2018/1725.

(c) Disse Bestemmelser må ikke fortolkes på en måde, der strider mod de rettigheder og forpligtelser, der er fastsat i forordning (EU) 2016/679/forordning (EU) 2018/1725, eller på en måde, som berører de registreredes grundlæggende rettigheder eller frihedsrettigheder.

Bestemmelse 4

Hierarki

I tilfælde af uoverensstemmelse mellem disse Bestemmelser og bestemmelserne i tilknyttede aftaler mellem parterne, der eksisterer på det tidspunkt, hvor disse Bestemmelser aftales eller indgås, har disse Bestemmelser forrang.

Bestemmelse 5 - Valgfri

Dockingklausul

(a) Enhver enhed, der ikke er part i disse Bestemmelser, kan efter aftale med alle parterne til enhver tid tiltræde disse Bestemmelser som dataansvarlig eller databehandler ved at udfylde bilagene og underskrive Bilag I.

(b) Når bilagene nævnt i punkt a) er udfyldt og underskrevet, behandles den tiltrædende enhed som part i disse Bestemmelser og har de rettigheder og forpligtelser, der tilkommer en dataansvarlig eller databehandler i overensstemmelse med udpegelsen af denne i Bilag I.

(c) Den tiltrædende enhed har ingen rettigheder eller forpligtelser som følge af disse Bestemmelser fra den periode, der går forud for enhedens tiltrædelse som part.

AFDELING II – PARTERNES FORPLIGTELSER

Bestemmelse 6

Beskrivelse af behandlingen af personoplysninger

Nærmere oplysninger om behandlingsaktiviteterne, navnlig de kategorier af personoplysninger og formålene med den behandling, hvortil personoplysningerne behandles på vegne af den dataansvarlige, er anført i Bilag II.

Bestemmelse 7

Parternes forpligtelser

7.1. Instrukser

(a) Databehandleren behandler kun personoplysninger efter dokumenterede instrukser fra den dataansvarlige, medmindre dette kræves i henhold til EU-retten eller medlemsstaternes nationale ret, som databehandleren er underlagt. I så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre loven forbyder dette af hensyn til vigtige samfundsinteresser. Efterfølgende instrukser kan også gives af den dataansvarlige under hele behandlingen af personoplysninger. Disse instrukser skal altid dokumenteres.

(b) Databehandleren underretter straks den dataansvarlige, hvis instrukser fra den dataansvarlige efter databehandlerens opfattelse er i strid med forordning (EU) 2016/679/forordning (EU) 2018/1725 eller de gældende databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

7.2. Formålsbegrænsning

Databehandleren må kun behandle personoplysningerne til det eller de specifikke formål med behandlingen, som er fastsat i Bilag II, medmindre han modtager yderligere instrukser fra den dataansvarlige.

7.3. Varigheden af behandlingen af personoplysninger

Behandlingen foretaget af databehandleren må kun finde sted i den periode, der er anført i Bilag II.

7.4. Behandlingssikkerhed

(a) Databehandleren gennemfører som minimum de tekniske og organisatoriske foranstaltninger, der er anført i Bilag III, for at garantere personoplysningernes sikkerhed. Dette omfatter beskyttelse af data mod brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til oplysningerne (brud på persondatasikkerheden). Ved vurderingen af det passende sikkerhedsniveau tager parterne behørigt hensyn til det aktuelle tekniske niveau, gennemførelsesomkostningerne, behandlingens karakter, omfang, kontekst og formål samt de risici, der består for de registrerede.

(b) Databehandleren giver kun sine medarbejdere adgang til personoplysninger, der behandles, i det omfang, det er strengt nødvendigt for gennemførelsen, forvaltningen og overvågningen af kontrakten. Databehandleren sikrer, at de personer, der er bemyndiget til at behandle de modtagne personoplysninger, har forpligtet sig til at iagttage fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

7.5. Følsomme oplysninger

Hvis behandlingen omfatter personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, genetiske data eller biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en persons seksuelle forhold eller seksuelle orientering eller oplysninger om straffedomme og lovovertrædelser (»følsomme oplysninger«), anvender databehandleren specifikke begrænsninger og/eller supplerende garantier.

7.6. Dokumentation og overholdelse

(a) Parterne skal kunne påvise, at de overholder disse Bestemmelser.

(b) Databehandleren behandler omgående og fyldestgørende forespørgsler fra den dataansvarlige om behandlingen af data i henhold til disse Bestemmelser.

(c) Databehandleren stiller alle de oplysninger til rådighed for den dataansvarlige, der er nødvendige for at påvise overholdelse af de forpligtelser, der er fastsat i disse Bestemmelser, og som følger direkte af forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725. På den dataansvarliges anmodning skal databehandleren også tillade og bidrage til revisioner af de behandlingsaktiviteter, der er omfattet af disse Bestemmelser, med rimelige mellemrum, eller hvis der er tegn på manglende overholdelse. Når den dataansvarlige træffer afgørelse om en gennemgang eller revision, kan denne tage hensyn til relevante certificeringer, som databehandleren er i besiddelse af.

(d) Den dataansvarlige kan vælge selv at gennemføre revisionen eller bemyndige en uafhængig revisor. Revisionen kan også omfatte inspektioner i databehandlerens lokaler eller fysiske faciliteter og skal, hvor det er relevant, gennemføres med et rimeligt varsel.

(e) Parterne stiller på anmodning de oplysninger, der er omhandlet i denne Bestemmelse, herunder resultaterne af eventuelle revisioner, til rådighed for de(n) kompetente tilsynsmyndighed(er).

7.7. Anvendelse af underdatabehandlere

(a) Databehandleren har den dataansvarliges generelle godkendelse til at indgå aftale med

underdatabehandlere fra en aftalt liste. Databehandleren underretter specifikt den dataansvarlige skriftligt om eventuelle påtænkte ændringer af denne liste som følge af, at underdatabehandlere tilføjes til listen eller erstattes, mindst tredive (30) dage på forhånd og giver derved den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer, inden aftale indgås med den eller de pågældende underdatabehandler(e). Databehandleren giver den dataansvarlige de oplysninger, der er nødvendige for, at den dataansvarlige kan udøve sin indsigelsesret.

(b) Hvis databehandleren indgår aftale med en underdatabehandler med henblik på at udføre specifikke behandlingsaktiviteter (på vegne af den dataansvarlige), skal databehandleren gøre dette i form af en kontrakt, der i det væsentlige pålægger underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der pålægges databehandleren i overensstemmelse med disse Bestemmelser. Databehandleren skal sikre, at underdatabehandleren opfylder de forpligtelser, som databehandleren er underlagt i henhold til disse Bestemmelser og til forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725.

(c) Databehandleren forelægger på den dataansvarliges anmodning en kopi af en sådan aftale med en underdatabehandler og eventuelle efterfølgende ændringer for den dataansvarlige. I det omfang det er nødvendigt for at beskytte forretningshemmeligheder eller andre fortrolige oplysninger, herunder personoplysninger, kan databehandleren redigere aftaleteksten, inden kopien videregives.

(d) Databehandleren forbliver fuldt ud ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser i henhold til dennes kontrakt med databehandleren. Databehandleren underretter den dataansvarlige om enhver manglende opfyldelse fra underdatabehandlerens side af dennes kontraktlige forpligtelser.

(e) Databehandleren indgår, hvor det er muligt en aftale om tredjemandsløfte med underdatabehandleren, hvorefter den dataansvarlige — i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller er blevet insolvent — har ret til at opsige kontrakten med underdatabehandleren og til at give underdatabehandleren en instruks om at slette eller tilbagelevere personoplysningerne.

7.8. Internationale overførsler

(a) Databehandlerens overførsel af oplysninger til et tredjeland eller en international organisation må kun ske på grundlag af dokumenterede instrukser fra den dataansvarlige eller for at opfylde et specifikt krav i henhold til EU-retten eller medlemsstaternes nationale ret, som databehandleren er underlagt, og skal finde sted i overensstemmelse med kapitel V i forordning (EU) 2016/679 eller forordning (EU) 2018/1725.

(b) Den dataansvarlige er enig i, at hvis databehandleren gør brug af en underdatabehandler i overensstemmelse med Bestemmelse 7.7 til at udføre specifikke behandlingsaktiviteter (på vegne af den dataansvarlige), og disse behandlingsaktiviteter indebærer en overførsel af personoplysninger som omhandlet i kapitel V i forordning (EU) 2016/679, kan databehandleren og underdatabehandleren sikre overensstemmelse med kapitel V i forordning (EU) 2016/679 ved hjælp af standardkontraktbestemmelser vedtaget af Kommissionen i overensstemmelse med artikel 46, stk. 2, i forordning (EU) 2016/679, forudsat at betingelserne for anvendelse af disse standardkontraktbestemmelser er opfyldt.

Bestemmelse 8

Bistand til den dataansvarlige

(a) Databehandleren henviser den registrerede til at kontakte den dataansvarlige, hvis databehandleren modtager en anmodning fra en registreret. Databehandleren må ikke selv besvare anmodningen, medmindre den dataansvarlige har givet tilladelse hertil.

(b) Databehandleren bistår den dataansvarlige med at opfylde dennes forpligtelse til at besvare registreredes anmodninger om udøvelse af deres rettigheder under hensyntagen til behandlingens karakter. Ved opfyldelsen af sine forpligtelser i henhold til punkt a) og b) skal databehandleren overholde den dataansvarliges instrukser.

(c) Ud over databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 8, punkt b), bistår databehandleren desuden den dataansvarlige med at sikre overholdelse af følgende forpligtelser under hensyntagen til databehandlingens karakter og de oplysninger, som databehandleren har til rådighed:

(1) forpligtelsen til at foretage en vurdering af de påtænkte behandlingsaktiviteters indvirkning på beskyttelsen af personoplysninger (en »konsekvensanalyse vedrørende databeskyttelse«), hvis en type behandling sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

(2) forpligtelsen til at høre de(n) kompetente tilsynsmyndighed(er) forud for behandling, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil medføre en høj risiko, hvis den dataansvarlige ikke træffer foranstaltninger til at mindske risikoen

(3) forpligtelsen til at sikre, at personoplysningerne er korrekte og ajourførte, ved straks at underrette den dataansvarlige, hvis databehandleren bliver opmærksom på, at de personoplysninger, der behandles, er ukorrekte eller er blevet forældede

(4) forpligtelserne i artikel 32 i forordning (EU) 2016/679.

(d) Parterne fastsætter i Bilag III de passende tekniske og organisatoriske foranstaltninger, som databehandleren skal anvende til at bistå den dataansvarlige ved anvendelsen af denne Bestemmelse, samt anvendelsesområdet for og omfanget af den nødvendige bistand.

Bestemmelse 9

Anmeldelse om brud på persondatasikkerheden

I tilfælde af brud på persondatasikkerheden samarbejder databehandleren med og bistår den dataansvarlige med henblik på, at den dataansvarlige opfylder sine forpligtelser i henhold til artikel 33 og 34 i forordning (EU) 2016/679 eller i henhold til artikel 34 og 35 i forordning (EU) 2018/1725, hvor det er relevant, under hensyntagen til behandlingens karakter og de oplysninger, som databehandleren har adgang til.

9.1 Brud på persondatasikkerheden vedrørende oplysninger, der behandles af den dataansvarlige

I tilfælde af brud på persondatasikkerheden vedrørende oplysninger, der behandles af den dataansvarlige, bistår databehandleren den dataansvarlige:

(a) med at anmelde bruddet på persondatasikkerheden til de(n) kompetente tilsynsmyndighed(er) uden unødig forsinkelse, efter at den dataansvarlige har fået kendskab til det, hvis det er relevant (medmindre bruddet på persondatasikkerheden sandsynligvis ikke vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder)

(b) med at indhente følgende oplysninger, som i henhold til artikel 33, stk. 3, i forordning (EU) 2016/679 skal angives i den dataansvarliges meddelelse, og skal som minimum omfatte:

(1) personoplysningernes art, herunder, hvis det er muligt, kategorierne og det

omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte personoplysninger

(2) de sandsynlige konsekvenser af bruddet på persondatasikkerheden

(3) de foranstaltninger, som den dataansvarlige har truffet eller foreslår at træffe for at afhjælpe bruddet på persondatasikkerheden, herunder, hvor det er relevant, foranstaltninger til at afbøde dets mulige negative virkninger.

Hvis og i det omfang det ikke er muligt at give alle disse oplysninger samtidig, skal den oprindelige anmeldelse indeholde de oplysninger, der er til rådighed, og yderligere oplysninger skal efterfølgende gives uden unødig forsinkelse, i takt med at de foreligger.

(c) i henhold til artikel 34 i forordning (EU) 2016/679 med at overholde forpligtelsen til uden unødig forsinkelse at underrette den registrerede om bruddet på persondatasikkerheden, hvis bruddet på persondatasikkerheden sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

9.2 Brud på persondatasikkerheden vedrørende oplysninger, der behandles af databehandleren

I tilfælde af brud på persondatasikkerheden vedrørende oplysninger, der behandles af databehandleren, underretter databehandleren uden unødig forsinkelse den dataansvarlige, efter at databehandleren har fået kendskab til bruddet. Meddelelsen skal som minimum indeholde:

a) en beskrivelse af overtrædelsens art (herunder om muligt kategorierne og det omtrentlige antal berørte registrerede og berørte personoplysninger)
b) nærmere oplysninger om et kontaktpunkt, hvor der kan indhentes flere oplysninger om bruddet på persondatasikkerheden
c) dets sandsynlige konsekvenser og de foranstaltninger, der er truffet eller foreslås truffet for at afhjælpe bruddet, herunder for at afbøde dets eventuelle negative virkninger.

Hvis og i det omfang det ikke er muligt at give alle disse oplysninger samtidig, skal den oprindelige anmeldelse indeholde de oplysninger, der er til rådighed, og yderligere oplysninger skal efterfølgende gives uden unødig forsinkelse, i takt med at de foreligger.

Parterne fastsætter i Bilag III alle andre elementer, som databehandleren skal fremlægge, når denne bistår den dataansvarlige i overensstemmelse med den dataansvarliges forpligtelser i henhold til artikel 33 og 34 i forordning (EU) 2016/679.

AFDELING III – AFSLUTTENDE BESTEMMELSER

Bestemmelse 10

Manglende overholdelse af Bestemmelserne og ophævelse

(a) Med forbehold af eventuelle Bestemmelser i forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725 kan den dataansvarlige i tilfælde af, at databehandleren misligholder sine forpligtelser i henhold til disse Bestemmelser, give databehandleren en instruks om at suspendere behandlingen af personoplysninger, indtil sidstnævnte overholder disse Bestemmelser, eller Hovedaftalen ophæves. Databehandleren underretter straks den dataansvarlige, hvis denne af en eller anden grund ikke er i stand til at overholde disse Bestemmelser.

(b) Den dataansvarlige har ret til at opsige Hovedaftalen, for så vidt den vedrører behandling af personoplysninger i henhold til disse Bestemmelser, hvis:

(1) databehandlerens behandling af personoplysninger er blevet suspenderet af den dataansvarlige i henhold til punkt a), og hvis overholdelsen af disse Bestemmelser ikke er blevet genoprettet inden for en rimelig frist og under alle omstændigheder

senest en måned efter suspensionen

(2) databehandleren i væsentlig eller vedvarende grad misligholder disse Bestemmelser eller sine forpligtelser i henhold til forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725

(3) databehandleren ikke overholder en bindende afgørelse fra en kompetent domstol eller de(n) kompetente tilsynsmyndighed(er) vedrørende sine forpligtelser i henhold til disse Bestemmelser eller til forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725.

(c) Databehandleren har ret til at opsige Hovedaftalen, for så vidt den vedrører behandling af personoplysninger i henhold til disse Bestemmelser, hvis den dataansvarlige efter at være blevet underrettet om, at dennes instrukser er i strid med gældende retlige krav i overensstemmelse med Bestemmelse 7.1, punkt b), insisterer på, at instrukserne overholdes.

(d) Når Hovedaftalen er bragt til ophør, sletter databehandleren efter den dataansvarliges valg alle personoplysninger, som denne har behandlet på vegne af den dataansvarlige, og attesterer over for den dataansvarlige, at oplysningerne er blevet slettet, eller tilbageleverer alle personoplysninger til den dataansvarlige og sletter eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret kræver, at personoplysningerne gemmes. Hvis den dataansvarlige ikke har anmodet om at få returneret alle personoplysninger, der er behandlet på vegne af den dataansvarlige indenfor tredive (30) dage efter ophør af Hovedaftalen, har databehandleren ret til efter eget skøn at slette personoplysningerne. Indtil oplysningerne er slettet eller leveret tilbage, skal databehandleren fortsat sikre, at disse Bestemmelser overholdes.

BILAG I: LISTE OVER PARTER

Dataansvarlig(e):

1. *Klienten (som defineret i Hovedaftalen eller Bestillingsformular)*

Databehandler(e):

1. *Glooko AB (som defineret i Hovedaftalen)*

BILAG II: BESKRIVELSE AF BEHANDLINGEN

Kategorier af registrerede, hvis personoplysninger behandles

- Autoriserede Brugere
- Patienter

Kategorier af personoplysninger, der behandles

For Autoriserede Brugere

- Generelle oplysninger (navn)
- Kontaktoplysninger (e-mailadresse, telefonnummer)
- Brugeroplysninger (brugernavn, adgangskode, adgangsrettigheder, auditlogning)

For Patienter

- Generelle oplysninger (navn, fødselsdato, køn)
- Kontaktoplysninger (postadresse, e-mailadresse, telefonnummer)
- Brugeroplysninger (brugernavn, adgangskode)
- Helbredsoplysninger (diabetes typer, årstal for diabetesdiagnoser, estimeret partus, målværdi, vægt, højde, behandlinger)
- Oplysninger om enhed (insulinpumpe, serienumre på glukosemåler og insulinen, doser, kulhydrater, indstillinger, alarmer)

Følsomme oplysninger, der behandles (hvis relevant) og anvendte begrænsninger eller garantier, der fuldt ud tager hensyn til oplysningernes art og de involverede risici, f.eks. streng formålsbegrænsning, adgangsbegrænsninger (herunder kun adgang for personale, der har fulgt en specialuddannelse), registrering af adgangen til oplysningerne, begrænsninger for videreoverførsel eller yderligere sikkerhedsforanstaltninger.

- Helbredsoplysninger

Der henvises til Bilag III for oplysninger om implementerede foranstaltninger

……..

Behandlingens art

Indsamling, analyse, visualisering og på anden måde behandling af personoplysninger i overensstemmelse med Hovedaftalen.

Formål, hvortil personoplysningerne behandles på vegne af den dataansvarlige
For at gøre det muligt for den dataansvarlige og dens autoriserede brugere at bruge Softwaren og andre Leverancer i overensstemmelse med Hovedaftalen.

Behandlingens varighed

Varigheden af levering af Softwaren og andre Leverancer i henhold til Hovedaftalen.

……
Ved behandling af (under)databehandlere angives også behandlingens genstand, art og varighed.

Se Bilag IV

Instruktioner under afsnit 7.8 a) i Bestemmelserne vedrørende internationale overførsler

Standardkontraktbestemmelserne for internationale overførsler ("SCC'erne") i Bilag V finder anvendelse, hvis databehandleren overfører personoplysninger uden for EØS til et land, der ikke er anerkendt af Europa-Kommissionen som havende et tilstrækkeligt beskyttelsesniveau for personoplysninger.

BILAG III: TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER, HERUNDER TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF DATASIKKERHEDEN

1. Formål. Dette Bilag beskriver Glookos sikkerhedsprogram, sikkerhedscertificeringer, og tekniske samt organisatoriske foranstaltninger med henblik på at beskytte (a) personoplysninger behandlet af databehandleren på vegne af den dataansvarlige imod uautoriseret brug, adgang, tilrådighedsstillelse, og tyveri samt (b) Software. Som følge af, at sikkerhedstrusler skifter og udvikler sig, opdaterer Glooke løbende dets sikkerhedsprogram og strategi for at beskytte personoplysninger og Software. Glooko reserverer retten til at opdatere dette Bilag fra tid til anden, under forudsætning af, at opdateringer ikke materielt vil reducere den generelle beskyttelse fastlagt i dette bilag.

2. Sikkerhedsorganisationen og -Programmet. Glooko opretholder en risikobaseret vurdering af sikkerhedsprogrammet. Grundlaget for Glookos sikkerhedsprogram inkluderer administrative, organisatoriske, tekniske og fysiske sikkerhedsforanstaltninger, der med rimelighed er designet til at beskytte Software og fortroligheden, integriteten og tilgængeligheden af personoplysninger. Glookos sikkerhedsprogram er tilrettelagt ud fra Softwarens art og størrelse samt kompleksiteten af Glookos forretningsdrift. Glooko har et særskilt og dedikeret informationssikkerhedsteam, der håndterer Glookos sikkerhedsprogram. Det pågældende team faciliterer og supporterer uafhængige revisioner og vurderinger udført af tredjeparter. Rammen for Glookos sikkerhedsprogram omfatter: Politikker og Procedurer, Aktivforvaltning, Adgangsstyring, Kryptografi, Fysisk Sikkerhed, Operationel sikkerhed, Kommunikationssikkerhed, Beredskabssikkerhed, Sikkerhed for Personer, Produktsikkerhed, Cloud- og Netværkssikkerhed, Sikkerhedscompliance, Tredjepartssikkerhed, Håndtering af Sårbarheder, og Overvågning af Sikkerhed samt Hændelsesrespons. Sikkerheden håndteres på det højeste niveau via Glookos Security Officer, der regelmæssigt afholder møder med direktionen for at diskutere problemstillinger samt for at koordinere sikkerhedsinitiativer. Informationssikkerhedspolitikker og –standarder bliver som minimum årligt gennemgået og godkendt af direktionen og bliver stillet til rådighed for Glookos medarbejdere.

3. Fortrolighed. Glooko har implementeret kontroller med henblik på at sikre fortroligheden af personoplysninger i overensstemmelse med Hovedaftalen. Samtlige af Glookos medarbejdere og konsulenter er bundet af Glookos interne politikker vedrørende fortrolig behandling af personoplysninger og er kontraktuelt forpligtede til at overholde disse krav.

4. Sikkerhed for Personer

a. Baggrundstjek af Personer. Glooko udfører baggrundstjek af alle nye medarbejdere på tidspunktet for ansættelse i overensstemmelse med gældende lokal lovgivning. Glooko verificerer på nuværende tidspunkt nye medarbejderes uddannelse og tidligere ansættelser samt udfører kontrol af referencer. Hvor det er tilladt i henhold til gældende lovgivning, kan Glooko også foretage kriminalitets-, kredit-, immigrations- og sikkerhedstjek afhængigt af arten og omfanget af en ny medarbejders rolle.

b. Uddannelse af Medarbejdere. Som minimum én (1) gang om året skal samtlige af Glookos medarbejdere gennemføre undervisning i sikkerhed og privatliv, der omfatter Glookos sikkerhedspolitikker, best practice for sikkerhed, og principperne for privatliv. Medarbejdere på barsel kan modtage ekstra tid med henblik på at gennemføre den årlige

undervisning. Glookos dedikerede sikkerhedsteam udfører også bevidsthedskampagner om phishing og meddeler løbende medarbejdere om nye trusler.

5. Tredjeparts Leverandørstyring

a. Leverandørvurdering. Glooko kan bruge tredjepartsleverandører til at levere Softwaren. Glooko foretager en sikkerhedsrisikobaseret vurdering af potentielle leverandører, inden vi indgår i et samarbejde med dem for at validere, at de opfylder Glookos sikkerhedskrav. Glooko gennemgår med jævne mellemrum hver leverandør i lyset af Glookos standarder for sikkerhed og forretningskontinuitet, herunder typen af adgang og klassificering af oplysninger der tilgås (hvis nogen), nødvendige kontrolelementer for at beskytte oplysninger og juridiske/lovgivningsmæssige krav. Glooko sikrer, at personoplysninger returneres og/eller slettes ved afslutningen af et leverandørforhold.

b. Leverandøraftaler. Glooko indgår skriftlige aftaler med alle sine leverandører, som omfatter forpligtelser vedrørende fortrolighed, privatliv og sikkerhed, der giver et passende beskyttelsesniveau for personoplysninger, som disse leverandører kan behandle.

6. Arkitektur, Firewalls og Datasegregering. Enhver netværksadgang mellem produktionsværter er begrænset ved hjælp af firewalls, så kun autoriserede tjenester kan interagere i produktionsnetværket. Firewalls bruges til at styre netværkssegregering mellem forskellige sikkerhedszoner i produktions- og virksomhedsmiljøer. Glooko adskiller logisk sine databaser. Glooko API'ere er designet og bygget til kun at identificere og give adgang til og fra de respektive afsendere. Disse kontroller forhindrer kunder i at få adgang til andre kunders oplysninger.

7. Fysisk Sikkerhed. De datacentre, der er genstand for Softwaren, er strengt kontrolleret både i perimeter og ved adgangspunkter af professionelt sikkerhedspersonale ved hjælp af videoovervågning, systemer til overvågning af indtrængen og andre elektroniske midler. Uafbrydelige strømforsyninger og generatorer på stedet kan levere nødstrøm i tilfælde af elektrisk fejl. Derudover har Glookos hovedkvarter og kontorlokaler et fysisk sikkerhedsprogram, der administrer besøgende, indgange til lokalerne og generel kontorsikkerhed.

8. Security by Design. Glooko følger principperne for security by design, når der Softwaren designes. Glooko anvender også standarden Glooko Software Development Lifecycle (SDLC) til at udføre adskillige sikkerhedsrelaterede aktiviteter for Softwaren på tværs af forskellige faser af produktudviklingens livscyklus, fra indsamling af produktkrav til produktdesign og hele vejen igennem produktimplementering.

9. Adgangskontrol

a. Tilvejebringelse af Adgang. For at minimere risikoen for dataeksponering følger Glooko princippet om mindst mulig forret ved hjælp af en teambaseret adgangskontrol, når der gives adgang til systemer. Glookos medarbejdere har tilladelse til at få adgang til personoplysninger baseret på deres jobfunktion, rolle og ansvar, og sådan adgang kræver godkendelse af medarbejderens leder. En medarbejders adgang til personoplysninger fjernes ved ophør af deres ansættelse. Inden en tekniker får adgang til produktionsmiljøet, skal adgangen godkendes af ledelsen, og teknikeren skal gennemføre intern undervisning til sådan adgang, herunder uddannelser i det relevante teams systemer. Glooko registrerer handlinger med høj risiko og ændringer i produktionsmiljøet. Glooko anvender

automatisering til at identificere enhver afvigelse fra interne tekniske standarder, der kan indikere unormal/uautoriseret aktivitet for at udløse en alarm inden for få minutter efter en konfigurationsændring.

b. Kontrol af Adgangskode. Når en Autoriseret Bruger logger ind på sin konto, hasher Glooko brugerens legitimationsoplysninger, før den gemmes. Klienter kan også kræve, at dets Autoriserede Brugere tilføjer endnu et sikkerhedslag til deres konto ved hjælp af tofaktorautentificering (2FA).

10. Forandringsledelse. Glooko har en formel proces for forandringsledelse, der følges for at administrere ændringer i produktionsmiljøet for Softwaren, herunder eventuelle ændringer i den underliggende software, applikationer, og systemer. Hver ændring gennemgås og evalueres omhyggeligt i et testmiljø, før den indsættes i produktionsmiljøet for Softwaren. Alle ændringer, herunder evaluering af ændringerne i et testmiljø, dokumenteres ved hjælp af et formaliseret, kontrollerbart registreringssystem. Der kræves implementeringsgodkendelse for højrisikoændringer fra de korrekte interessenter i organisationen. Planer og procedurer implementeres også, hvis en implementeret ændring skal rulles tilbage for at sikre Softwarens sikkerhed.

11. Kryptering. For Softwaren er (a) de databaser, der opbevarer personoplysninger, krypterede ved hjælp af Advanced Encryption Standard og (b) personoplysninger er krypterede, når de transmitteres mellem Klientens softwareapplikation og Softwaren ved hjælp af TLS v1.2.

12. Sårbarhedsstyring. Glooko opretholder kontroller og politikker for at afbøde risikoen for sikkerhedshuller, for at afbalancere risici samt forretnings- og operationelle krav. Glooko bruger et tredjepartsværktøj til regelmæssigt at foretage scanninger for at vurdere sårbarheder i Glookos cloud-infrastruktur og systemer i virksomheden.

13. Penetrationstest. Glooko udfører penetrationstest og engagerer tredjepartsenheder til at gennemføre penetrationstest på applikationsniveau. Sikkerhedstrusler og sårbarheder, der opdages prioriteres, sorteres og afbødes.

14. Håndtering af Sikkerhedshændelser. Glooko opretholder politikker for håndtering af sikkerhedshændelser. Glookos hændelsesresponsteam (T-SIRT) vurderer alle relevante sikkerhedstrusler og -sårbarheder og etablerer passende foranstaltninger for afbødning. Glooko bevarer sine sikkerhedslogfiler.

15. Modstandsdygtighed og kontinuitet i Software. Softwaren anvender en række forskellige værktøjer og mekanismer til at opnå høj tilgængelighed og modstandsdygtighed. For Softwaren spænder Glookos infrastruktur over flere fejluafhængige tilgængelighedszoner i geografiske områder, der er fysisk adskilt fra hinanden. Glooko anvender også specialiserede værktøjer, der overvåger serverens ydeevne, data og trafikkapacitet inden for hver tilgængelighedszone og colocation-datacenter. Hvis der opdages serverydelse under det optimale eller overbelastet kapacitet på en server inden for en tilgængelighedszone eller colocation-datacenter, øger disse specialiserede værktøjer kapaciteten eller skifter trafik for at aflaste enhver suboptimal serverydelse eller kapacitetsoverbelastning. Ligeledes får Glooko straks besked i tilfælde af suboptimal serverydelse eller overbelastet kapacitet.

16. Sikkerhedskopier og gendannelse. Glooko foretager regelmæssig sikkerhedskopiering af personoplysninger. Personoplysninger der sikkerhedskopieres, opbevares redundant på tværs af flere tilgængelighedszoner og krypteres under transmission og i hvile ved hjælp af Advanced Encryption Standards.

BILAG IV: LISTE OVER UNDERDATABEHANDLERE

Den dataansvarlige har givet tilladelse til, at følgende underdatabehandlere anvendes:

1.

Navn: Amazon Web Services EMEA SARL

Adresse: 38 Avenue John F. Kennedy, L-1855, Luxembourg

Beskrivelse af behandlingen (herunder en klar ansvarsfordeling, hvis flere underdatabehandlere er godkendt): Cloud udbyder

2.

Navn: Cegedim SA

Adresse: 137 rue d'Aguesseau, 92100 Boulogne-Billancourt, Frankrig

Beskrivelse af behandlingen (herunder en klar ansvarsfordeling, hvis flere underdatabehandlere er godkendt): Cloud udbyder (kan anvendes af Klienter, der er lokaliseret i Frankrig).

3.

Navn: Pictime Groupe

Adresse: Campus du Digital 61, rue de l'Harmonie - 59262 Sainghin-en-Mélantois, Frankrig

Beskrivelse af behandlingen (herunder en klar ansvarsfordeling, hvis flere underdatabehandlere er godkendt): Certificeret sundhedsdatavært (kan anvendes af Klienter, der er lokaliseret i Frankrig og Tyskland).

BILAG V: STANDARDKONTRAKTBESTEMMELSER

AFSNIT I

Bestemmelse 1

Formål og anvendelsesområde

(a) Formålet med disse standardkontraktbestemmelser er at sikre overholdelse af kravene i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)[1] ved overførsel af personoplysninger til et tredjeland.

(b) Parterne:

(i) Den/det eller de fysiske eller juridiske person(er), offentlige myndighed(er), kontor(er) eller andre organ(er) (herefter benævnt "enhed(er)"), der overfører personoplysningerne, jf. bilag I.A., (herefter benævnt "dataeksportør") og

(ii) den/de enhed(er) i et tredjeland, der modtager personoplysningerne fra dataeksportøren, direkte eller indirekte via en anden enhed, der også anvender disse standardkontraktbestemmelser, jf. bilag I.A., (herefter begge benævnt ("dataimportør")

har aftalt at anvende disse standardkontraktbestemmelser (herefter benævnt: "bestemmelser").

(c) Disse bestemmelser gælder for overførsel af personoplysninger som omhandlet i bilag I.B.

(d) Tillægget til disse bestemmelser, der indeholder de bilag, der henvises til heri, udgør en integreret del af disse bestemmelser.

Bestemmelse 2

Bestemmelsernes virkning og ufravigelighed

(a) Disse bestemmelser fastsætter fornødne garantier, herunder rettigheder for registrerede, som kan håndhæves, samt effektive retsmidler, jf. artikel 46, stk. 1, og artikel 46, stk. 2, litra c), i forordning (EU) 2016/679, og vedrørende dataoverførsler fra dataansvarlige til databehandlere og/eller fra databehandlere til databehandlere standardkontraktbestemmelser, jf. artikel 28, stk. 7, i forordning (EU) 2016/679,

[1] Hvis dataeksportøren er en databehandler i medfør af forordning (EU) 2016/679, der handler på vegne af en EU-institution eller et EU-organ i egenskab af dataansvarlig, skal anvendelse af disse standardkontraktbestemmelser ved brug af en anden databehandler (underkontraheret databehandling), der ikke er omfattet af forordning (EU) 2016/679, også sikre overholdelse af artikel 29, stk. 4, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39) i det omfang, at disse standardkontraktbestemmelser samt databeskyttelsesforpligtelser som fastsat i kontrakten eller et andet retligt dokument mellem den dataansvarlige og databehandleren, jf. artikel 29, stk. 3, i forordning (EU) 2018/1725, er tilpasset hinanden. Dette vil navnlig være tilfældet, hvis den dataansvarlige og databehandleren baserer sig på standardkontraktbestemmelserne i afgørelse [...].

forudsat at disse ikke ændres, undtaget med det formål at vælge det/de passende modul(er) eller tilføje eller opdatere oplysninger i tillægget. Dette forhindrer ikke parterne i at inkludere standardkontraktbestemmelserne, der er fastsat i disse bestemmelser, i en bredere kontrakt og/eller tilføje andre bestemmelser eller yderligere garantier, forudsat at disse ikke direkte eller indirekte er i modstrid med disse bestemmelser eller udgør en krænkelse af de registreredes grundlæggende rettigheder eller frihedsrettigheder.

(b) Disse bestemmelser berører ikke de forpligtelser, som dataeksportøren er underlagt i medfør af forordning (EU) 2016/679.

Bestemmelse 3

Begunstigede tredjemænd

(a) De registrerede kan påberåbe sig og håndhæve disse bestemmelser som begunstigede tredjemænd over for dataeksportøren og/eller dataimportøren med følgende undtagelser:

(i) Bestemmelse 1, bestemmelse 2, bestemmelse 3, bestemmelse 6, bestemmelse 7

(ii) Bestemmelse 8 — Modul et: Bestemmelse 8.5, litra e), og bestemmelse 8.9, litra b), Modul to: Bestemmelse 8.1, litra b), bestemmelse 8.9, litra a), c), d) og e), Modul tre: Bestemmelse 8.1, litra a), c) og d), og bestemmelse 8.9, litra a), c), d), e), f) og g), Modul fire: Bestemmelse 8.1, litra b), og bestemmelse 8.3, litra b)

(iii) Bestemmelse 9 — Modul to: Bestemmelse 9, litra a), c), d) og e), Modul tre: Bestemmelse 9, litra a), c), d) og e)

(iv) Bestemmelse 12 — Modul et: Bestemmelse 12, litra a) og d), Modul to og tre: Bestemmelse 12, litra a), d) og f)

(v) Bestemmelse 13

(vi) Bestemmelse 15.1, litra c), d) og e)

(vii) Bestemmelse 16, litra e)

(viii) Bestemmelse 18 — Modul et, to og tre: Bestemmelse 18, litra a) og b), Modul fire: Bestemmelse 18.

(b) Litra a) berører ikke de registreredes rettigheder i henhold til forordning (EU) 2016/679.

Bestemmelse 4

Fortolkning

(a) Hvis begreber, der er fastlagt i forordning (EU) 2016/679, anvendes i disse bestemmelser, har de den samme betydning som i forordningen.

(b) Disse bestemmelser skal læses og fortolkes på baggrund af bestemmelserne i forordning (EU) 2016/679.

(c) Disse bestemmelser må ikke fortolkes på måder, der er i strid med de rettigheder og forpligtelser, der er fastsat i forordning (EU) 2016/679.

Bestemmelse 5

Hierarki

I tilfælde af en modsætning mellem disse bestemmelser og bestemmelser i andre relevante aftaler mellem parterne, der er indgået på det tidspunkt, hvor disse bestemmelser bliver aftalt, eller som efterfølgende indgås, har disse bestemmelser forrang.

Bestemmelse 6

Beskrivelse af overførslen/overførslerne

Detaljerede oplysninger om overførslen eller overførslerne, navnlig de kategorier af personoplysninger, der overføres, og formålet eller formålene med overførslen, er anført i bilag I.B.

Bestemmelse 7 — Fakultative bestemmelser

Tillægsbestemmelse

Ikke relevant.

AFSNIT II — PARTERNES FORPLIGTELSER

Bestemmelse 8

Databeskyttelsesgarantier

Dataeksportøren garanterer, at denne har gjort en rimelig indsats for at kontrollere, at dataimportøren, når denne gennemfører tilstrækkelige tekniske og organisatoriske foranstaltninger, kan opfylde sine forpligtelser i henhold til disse bestemmelser.

8.1 Instrukser

(a) Dataeksportøren behandler kun personoplysningerne efter dokumenterede instrukser fra dataimportøren, der optræder i egenskab af dataansvarlig.

(b) Dataeksportøren underretter straks dataimportøren, hvis denne ikke er i stand til at følge disse instrukser, herunder hvis sådanne instrukser er i strid med forordning (EU) 2016/679 eller anden EU-ret eller medlemsstatslovgivning om databeskyttelse.

(c) Dataimportøren afstår fra enhver handling, der forhindrer dataeksportøren i at opfylde sine forpligtelser i henhold til forordning (EU) 2016/679, herunder i forbindelse med underkontraheret databehandling eller for så vidt angår samarbejde med de kompetente tilsynsmyndigheder.

(d) Når behandlingen er afsluttet og efter dataimportørens anvisning, sletter dataeksportøren alle personoplysninger, som denne har behandlet på vegne af dataimportøren, og bekræfter over for dataimportøren, at arbejdet er afsluttet, eller tilbageleverer alle personoplysninger til dataimportøren, som er blevet behandlet på vegne af denne, og sletter eksisterende kopier.

8.2 Sikkerhed i forbindelse med behandling

(a) Parterne iværksætter tilstrækkelige tekniske og organisatoriske sikkerhedsforanstaltninger til at garantere datasikkerheden, herunder under videregivelse, samt til beskyttelse mod sikkerhedsbrud, der kan føre til hændelig eller ulovlig ødelæggelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysningerne (herefter benævnt "brud på persondatasikkerheden"). Når de vurderer det passende sikkerhedsniveau, tager de behørigt hensyn til den bedste teknologi, implementeringsomkostninger, personoplysningernes art[2], behandlingens art, omfang, sammenhæng og formål samt de risici, som behandlingen indebærer for de registrerede, og overvejer især at anvende kryptering eller pseudonymisering, herunder under overførslen, hvis dette ikke forhindrer opfyldelsen af formålet med behandlingen.

(b) Dataeksportøren bistår dataimportøren med at garantere en passende datasikkerhed i overensstemmelse med litra a). I tilfælde af brud på persondatasikkerheden vedrørende de personoplysninger, som dataeksportøren behandler i henhold til disse bestemmelser, underretter dataeksportøren dataimportøren uden unødig forsinkelse efter at have fået kendskab hertil og bistår dataimportøren med at afhjælpe sikkerhedsbruddet.

(c) Dataimportøren sikrer, at personer, der har tilladelse til at behandle personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

8.3 Dokumentation og overholdelse

(a) Parterne skal kunne påvise, at de overholder disse bestemmelser.

(b) Dataeksportøren stiller alle de oplysninger til rådighed for dataimportøren, der er nødvendige for at påvise, at dataeksportøren overholder sine forpligtelser i henhold til disse bestemmelser, og giver mulighed for samt bidrager til revisioner.

Bestemmelse 9

Brug af underdatabehandlere

Ikke relevant.

Bestemmelse 10

De registreredes rettigheder

Parterne bistår hinanden med at besvare forespørgsler og anmodninger fra registrerede i henhold til den lokale lovgivning, der finder anvendelse på dataimportøren, eller i henhold til forordning (EU) 2016/679 ved databehandling foretaget af dataeksportøren i EU.

[2] Dette omfatter, om overførslen og den videre behandling omfatter personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, genetiske data eller biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en persons seksuelle forhold eller seksuelle orientering eller om straffedomme eller lovovertrædelser.

Bestemmelse 11

Klageadgang

(a) Dataimportøren underretter de registrerede i et gennemsigtigt og lettilgængeligt format, via individuel meddelelse eller på sit websted om et kontaktpunkt, der er bemyndiget til at behandle klager. Dataimportøren behandler straks klager, som den modtager fra en registreret.

Bestemmelse 12

Ansvar

(a) Parterne er ansvarlige over for den eller de andre parter for eventuel skade, som en part påfører den eller de andre parter ved overtrædelse af disse bestemmelser.

(b) Parterne er ansvarlige over for den registrerede, og den registrerede har ret til erstatning for materiel eller immateriel skade, som parten forårsager den registrerede ved at tilsidesætte tredjemandsløftet i henhold til disse bestemmelser. Dette berører ikke dataeksportørens forpligtelser, jf. forordning (EU) 2016/679.

(c) Hvis mere end én part er ansvarlig for skader, der påføres den registrerede som følge af en overtrædelse af disse bestemmelser, hæfter alle ansvarlige parter solidarisk, og den registrerede har ret til at anlægge sag mod enhver af disse parter.

(d) Parterne er enige om, at hvis en part drages til ansvar i henhold til litra c), har denne part ret til at kræve kompensation fra den eller de andre parter for den del af erstatningen, der svarer til dens eller deres ansvar for skaden.

(e) Dataimportøren kan ikke unddrage sig sit eget ansvar ved at påberåbe sig en databehandlers eller underdatabehandlers adfærd.

Bestemmelse 13

Tilsyn

Ikke relevant.

AFSNIT III — LOKALE LOVE OG FORPLIGTELSER I TILFÆLDE AF OFFENTLIGE MYNDIGHEDERS ADGANG

Bestemmelse 14

Lokale love og praksis, der påvirker overholdelsen af bestemmelserne

Ikke relevant.

Bestemmelse 15

Dataimportørens forpligtelser i tilfælde af offentlige myndigheders adgang

Ikke relevant.

AFSNIT IV — AFSLUTTENDE BESTEMMELSER

Bestemmelse 16

Manglende overholdelse af bestemmelserne og ophævelse

(a) Dataimportøren informerer omgående dataeksportøren, hvis dataimportøren uanset årsagen ikke kan overholde disse bestemmelser.

(b) Hvis dataimportøren overtræder disse bestemmelser eller ikke er i stand til at overholde bestemmelserne, suspenderer dataeksportøren overførslen af personoplysninger til dataimportøren, indtil overtrædelsen bringes til ophør eller kontrakten ophører. Dette berører ikke bestemmelse 14, litra f).

(c) Dataeksportøren har ret til at opsige kontrakten, for så vidt den vedrører behandling af personoplysninger i henhold til disse bestemmelser, hvis:

(i) dataeksportøren har suspenderet videregivelsen af personoplysninger til dataimportøren i henhold til litra b), og overholdelsen af disse bestemmelser ikke genetableres inden for en rimelig frist og under alle omstændigheder senest en måned efter suspensionen

(ii) dataimportøren på alvorlig eller vedvarende vis tilsidesætter disse bestemmelser eller

(iii) dataimportøren ikke efterkommer en bindende afgørelse truffet af en kompetent domstol eller tilsynsmyndighed vedrørende dennes forpligtelser i henhold til disse bestemmelser.

I så fald underretter dataimportøren den kompetente tilsynsmyndighed [til modul tre: og den dataansvarlige] om en sådan manglende overholdelse. Hvis kontrakten omfatter mere end to parter, kan dataeksportøren kun udøve denne opsigelsesret over for den relevante

(d) Personoplysninger indsamlet af dataeksportøren i EU, som allerede er overført inden kontraktens ophør i henhold til litra c), skal straks slette i deres helhed, herunder eventuelle kopier heraf. Dataimportøren dokumenterer sletningen af oplysningerne over for dataeksportøren. Indtil dataene slettes eller returneres, skal dataimportøren fortsat sikre, at disse bestemmelser overholdes. I tilfælde, hvor lokal lovgivning, der er gældende for dataimportøren, forbyder sletning eller tilbagelevering af de overførte personoplysninger, garanterer dataimportøren, at denne fortsat sikrer overholdelse af disse bestemmelser og kun behandler personoplysningerne i det omfang og i den periode, der er krævet i henhold til den lokale lovgivning.

(e) Hver part kan tilbagekalde sit samtykke til at være bundet af disse bestemmelser, hvis i) Europa-Kommissionen vedtager en afgørelse i henhold til artikel 45, stk. 3, i forordning (EU) 2016/679, som omfatter overførsel af personoplysninger, som disse bestemmelser finder anvendelse på, eller ii) forordning (EU) 2016/679 bliver en del af de retlige rammer i det land, hvortil personoplysningerne overføres. Dette berører ikke de øvrige forpligtelser, der gælder for den pågældende behandling, jf. forordning (EU) 2016/679.

Bestemmelse 17

Gældende lovgivning

Disse bestemmelser er underlagt lovgivningen i et land, der giver mulighed for påberåbelse af tredjemandsløftet. Parterne er enige om, at dette skal være lovgivningen som beskrevet i Hovedaftalen.

Bestemmelse 18

Valg af værneting og kompetent domstol

Tvister, der opstår i forbindelse med disse bestemmelser, afgøres af domstolene som beskrevet i Hovedaftalen.

TILLÆG

BILAG I

A. LISTE OVER PARTER

Dataeksportør(er): [*Identitet og kontaktoplysninger for dataeksportøren eller dataeksportørerne og, hvis det er relevant, for dataeksportørens eller dataeksportørernes databeskyttelsesrådgiver og/eller repræsentant i Den Europæiske Union]*

1. Navn: Glooko selskab som angivet i Hovedaftalen

Adresse: Som angivet i Hovedaftalen

Kontaktpersonens navn, stilling og kontaktoplysninger: Jesper Forster, datatilsynsmedarbejder. Glooko AB, Nellickevägen 20B412 63 Göteborg, Sverige. E-mail: dpo@glooko.com

Aktiviteter med relevans for de oplysninger, der overføres i henhold til disse bestemmelser: Levering af Leverancer som specificeret i Bestillingsformular.

Underskrift og dato: Som angivet i gældende Bestillingsformular i henhold til Hovedaftalen

Rolle (dataansvarlig/databehandler): Databehandler

2.

Dataimportør(er): [*Identitet og kontaktoplysninger for dataimportøren eller dataimportørerne, herunder eventuelle kontaktpersoner med ansvar for databeskyttelse]*

1. Navn: Klienten (som angivet i gældende Bestillingsformular)

Adresse: Klientadresse (som angivet i gældende Bestillingsformular)

Kontaktpersonens navn, stilling og kontaktoplysninger: Klientadresse (som angivet i gældende Bestillingsformular)

Aktiviteter med relevans for de oplysninger, der overføres i henhold til disse bestemmelser: Modtage Leverancerne som specificeret i Bestillingsformular.

Underskrift og dato: Som angivet i gældende Bestillingsformular i henhold til Hovedaftalen

Rolle (dataansvarlig/databehandler): Dataansvarlig

2.

B. BESKRIVELSE AF OVERFØRSLEN

Kategorier af registrerede personer for hvem personoplysninger overføres

- Autoriserede Brugere
- Patienter

Kategorier af personoplysninger, der overføres

- Autoriserede Brugere

- Patienter

Kategorier af personoplysninger, der behandles
For Autoriserede Brugere

- Generelle oplysninger (navn)
- Kontaktoplysninger (e-mailadresse, telefonnummer)
- Brugeroplysninger (brugernavn, adgangskode, adgangsrettigheder, auditlogning)

For Patienter

- Generelle oplysninger (navn, fødselsdato, køn)
- Kontaktoplysninger (postadresse, e-mailadresse, telefonnummer)
- Brugeroplysninger (brugernavn, adgangskode)
- Helbredsoplysninger (diabetes typer, årstal for diabetesdiagnoser, estimeret partus, målværdi, vægt, højde, behandlinger)
- Oplysninger om enhed (insulinpumpe, serienumre på glukosemåler og insulinen, doser, kulhydrater, indstillinger, alarmer)

Følsomme personoplysninger, der overføres (hvis relevant), og anvendte begrænsninger eller garantier, der fuldt ud tager hensyn til oplysningernes art og de involverede risici, f.eks. streng formålsbegrænsning, adgangsbegrænsninger (herunder kun adgang for særligt uddannet personale), registrering af adgangen til oplysningerne, begrænsninger for videreoverførsel eller yderligere sikkerhedsforanstaltninger.

- Helbredsoplysninger (diabetestype, år med diabetesdiagnoser, estimeret partus, målområde, vægt, højde, behandlinger)

Adgangsbegrænsninger for personale på et need-to-know grundlag (for både databehandleren og den dataansvarlige)
Registrering af adgang til dataene logføres
Data i transit og i hvile krypteres

Overførslens hyppighed (f.eks. om dataene overføres på engangsbasis eller løbende).

De personlige data gemmes af databehandleren, men kan tilgås af den dataansvarlige til enhver tid (hvis f.eks. hvis Leverancerne består af en software som en service). Personoplysninger kan i disse tilfælde betragtes som overført fra EØS til et tredjeland.

Behandlingens art

Overfør, beregn, analysér, visualisere, overføre og på anden måde behandle personoplysninger, så Autoriserede Brugere kan bruge Leverancerne.

Formål med dataoverførslen og den videre behandling

Formålet med dataoverførslen er at gøre det muligt for Klienten at bruge Leverancerne.

Den periode, hvor personoplysningerne opbevares eller, hvis det ikke kan oplyses, kriterier for fastsættelse af perioden

Behandlingen er ikke tidsbegrænset og skal udføres, så længe Leverancerne leveres, eller indtil den gældende databehandleraftale opsiges.

For overførsler til (under-)databehandlere angives også genstanden for behandlingen og behandlingens varighed og karakter

Ikke relevant.

C. KOMPETENT TILSYNSMYNDIGHED

Ikke relevant.

BILAG II — TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER, HERUNDER TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF DATASIKKERHEDEN

Ikke relevant.

BILAG III — LISTE OVER UNDERDATABEHANDLERE

Ikke relevant.