GLOOKO STANDARDAVTALSKLAUSULER

AVSNITT I

Klausul 1

Syfte och tillämpningsområde

(a) Syftet med dessa standardavtalsklausuler (klausulerna) är att säkerställa överensstämmelse med artikel 28.3 och 28.4 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

(b) De personuppgiftsansvariga och de personuppgiftsbiträden som anges i bilaga I har kommit överens om att tillämpa dessa klausuler för att säkerställa efterlevnaden av artikel 28.3 och 28.4 i förordning (EU) 2016/679 och/eller artikel 29.3 och 29.4 i förordning (EU) 2018/1725.

(c) Dessa klausuler är tillämpliga på behandling av personuppgifter i enlighet med bilaga II om de krav som anges i Huvudavtalet är uppfyllda.

(d) Bilagorna I–IV utgör en integrerad del av klausulerna.

(e) Dessa klausuler påverkar inte de skyldigheter som den personuppgiftsansvarige har enligt förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725.

(f) Genom dessa klausuler säkerställs inte i sig att skyldigheterna i samband med internationella överföringar i enlighet med kapitel V i förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725 fullgörs.

Klausul 2

Klausulernas oföränderlighet

(a) Parterna förbinder sig att inte ändra klausulerna, förutom för att lägga till information i bilagorna eller uppdatera informationen i dem.

(b) Detta hindrar inte parterna från att inkludera de standardavtalsklausuler som fastställs i dessa klausuler i ett mer omfattande avtal eller att lägga till andra klausuler eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt strider mot klausulerna eller begränsar de registrerades grundläggande rättigheter eller friheter.

Klausul 3

Tolkning

(a) Om de begrepp som definieras i förordning (EU) 2016/679 respektive förordning (EU) 2018/1725 används i dessa klausuler ska dessa begrepp ha samma betydelse som i den förordningen.

(b) Dessa klausuler ska läsas och tolkas mot bakgrund av bestämmelserna i förordning (EU) 2016/679 respektive förordning (EU) 2018/1725.

(c) Dessa klausuler ska inte tolkas så att de strider mot de rättigheter och skyldigheter som föreskrivs i förordning (EU) 2016/679 respektive förordning (EU) 2018/1725 eller påverkar de registrerades grundläggande rättigheter eller friheter.

Klausul 4

Hierarki

Om dessa klausuler strider mot bestämmelser i tillhörande avtal mellan parterna som gäller vid den tidpunkt då dessa klausuler avtalas eller ingås därefter, ska dessa klausuler ha företräde.

Klausul 5 - Frivillig

Dockningsklausul

(a) Varje enhet som inte är part i dessa klausuler får, med godkännande från samtliga parter, när som helst ansluta sig till dessa klausuler som personuppgiftsansvarig eller personuppgiftsbiträde genom att fylla i bilagorna och underteckna bilaga I.

(b) När de bilagor som avses i led a har fyllts i och undertecknats ska den anslutande enheten behandlas som part i dessa klausuler och ha de rättigheter och skyldigheter som gäller personuppgiftsansvariga eller personuppgiftsbiträden i överensstämmelse med dess intagande i bilaga I.

(c) Den anslutande enheten ska inte ha några rättigheter eller skyldigheter som följer av dessa klausuler innan den blir part.

AVSNITT II – PARTERNAS SKYLDIGHETER

Klausul 6

Beskrivning av behandlingen

Närmare uppgifter om behandlingen, särskilt kategorierna av personuppgifter och de ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning, anges i bilaga II.

Klausul 7

Parternas skyldigheter

7.1. Instruktioner

(a) Personuppgiftsbiträdet får endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida detta inte är förbjudet med hänvisning till ett viktigt allmänintresse enligt denna rätt. Den personuppgiftsansvarige får även ge efterföljande instruktioner under hela den tid som personuppgifterna behandlas. Dessa instruktioner ska alltid dokumenteras.

(b) Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om personuppgiftsbiträdet anser att en instruktion från den personuppgiftsansvarige strider mot förordning (EU) 2016/679 eller förordning (EU) 2018/1725 eller mot unionens eller medlemsstaternas tillämpliga dataskyddsbestämmelser.

7.2. Ändamålsbegränsning

Personuppgiftsbiträdet får behandla personuppgifterna endast för det eller de specifika ändamål med behandlingen, som anges i bilaga II, såvida det inte erhåller ytterligare instruktioner från den personuppgiftsansvarige.

7.3. Varaktigheten för behandlingen av personuppgifter.

Behandling som utförs av personuppgiftsbiträdet får endast äga rum under den tid som anges i bilaga II.

7.4. Säkerhet i samband med behandlingen

(a) Personuppgiftsbiträdet ska åtminstone genomföra de tekniska och organisatoriska åtgärder som anges i bilaga III för att säkerställa säkerheten för personuppgifterna. Detta omfattar att

skydda uppgifterna mot säkerhetsincidenter som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till uppgifterna (personuppgiftsincident). Vid bedömningen av lämplig säkerhetsnivå ska parterna ta vederbörlig hänsyn till den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerade.

(b) Personuppgiftsbiträdet ska bevilja sin personal tillgång till de personuppgifter som behandlas endast i den mån det är absolut nödvändigt för att genomföra, förvalta och övervaka avtalet. Personuppgiftsbiträdet ska säkerställa att personer med behörighet att behandla de erhållna personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

7.5. Känsliga uppgifter

Om behandlingen omfattar personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska uppgifter eller biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning eller uppgifter om fällande domar i brottmål och överträdelser (känsliga uppgifter), ska personuppgiftsbiträdet tillämpa särskilda begränsningar och/eller ytterligare skyddsåtgärder.

7.6 Dokumentation och efterlevnad

(a) Parterna ska kunna visa att dessa Klausuler följs.

(b) Personuppgiftsbiträdet ska skyndsamt och på lämpligt sätt hantera förfrågningar från den personuppgiftsansvarige om behandlingen av uppgifter i enlighet med dessa klausuler.

(c) Personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som behövs för att påvisa efterlevnad av de skyldigheter som fastställs i dessa klausuler och härrör direkt från förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725. På den personuppgiftsansvariges begäran ska personuppgiftsbiträdet även tillåta och bidra till granskningar av den behandling som omfattas av dessa klausuler, med rimliga intervall eller om det finns tecken på bristande efterlevnad. Vid beslut om översyn eller granskning får den personuppgiftsansvarige ta hänsyn till relevanta certifieringar som personuppgiftsbiträdet innehar.

(d) Den personuppgiftsansvarige kan välja att själv utföra granskningen eller bemyndiga en oberoende revisor. Granskningar får även omfatta inspektioner i personuppgiftsbiträdets lokaler eller fysiska anläggningar och ska vid behov utföras med rimligt varsel.

(e) Parterna ska på begäran göra den information som avses i denna klausul, inklusive resultaten av eventuella granskningar, tillgänglig för den (de) behöriga tillsynsmyndigheten(-erna).

7.7. Användning av underleverantörer

(a) Personuppgiftsbiträdet har erhållit ett allmänt tillstånd från den personuppgiftsansvarige att anlita underleverantörer från en överenskommen förteckning. Personuppgiftsbiträdet ska skriftligen informera den personuppgiftsansvarige om eventuella planerade ändringar av förteckningen genom att underleverantörer läggs till eller ersätts minst trettio (30) dagar i förväg, så att den personuppgiftsansvarige får tillräckligt med tid för att kunna invända mot sådana ändringar innan den eller de berörda underleverantörerna anlitas. Personuppgiftsbiträdet ska tillhandahålla den personuppgiftsansvarige den information som krävs för att denne ska kunna utöva sin rätt att göra invändningar.

(b) Om personuppgiftsbiträdet anlitar en underleverantör för att utföra en specifik behandling (för den personuppgiftsansvariges räkning) ska personuppgiftsbiträdet göra detta genom ett avtal som i sak ålägger underleverantören samma skyldigheter i fråga om uppgiftsskydd som de som personuppgiftsbiträdet åläggs i enlighet med dessa klausuler. Personuppgiftsbiträdet

ska se till att underleverantören uppfyller de skyldigheter som personuppgiftsbiträdet omfattas av enligt dessa klausuler och förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725.

(c) På den personuppgiftsansvariges begäran ska personuppgiftsbiträdet tillhandahålla den personuppgiftsansvarige en kopia av ett sådant underleverantörsavtal och eventuella senare ändringar. I den mån det är nödvändigt för att skydda affärshemligheter eller annan konfidentiell information, inbegripet personuppgifter, får personuppgiftsbiträdet redigera avtalstexten innan kopian delas.

(d) Personuppgiftsbiträdet ska fortsatt vara fullt ut ansvarig gentemot den personuppgiftsansvarige för att underleverantören fullgör sina skyldigheter i enlighet med sitt avtal med personuppgiftsbiträdet. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige om underleverantören underlåter att uppfylla sina skyldigheter enligt avtalet.

(e) Personuppgiftsbiträdet och underleverantören ska, om möjligt, avtala om en klausul om tredjepartsberättigande, enligt vilken den personuppgiftsansvarige – om personuppgiftsbiträdet har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd – ska ha rätt att säga upp underleverantörsavtalet och instruera underleverantören att radera eller återlämna personuppgifterna.

7.8. Internationella överföringar

(a) Personuppgiftsbiträdet får endast överföra uppgifter till ett tredjeland eller en internationell organisation på grundval av dokumenterade instruktioner från den personuppgiftsansvarige eller för att uppfylla ett särskilt krav enligt unionsrätten eller en medlemsstats lagstiftning som personuppgiftsbiträdet omfattas av, och överföringen ska genomföras i enlighet med kapitel V i förordning (EU) 2016/679 eller förordning (EU) 2018/1725.

(b) Den personuppgiftsansvarige samtycker till att, om personuppgiftsbiträdet anlitar en underleverantör i enlighet med klausul 7.7 för att utföra specifik behandling (för den personuppgiftsansvariges räkning) och denna behandling omfattar en överföring av personuppgifter i den mening som avses i kapitel V i förordning (EU) 2016/679, personuppgiftsbiträdet och underleverantören kan säkerställa att kapitel V i förordning (EU) 2016/679 efterlevs genom att använda standardavtalsklausuler som antagits av kommissionen i enlighet med artikel 46.2 i förordning (EU) 2016/679, förutsatt att villkoren för att använda dessa standardavtalsklausuler är uppfyllda.

Klausul 8

Stöd till den personuppgiftsansvarige

(a) Personuppgiftsbiträdet ska hänvisa registrerade till att kontakta den personuppgiftsansvarige, om personuppgiftsbiträde får en begäran avseende en registrerad person. Personuppgiftsbiträdet ska inte själv besvara begäran, såvida inte den personuppgiftsansvarige har godkänt detta.

(b) Personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige att fullgöra sin skyldighet att besvara framställningar från registrerade för att utöva sina rättigheter, med hänsyn till behandlingens art. Personuppgiftsbiträdet ska följa den personuppgiftsansvariges instruktioner när det fullgör sina skyldigheter i enlighet med leden a och b.

(c) Utöver personuppgiftsbiträdets skyldighet att bistå den personuppgiftsansvarige enligt klausul 8 b ska personuppgiftsbiträdet dessutom bistå den personuppgiftsansvarige med att säkerställa att följande skyldigheter fullgörs, med beaktande av uppgiftsbehandlingens art och den information som personuppgiftsbiträdet har att tillgå:

(1) Skyldigheten att utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (en konsekvensbedömning avseende dataskydd) om en

typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

(2) Skyldigheten att samråda med den (de) behöriga tillsynsmyndigheten(-erna) före behandling om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.

(3) Skyldigheten att säkerställa att personuppgifterna är korrekta och uppdaterade genom att utan dröjsmål informera den personuppgiftsansvarige om personuppgiftsbiträdet får kännedom om att de personuppgifter som behandlas är felaktiga eller har blivit föråldrade.

(4) Skyldigheterna i artikel 32 i förordning (EU) 2016/679.

(d) Parterna ska i bilaga III ange de lämpliga tekniska och organisatoriska åtgärder genom vilka personuppgiftsbiträdet ska bistå den personuppgiftsansvarige vid tillämpningen av denna klausul samt räckvidden och omfattningen av det bistånd som krävs.

Klausul 9

Anmälan av personuppgiftsincidenter

Vid en personuppgiftsincident ska personuppgiftsbiträdet samarbeta med och bistå den personuppgiftsansvarige för att denne ska kunna fullgöra sina skyldigheter enligt artiklarna 33 och 34 i förordning (EU) 2016/679 eller artiklarna 34 och 35 i förordning (EU) 2018/1725, i tillämpliga fall, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

9.1 Personuppgiftsincidenter som rör uppgifter som behandlas av den personuppgiftsansvarige

I händelse av en personuppgiftsincident som rör uppgifter som behandlas av den personuppgiftsansvarige ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att:

(a) anmäla personuppgiftsincidenten till den (de) behöriga tillsynsmyndigheten(-erna), utan onödigt dröjsmål efter det att den personuppgiftsansvarige har fått kännedom om den, i förekommande fall/(med undantag för om det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter),

(b) erhålla följande information som, i enlighet med artikel 33.3 i förordning (EU) 2016/679/, ska anges i den personuppgiftsansvariges anmälan, och åtminstone ska omfatta:

(1) personuppgifternas art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

(2) de sannolika konsekvenserna av personuppgiftsincidenten,

(3) de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om och i den mån det inte är möjligt att tillhandahålla all denna information samtidigt ska den ursprungliga anmälan innehålla den information som finns tillgänglig, och ytterligare information ska därefter, i den mån den blir tillgänglig, tillhandahållas utan onödigt dröjsmål.

(c) uppfylla, i enlighet med artikel 34 i förordning (EU) 2016/679 skyldigheten att utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten, om den sannolikt kommer att medföra en hög risk för fysiska personers rättigheter och friheter.

9.2 Personuppgiftsincident som rör uppgifter som behandlas av personuppgiftsbiträdet

I händelse av en personuppgiftsincident som rör uppgifter som behandlas av personuppgiftsbiträdet ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter det att personuppgiftsbiträdet har fått kännedom om incidenten. En sådan anmälan ska åtminstone innehålla:

(a) en beskrivning av incidentens art (inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade och uppgiftsposter som berörs),

(b) uppgifter från en kontaktpunkt där mer information om personuppgiftsincidenten kan erhållas,

(c) de sannolika konsekvenserna och de åtgärder som vidtagits eller föreslagits för att åtgärda incidenten, inbegripet åtgärder för att mildra dess potentiella negativa effekter.

Om och i den mån det inte är möjligt att tillhandahålla all denna information samtidigt ska den ursprungliga anmälan innehålla den information som finns tillgänglig, och ytterligare information ska därefter, i den mån den blir tillgänglig, tillhandahållas utan onödigt dröjsmål.

Parterna ska i bilaga III ange alla andra uppgifter som personuppgiftsbiträdet ska tillhandahålla när denne bistår den personuppgiftsansvarige vid fullgörandet av den personuppgiftsansvariges skyldigheter enligt artiklarna 33 och 34 i förordning (EU) 2016/679.

AVSNITT III – SLUTBESTÄMMELSER

Klausul 10

Bristande efterlevnad av klausulerna och uppsägning

(a) Utan att det påverkar tillämpningen av bestämmelserna i förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725 får den personuppgiftsansvarige, om personuppgiftsbiträdet inte fullgör sina skyldigheter enligt dessa klausuler, instruera personuppgiftsbiträdet att avbryta behandlingen av personuppgifter till dess att denne uppfyller dessa klausuler eller Huvudavtalet sägs upp. Personuppgiftsbiträdet ska omedelbart underrätta den personuppgiftsansvarige om denne av något skäl inte kan följa dessa klausuler.

(b) Den personuppgiftsansvarige ska ha rätt att säga upp Huvudavtalet i den mån det avser behandling av personuppgifter i enlighet med dessa klausuler om:

(1) personuppgiftsbiträdets behandling av personuppgifter har avbrutits av den personuppgiftsansvarige i enlighet med led a och om efterlevnaden av dessa klausuler inte återställs inom rimlig tid och i alla händelser inom en månad efter det att behandlingen avbrutits;

(2) personuppgiftsbiträdet allvarligt eller ihållande åsidosätter dessa klausuler eller sina skyldigheter enligt förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725;

(3) personuppgiftsbiträdet underlåter att följa ett bindande beslut från en behörig domstol eller den (de) behöriga tillsynsmyndigheten(-erna) som rör dennes skyldigheter i enlighet med dessa klausuler eller förordning (EU) 2016/679 och/eller förordning (EU) 2018/1725.

(c) Personuppgiftsbiträdet ska ha rätt att säga upp Huvudavtalet i den mån det avser behandling av personuppgifter enligt dessa klausuler, om den personuppgiftsansvarige, efter att ha informerats av personuppgiftsbiträdet om att dennes instruktioner strider mot tillämpliga rättsliga krav i enlighet med klausul 7.1 b, insisterar på att instruktionerna följs.

(d) Efter uppsägningen av Huvudavtalet ska personuppgiftsbiträdet, beroende på vad den personuppgiftsansvarige väljer, radera alla personuppgifter som behandlats för den personuppgiftsansvariges räkning och intyga för den personuppgiftsansvarige att detta är utfört, eller återlämna alla personuppgifter till den personuppgiftsansvarige och radera befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt. Om den personuppgiftsansvarige inte har begärt att få alla personuppgifter som behandlas för den personuppgiftsansvariges räkning återlämnade inom trettio (30) dagar från det att Huvudavtalet upphört, ska personuppgiftsbiträdet ha rätt att, efter eget gottfinnande, radera personuppgifterna. Till dess att uppgifterna raderas eller återlämnas ska personuppgiftsbiträdet säkerställa efterlevnaden av dessa klausuler.

BILAGA I: FÖRTECKNING ÖVER PARTER

Personuppgiftsansvarig (a):

1. Klient (såsom angivits i Huvudavtalet eller Beställningsformuläret)

Personuppgiftsbiträde (n):

1. Glooko AB (såsom angivits i Huvudavtalet)

BILAGA II: BESKRIVNING AV BEHANDLINGEN

Kategorier av registrerade vars personuppgifter behandlas
- Auktoriserade Användare
- Patienter

Kategorier av personuppgifter
För Auktoriserade Användare
- Allmän information (namn)
- Kontaktinformation (emailadress, telefonnummer)
- Användarinformation (användarnamn, lösenord, åtkomsträttigheter, ändringsloggar)

För Patienter
- Allmän information (namn, födelsedatum kön)
- Kontaktinformation (postadress, emailadress, telefonnummer)
- Användarinformation (användarnamn, lösenord)
- Hälsoinformation (diabetstyp, år för diabetesdiagnos, beräknat förlossningsdatum, målintervall, vikt, längd, behandling)
- Enhetsinformation (insulinpump, glukosmätare och insulinpennas serienummer, doser, kolhydrater, inställningar, larm)

Känsliga uppgifter som behandlas (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder som fullt ut tar hänsyn till uppgifternas art och de risker som är förknippade med dem, t.ex. strikt ändamålsbegränsning, åtkomstbegränsningar (inbegripet åtkomst endast för personal som har gått en specialiserad utbildning), registrering av åtkomst till uppgifterna, begränsningar för vidareöverföring eller ytterligare säkerhetsåtgärder.

- Uppgifter om hälsa

För information gällande tillämpade skyddsåtgärder, se bilaga III

Behandlingens art

Samla in, analysera, visualisera och på annat sätt behandla personuppgifterna i enlighet med Huvudavtalet.

Ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning

För att möjliggöra för personuppgiftsbiträdet och dess Auktoriserade Användare att använda Programvaran och andra Produkter i enlighet med Huvudavtalet.

Behandlingens varaktighet

Under den period Programvaran och andra Produkter tillhandahålls enligt Huvudavtalet.

För behandling som utförs av personuppgiftsbiträden (eller underleverantörer), ange även föremålet för behandlingen, behandlingens art och dess varaktighet.

Se bilaga IV

Anvisningar under avsnitt 7.8 a) i klausulerna om internationella överföringar
Standardavtalsklausulerna för internationella överföringar (”**SCCs**”) i bilaga V gäller om personuppgiftsbiträdet överför personuppgifter utanför EES, till ett land som inte erkänts av Europeiska kommissionen som tillhandahållande en adekvat skyddsnivå för personuppgifter.

BILAGA III: TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INBEGRIPET TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA DATASÄKERHETEN

1. Syfte. Denna bilaga beskriver Glookos säkerhetsprogram, säkerhetscertifieringar och tekniska och organisatoriska åtgärder för att skydda (a) personuppgifter som behandlas av personuppgiftsbiträdet på uppdrag av den personuppgiftsansvarig från obehörig användning, åtkomst, utlämnande eller stöld och (b) Programvaran. När säkerhetshoten förändras och utvecklas fortsätter Glooko att uppdatera sitt säkerhetsprogram och sin strategi för att skydda personuppgifter och Programvaran. I detta syfte förbehåller sig Glooko rätten att uppdatera denna bilaga från tid till annan; förutsatt att en uppdatering inte väsentligt minskar de övergripande skydden som anges i denna bilaga.

   2. Säkerhetsorganisation och -program. Glooko har ett riskbaserat säkerhetsbedömningsprogram. Glookos säkerhetsprogram inkluderar administrativa, organisatoriska, tekniska och fysiska säkerhetsåtgärder som är skäligen utformade för att skydda Programvaran och konfidentialitet, integritet och tillgänglighet för personuppgifter. Glookos säkerhetsprogram är avsett att vara lämpligt för Programvarans karaktär och storleken och komplexiteten hos Glookos affärsverksamhet. Glooko har ett separat och dedikerat informationssäkerhetsteam som hanterar Glookos säkerhetsprogram. Detta team underlättar och stödjer oberoende revisioner och bedömningar som utförs av tredje part. Glookos säkerhetssystem inkluderar program som täcker: Policyer och processer, Förvaltning av tillgångar, Åtkomsthantering, Kryptografi, Fysisk säkerhet, Driftsäkerhet, Kommunikationssäkerhet, Kontinuitetsskydd, Interna säkerhetsåtgärder avseende företagets medarbetare Security, Produktsäkerhet, Moln- och nätverksinfrastruktursäkerhet, Uppfyllande av säkerhetskrav, Tredjepartssäkerhet, Sårbarhetshantering och Säkerhetsövervakning och Incidenthantering. Säkerhet hanteras på företagets högsta nivå, med Glookos säkerhetsansvarige som har regelbundna möten med ledningen för att diskutera frågor och koordinera företagsomfattande säkerhetsinitiativ. Informationssäkerhetspolicyer och -standarder granskas och godkänns av ledningen åtminstone årligen och görs tillgängliga för alla Glooko-anställda.

3. Sekretess. Glooko har kontroller på plats för att upprätthålla sekretessen för personuppgifter i enlighet med Huvudavtalet. Alla Glookos anställda och kontraktsanställda är bundna av Glookos interna policyer när det gäller att upprätthålla sekretess för personuppgifter och är skyldiga enligt avtal att efterleva dessa skyldigheter.

4. Interna säkerhetsåtgärder avseende företagets medarbetare

   a. Bakgrundskontroller av anställda. Glooko utför bakgrundskontroller av alla nyanställda vid anställningstillfället i enlighet med gällande lokala lagar. Glooko verifierar för närvarande en nyanställds utbildning och tidigare anställning och utför referenskontroller. Där det är tillåtet enligt tillämplig lag kan Glooko också komma att utföra brotts-, kredit-, immigrations- och säkerhetskontroller beroende på arten och omfattningen av en ny anställds roll.

   b. Utbildning för anställda. Minst en gång (1) om året måste alla Glooko-anställda genomgå en säkerhets- och sekretessutbildning som täcker Glookos säkerhetspolicyer, bästa säkerhetspraxis och sekretessprinciper. Anställda som är tjänstlediga kan få ytterligare tid att genomföra denna årliga utbildning. Glookos särskilda säkerhetsteam genomför också kampanjer för medvetenhet om nätfiske och kommunicerar nya hot till anställda.

5. Hantering av tredjeparts-leverantörer

   a. Leverantörsbedömning. Glooko kan komma att använda tredjepartsleverantörer för att tillhandahålla Programvaran. Glooko utför en säkerhetsriskbaserad

bedömning av potentiella leverantörer innan man arbetar med dem för att bekräfta att de uppfyller Glookos säkerhetskrav. Glooko granskar med jämna mellanrum alla leverantörer baserat på Glookos säkerhets- och affärskontinuitetsstandarder, inklusive typen av åtkomst och klassificering av data som ges åtkomst till (om någon), kontroller som är nödvändiga för att skydda data och juridiska/regulatoriska krav. Glooko säkerställer att personuppgifter returneras och/eller raderas när en leverantörsrelation avslutas.

b. Leverantörsavtal. Glooko ingår skriftliga avtal med alla sina leverantörer som inkluderar sekretess-, integritets- och säkerhetsskyldigheter som ger lämplig nivå av skydd för personuppgifter som dessa leverantörer kan komma att behandla.

6. Arkitektur, brandväggar och datasegregation. All nätverksåtkomst mellan produktionsvärdar är begränsad med hjälp av brandväggar så att endast auktoriserade tjänster kan interagera i produktionsnätverket. Brandväggar används för att hantera nätverkssegregation mellan olika säkerhetszoner i produktions- och bolagsmiljö. Glooko separerar logiskt sina databaser. Glooko API:erna är designade och byggda för att identifiera och tillåta åtkomst endast till och från respektive avsändare. Dessa kontroller hindrar kunder från att få tillgång till andra kunders data.

7. Fysisk säkerhet. Datacentren som är värd för Programvaran kontrolleras strikt, både runt byggnader och vid ingångar, av professionell säkerhetspersonal som använder videoövervakning, system för intrångsdetektering och andra elektroniska medel. Avbrottsfri elförsörjning och generatorer på plats finns tillgängliga för att ge reservkraft i händelse av elavbrott. Dessutom har Glookos huvudkontor och kontorsutrymmen ett fysiskt säkerhetsprogram som hanterar besökare, ingångar och övergripande kontorssäkerhet.

8. "Security by Design." Glooko följer "security by design"-principer när man designar Programvaran. Glooko tillämpar också standarden Glooko Software Development Lifecycle (SDLC) för att utföra många säkerhetsrelaterade aktiviteter för Programvaran under olika faser av produktskapandets från kravinsamling och produktdesign hela vägen genom produktdistributionen.

9. Access Controls

    a. Tillhandahållande av åtkomst. För att minimera risken för dataexponering följer Glooko principerna om lägsta behörighet genom en teambaserad åtkomstkontrollmodell vid tillhandahållande av systemåtkomst. Glookos personal har behörighet att komma åt personuppgifter baserat på deras arbetsfunktion, roll och ansvar, och sådan åtkomst kräver godkännande av den anställdes chef. En anställds tillgång till personuppgifter försvinner när anställningen upphör. Innan en ingenjör beviljas åtkomst till produktionsmiljön måste åtkomst godkännas av ledningen och ingenjören måste genomföra interna utbildningar för sådan åtkomst inklusive utbildningar i det relevanta teamets system. Glooko loggar högriskåtgärder och förändringar i produktionsmiljön. Glooko utnyttjar automatisering för att identifiera eventuella avvikelser från interna tekniska standarder som kan indikera onormal/otillåten aktivitet för att larma inom några minuter efter en konfigurationsändring.

    b. Lösenordskontroll. När en Auktoriserad Användare loggar in på sitt konto hashar Glooko användarens autentiseringsuppgifter innan de lagras. Kunder kan också kräva att deras Auktoriserade Användare lägger till ytterligare säkerhet till sitt konto genom att använda tvåfaktorsautentisering (2FA).

10. Ändringshantering. Glooko har en formell process för att hantera ändringar som man följer för att administrera ändringar i produktionsmiljön för Programvaran, inklusive alla ändringar av underliggande programvara, applikationer och system. Varje ändring granskas noggrant och utvärderas i en testmiljö innan den distribueras i produktionsmiljön för

Programvaran. Alla ändringar, inklusive utvärderingen av ändringarna i en testmiljö, dokumenteras med hjälp av ett formellt, granskningsbart, registersystem. Implementeringsgodkännande för högriskändringar krävs från rätt organisatoriska intressenter. Planer och procedurer implementeras också i händelse av att en implementerad ändring måste återställas för att bevara Programvarans säkerhet.

11. Kryptering. För Programvaran är (a) databaserna som lagrar personuppgifter krypterade med Advanced Encryption Standard och (b) personuppgifter krypteras när de överförs mellan Klientens program och Programvaran med TLS v1.2

12. Sårbarhetshantering. Glooko har kontroller och policyer för att minska risken för säkerhetssårbarhet för att balansera risk och affärs-/operativa krav. Glooko använder ett tredjepartsverktyg för att utföra sårbarhetsskanningar regelbundet för att bedöma sårbarheter i Glookos molninfrastruktur och bolagsgemensamma system.

13. Penetrationstestning. Glooko utför penetrationstester och engagerar oberoende tredjepartsföretag för att utföra penetrationstester på applikationsnivå. Säkerhetshot och sårbarheter som upptäcks bedöms, prioriteras och åtgärdas.

14. Hantering av säkerhetsincidenter. Glooko har policyer för hantering av säkerhetsincidenter. Glookos Security Incident Response Team (T-SIRT) bedömer alla relevanta säkerhetshot och sårbarheter och upprättar lämpliga åtgärder för avhjälpande och begränsning. Glooko lagrar relevanta säkerhetsloggar.

15. Resiliens och programvarukontinuitet. Programvaran använder en mängd olika verktyg och mekanismer för att uppnå hög tillgänglighet och resiliens. För Programvaran spänner Glookos infrastruktur över flera feloberoende tillgänglighetszoner i geografiska områden som är fysiskt åtskilda från varandra. Glooko använder också specialiserade verktyg som övervakar serverprestanda, data och trafikbelastningskapacitet inom varje tillgänglighetszon och samlokaliseringsdatacenter. Om suboptimal serverprestanda eller överbelastad kapacitet upptäcks på en server inom en tillgänglighetszon eller samlokaliseringsdatacenter, ökar dessa specialiserade verktyg kapaciteten eller flyttar trafik för att lindra eventuell suboptimal serverprestanda eller kapacitetsöverbelastning. Glooko underrättas även omedelbart i händelse av suboptimal serverprestanda eller överbelastad kapacitet.

16. Säkerhetskopiering och återställning. Glooko gör regelbundna säkerhetskopior av personuppgifter. Personuppgifter som säkerhetskopieras bevaras redundant över flera tillgänglighetszoner och krypteras under överföring och lagring med hjälp av Advanced Encryption Standards.

BILAGA IV: FÖRTECKNING ÖVER UNDERLEVERANTÖRER

Den personuppgiftsansvarige har godkänt användning av följande underleverantörer:

1. Namn: Amazon Web Services EMEA SARL
Adress: 38 Avenue John F. Kennedy, L-1855, Luxemburg

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts): Molntjänstleverantör

2. Namn: Cegedim SA
Adress: 137 rue d'Aguesseau, 92100 Boulogne-Billancourt, Frankrike

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts): Molntjänstleverantör (kan användas för Klienter i Frankrike)

3. Namn: Pictime Groupe
Adress: Campus du Digital 61, rue de l'Harmonie - 59262 Sainghin-en-Mélantois, Frankrike

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts): Certifierad Health Data Host (kan användas för klienter i Frankrike och Tyskland)

BILAGA V: Standardavtalsklausuler för internationella överföringar ("SCC")

Klausul 1

Syfte och tillämpningsområde

(a) Syftet med dessa standardavtalsklausuler är att säkerställa överensstämmelse med kraven i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning) [1] vid överföring av personuppgifter till ett tredjeland.

(b) Parterna:

(i) den eller de fysiska eller juridiska personer, den eller de offentliga myndigheter, den eller de byråer eller andra organ (enheterna) som överför personuppgifter enligt förteckningen i bilaga I.A. (*uppgiftsutföraren*), och

(ii) den eller de enheter i ett tredjeland som tar emot personuppgifter från uppgiftsutföraren, direkt eller indirekt via en annan enhet som också är part i dessa klausuler, enligt förteckningen i bilaga I.A. (*uppgiftsinföraren*)

har kommit överens om dessa standardavtalsklausuler (*klausulerna*).

(c) Dessa klausuler är tillämpliga med avseende på överföring av personuppgifter enligt vad som anges i bilaga I.B.

(d) Det tillägg till dessa klausuler som innehåller de bilagor som det hänvisas till utgör en integrerad del av dessa klausuler.

Klausul 2

Klausulernas verkan och beständighet

(a) Genom dessa klausuler fastställs lämpliga skyddsåtgärder, däribland verkställbara rättigheter och effektiva rättsmedel för de registrerade enligt artikel 46.1 och artikel 46.2 c i förordning (EU) 2016/679 och, när det gäller överföring av personuppgifter från personuppgiftsansvariga till personuppgiftsbiträden och/eller från personuppgiftsbiträden till personuppgiftsbiträden, standardavtalsklausuler enligt artikel 28.7 i förordning (EU) 2016/679, under förutsättning att de inte ändras, förutom för att välja en eller flera lämpliga moduler eller lägga till eller uppdatera informationen i tillägget. Detta hindrar inte parterna från att inbegripa de standardavtalsklausuler som fastställs i dessa klausuler i ett mer övergripande avtal och/eller att lägga till andra klausuler eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med dessa klausuler eller påverkar de registrerades grundläggande rättigheter eller friheter.

---

[1] Om uppgiftsutföraren är ett personuppgiftsbiträde som omfattas av förordning (EU) 2016/679 och som agerar på uppdrag av en unionsinstitution eller ett unionsorgan som personuppgiftsansvarig, säkerställer användningen av dessa klausuler vid anlitande av ett annat personuppgiftsbiträde (som underentreprenörer) som inte omfattas av förordning (EU) 2016/679 även överensstämmelse med artikel 29.4 i Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39), i den utsträckning som dessa klausuler och de skyldigheter i fråga om uppgiftsskydd som fastställs i avtalet eller en annan rättsakt mellan den personuppgiftsansvarige och personuppgiftsbiträdet i enlighet med artikel 29.3 i förordning (EU) 2018/1725 har samordnats. Detta kommer särskilt att vara fallet om den personuppgiftsansvarige och personuppgiftsbiträdet använder de standardavtalsklausuler som ingår i beslut 2021/915.

(b) Dessa klausuler påverkar inte de skyldigheter som uppgiftsutföraren omfattas av med stöd av förordning (EU) 2016/679.

Klausul 3

Berättigade tredje parter

(a) Registrerade personer får åberopa och verkställa dessa klausuler, i egenskap av berättigade tredje parter, gentemot uppgiftsutföraren och/eller uppgiftsinföraren, med följande undantag:

(i) Klausul 1, klausul 2, klausul 3, klausul 6, klausul 7.

(ii) Klausul 8 – modul ett: klausul 8.5 e och klausul 8.9 b; modul två: klausul 8.1 b, 8.9 a, c, d och e; modul tre: klausul 8.1 a, c och d och klausul 8.9 a, c, d, e, f och g; modul fyra: klausul 8.1 b och klausul 8.3 b.

(iii) Klausul 9 – modul två: klausul 9 a, c, d och e; modul tre: klausul 9 a, c, d och e.

(iv) Klausul 12 – modul ett: klausul 12 a och d; modulerna två och tre: klausul 12 a, d och f.

(v) Klausul 13.

(vi) Klausul 15.1 c, d och e.

(vii) Klausul 16 e.

(viii) Klausul 18 – modulerna ett, två och tre: klausul 18 a och b; modul fyra: klausul 18.

(b) Led a påverkar inte de registrerades rättigheter enligt förordning (EU) 2016/679.

Klausul 4

Tolkning

(a) Om begrepp som definieras i förordning (EU) 2016/679 används i dessa klausuler ska begreppen ha samma betydelse som i den förordningen.

(b) Dessa klausuler ska läsas och tolkas mot bakgrund av bestämmelserna i förordning (EU) 2016/679.

(c) Dessa klausuler ska inte tolkas på ett sätt som står i strid med de rättigheter och skyldigheter som föreskrivs i förordning (EU) 2016/679.

Klausul 5

Hierarki

Om en konflikt uppstår mellan dessa klausuler och bestämmelserna i de överenskommelser mellan parterna som gäller vid den tidpunkt då dessa klausuler överenskoms eller därefter träder i kraft, ska dessa klausuler ha företräde.

Klausul 6

Beskrivning av överföringen eller överföringarna

Närmare uppgifter om överföringen eller överföringarna, och i synnerhet de kategorier av personuppgifter som överförs och det eller de ändamål för vilka de överförs, anges i bilaga I.B.

Klausul 7 – Valfri

Dockningsklausul

Inte tillämpligt

AVSNITT II – PARTERNAS SKYLDIGHETER

Klausul 8

Skyddsåtgärder för uppgifter

Uppgiftsutföraren garanterar att han eller hon har gjort rimliga ansträngningar för att se till att uppgiftsinföraren, genom genomförandet av lämpliga tekniska och organisatoriska åtgärder, kan fullgöra sina skyldigheter enligt dessa klausuler.

8.1 Instruktioner

(a) Uppgiftsutföraren ska endast behandla personuppgifterna enligt dokumenterade instruktioner från den uppgiftsinförare som agerar som dess personuppgiftsansvarige.

(b) Uppgiftsutföraren ska omedelbart informera uppgiftsinföraren om han eller hon inte kan följa dessa instruktioner, däribland om instruktionerna bryter mot förordning (EU) 2016/679 eller någon annan dataskyddslagstiftning i unionen eller medlemsstaterna.

(c) Uppgiftsinföraren ska avstå från varje åtgärd som skulle hindra uppgiftsutföraren från att fullgöra sina skyldigheter enligt förordning (EU) 2016/679, däribland vid anlitande av en underentreprenör eller när det gäller samarbete med de behöriga tillsynsmyndigheterna.

(d) När tillhandahållandet av behandlingstjänsterna har avslutats ska uppgiftsutföraren, enligt uppgiftsinförarens val, radera alla personuppgifter som behandlats på uppdrag av uppgiftsinföraren och intyga för uppgiftsinföraren att detta har skett, eller till uppgiftsinföraren återlämna alla personuppgifter som har behandlats på uppdrag av uppgiftsinföraren och radera befintliga kopior.

8.2 Säkerhet vid behandling

(a) Parterna ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa uppgifternas säkerhet, även under överföring, däribland genom skydd mot säkerhetsbrott som skulle leda till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande eller obehörig åtkomst (personuppgiftsincident). Vid bedömning av lämplig säkerhetsnivå ska de ta vederbörlig hänsyn till de senaste rönen, kostnaderna för genomförandet, personuppgifternas karaktär[2], behandlingens karaktär, omfattning, sammanhang och ändamål samt riskerna för de registrerade i samband med

[2] Detta omfattar huruvida överföringen och den efterföljande behandlingen inbegriper personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter för unik identifiering av en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning, eller uppgifter om brottmålsdomar eller lagöverträdelser.

behandlingen, och särskilt överväga att använda kryptering eller pseudonymisering, även under överföringen, om ändamålet med behandlingen kan uppfyllas på detta sätt.

(b) Uppgiftsutföraren ska bistå uppgiftsinföraren med att säkerställa en lämplig säkerhetsnivå för uppgifterna i enlighet med led a. I händelse av en personuppgiftsincident som gäller personuppgifter som har behandlats av uppgiftsutföraren enligt dessa klausuler ska uppgiftsutföraren utan onödigt dröjsmål meddela uppgiftsinföraren efter att ha fått kännedom om incidenten och bistå uppgiftsinföraren i hanteringen av densamma.

(c) Uppgiftsutföraren ska säkerställa att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

8.3 Dokumentation och efterlevnad

(a) Parterna ska kunna visa att de uppfyller kraven i dessa klausuler.

(b) Uppgiftsutföraren ska se till att uppgiftsinföraren får tillgång till all information som behövs för att visa att skyldigheterna enligt dessa klausuler har fullgjorts och för att möjliggöra och bidra till revisioner.

Klausul 9

Användning av underentreprenörer

Inte tillämpligt

Klausul 10

De registrerades rättigheter

Parterna ska bistå varandra med att svara på förfrågningar och begäranden från registrerade enligt den lokala lagstiftning som är tillämplig på uppgiftsinföraren eller, vid databehandling av uppgiftsutföraren inom EU, enligt förordning (EU) 2016/679.

Klausul 11

Tillgång till prövning

(a) Uppgiftsinföraren ska informera de registrerade i ett öppet och lättillgängligt format, genom enskilda meddelanden eller på sin webbplats, om en kontaktpunkt som har tillstånd att hantera klagomål. Uppgiftsinföraren ska skyndsamt hantera varje klagomål som tas emot från en registrerad.

Klausul 12

Ansvarsskyldighet

(a) Varje part ska vara ansvarig inför den andra parten eller de andra parterna för eventuella skador den orsakar den andra parten eller de andra parterna genom överträdelse av dessa klausuler.

(b) Varje part ska vara ansvarig inför den registrerade, och den registrerade ska ha rätt till ersättning, för varje materiell eller immateriell skada som parten orsakar den registrerade genom att kränka

rättigheterna för en berättigad tredje part enligt dessa klausuler. Detta påverkar inte uppgiftsutförarens ansvarsskyldighet enligt förordning (EU) 2016/679.

(c) Om fler än en part är ansvariga för eventuell skada som orsakats den registrerade till följd av en överträdelse av dessa klausuler ska alla ansvarsskyldiga parter vara solidariskt ansvariga, och den registrerade ska ha rätt att väcka talan i domstol mot var och en av dessa parter.

(d) Parterna är överens om att en part som hålls ansvarig enligt led c ska ha rätt att återkräva från den andra parten eller de andra parterna den del av ersättningen som motsvarar dess/deras ansvarsskyldighet för skadan.

(e) Uppgiftsinföraren får inte åberopa ett personuppgiftsbiträdes eller en underentreprenörs uppförande för att undvika sitt eget ansvar.

Klausul 13

Tillsyn

Inte tillämpligt

AVSNITT III – LOKALA LAGAR OCH SKYLDIGHETER VID ÅTKOMST AV OFFENTLIGA MYNDIGHETER

Klausul 14

Lokala lagar och förfaranden som påverkar efterlevnaden av klausulerna

Inte tillämpligt

Klausul 15

Uppgiftsinförarens skyldigheter vid åtkomst av offentliga myndigheter

Inte tillämpligt

AVSNITT IV – SLUTBESTÄMMELSER

Klausul 16

Bristande efterlevnad av klausulerna och avtalets uppsägning

(a) Uppgiftsinföraren ska skyndsamt informera uppgiftsutföraren om han eller hon inte kan uppfylla kraven i dessa klausuler, oavsett orsak.

(b) Om uppgiftsinföraren bryter mot dessa klausuler eller inte kan uppfylla kraven i dessa klausuler ska uppgiftsutföraren avbryta överföringen av personuppgifter till uppgiftsinföraren tills efterlevnaden åter har säkerställts eller avtalet har sagts upp. Detta påverkar inte tillämpningen av klausul 14 f.

(c) Uppgiftsutföraren ska ha rätt att säga upp avtalet i den mån det gäller behandlingen av personuppgifter enligt dessa klausuler om:

(i) uppgiftsutföraren har avbrutit överföringen av personuppgifter till uppgiftsinföraren enligt led b och om efterlevnaden av dessa klausuler inte har återupprättats inom en rimlig tidsperiod, under alla omständigheter inom en månad efter avbrytandet,

(ii) uppgiftsinföraren gör sig skyldig till allvarliga eller upprepade överträdelser av dessa klausuler, eller

(iii) uppgiftsinföraren inte följer ett bindande beslut av en behörig domstol eller tillsynsmyndighet angående hans eller hennes skyldigheter enligt dessa klausuler.

I sådana fall ska uppgiftsutföraren informera den behöriga tillsynsmyndigheten om denna bristande efterlevnad. Om avtalet omfattar fler än två parter får uppgiftsutföraren utöva denna rätt att säga upp avtalet med endast den berörda parten, såvida inte parterna har kommit överens om annat.

(d) Personuppgifter som samlats in av uppgiftsutföraren i EU och som överförts före uppsägningen av avtalet enligt led c ska omedelbart raderas i sin helhet, inklusive eventuella kopior. Uppgiftsinföraren ska intyga för uppgiftsutföraren att uppgifterna har raderats. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsinföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av de överförda personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsinföraren ska uppgiftsinföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen.

(e) Endera parten får återkalla sin överenskommelse om att vara bunden av dessa klausuler om i) Europeiska kommissionen antar ett beslut i enlighet med artikel 45.3 i förordning (EU) 2016/679 som omfattar den överföring av personuppgifter som dessa klausuler gäller för, eller ii) förordning (EU) 2016/679 blir en del av den rättsliga ramen i det land till vilket personuppgifterna överförs. Detta påverkar inte övriga skyldigheter som är tillämpliga på behandlingen i fråga enligt förordning (EU) 2016/679.

Klausul 17

Tillämplig lag

Dessa klausuler ska regleras genom lagstiftningen i ett land som omfattar rättigheter för berättigade tredje parter. Parterna är överens om att detta ska vara lagstiftningen som anges i Huvudavtalet.

Klausul 18

Val av forum och jurisdiktion

Varje tvist som uppstår på grund av dessa klausuler ska lösas av domstolarna i det land som ange i Huvudavtalet.

BILAGA

BILAGA I

A. FÖRTECKNING ÖVER PARTER

Uppgiftsutförare: [*Uppgiftsutförarens/uppgiftsutförarnas identitet och kontaktuppgifter och, i tillämpliga fall, uppgifter om hans/hennes eller deras dataskyddsombud och/eller företrädare i Europeiska unionen]*

1. Namn: Den Glooko-enhet som anges i Huvudavtalet

   Adress: Som anges i Huvudavtalet

   Kontaktpersonens namn, befattning och kontaktuppgifter: Jesper Forster, Data Protection Officer. Glooko AB, Nellickevägen 20B412 63 Göteborg, Sverige. Email: dpo@glooko.com

   Verksamheter som är relevanta för de uppgifter som överförs enligt dessa klausuler: Tillhandahållande av de Produkter som anges i tillämpligt Beställningsformulär.

   Underskrift och datum: Som anges i Beställningsformulär i enlighet med Huvudavtalet.

   Roll (personuppgiftsbiträde/personuppgiftsansvarig): Personuppgiftsbiträde

2. …

Uppgiftsinförare: [*Uppgiftsinförarens/uppgiftsinförarnas identitet och kontaktuppgifter, inklusive eventuella kontaktpersoner med ansvar för dataskydd]*

1. Namn: Klient (som anges i tillämpligt Beställningsformulär)

   Adress: Klientens adress (som anges i tillämpligt Beställningsformulär)

   Kontaktpersonens namn, befattning och kontaktuppgifter: Klientens adress (som anges i tillämpligt Beställningsformulär)

   Verksamheter som är relevanta för de uppgifter som överförs enligt dessa klausuler: Mottagande av de Produkter som anges i tillämpligt Beställningsformulär

   Underskrift och datum: Som anges i tillämpligt Beställningsformulär i enlighet med Huvudavtalet

   Roll (personuppgiftsbiträde/personuppgiftsansvarig): Personuppgiftsansvarig

2. …

B. BESKRIVNING AV ÖVERFÖRINGEN

Kategorier av registrerade vars personuppgifter överförs

- Klientens Auktoriserade Användare
- Patienter

Kategorier av personuppgifter som överförs

<u>Klientens Auktoriserade Användare</u>

- Allmän information (namn)

- Kontaktinformation (emailadress, telefonnummer)
- Information om användning (användarnamn, lösenord, åtkomsträttigheter, revisionsloggar)

Patienter

- Allmän information (namn, födelsedatum, kön)
- Kontaktinformation (postadress, emailadress, telefonnummer)
- Information om användning (användarnamn, lösenord)
- Hälsoinformation (diabetstyp, år för diabetesdiagnos, beräknat förlossningsdatum , målintervall, vikt, längd, behandling)
- Enhetsinformation (insulinpump, glukosmätare och insulinpennas serienummer, doser, kolhydrater, inställningar, larm)

Känsliga uppgifter som överförs (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder där full hänsyn tas till uppgifternas karaktär och de medföljande riskerna, till exempel strikt ändamålsbegränsning, åtkomstbegränsningar (däribland åtkomst endast för personal som har specialutbildning), registrering av åtkomst till uppgifterna, begränsningar av vidare överföringar eller ytterligare säkerhetsåtgärder.

- Hälsoinformation (diabetstyp, år för diabetesdiagnos, beräknat förlossningsdatum , målintervall, vikt, längd, behandling)

Åtkomstbegränsningar för personal baserat på vad de behöver veta (för både personuppgiftsansvarig och personuppgiftsbiträdet)

Register över åtkomst till data loggas

Under överföring och lagring är uppgifter krypterade

Frekvens för överföringen (t.ex. om uppgifterna överförs vid ett engångstillfälle eller kontinuerligt).

Personuppgifterna lagras av personuppgiftsbiträdet, men kan när som helst nås av den personuppgiftsansvarige (om t.ex. Produkterna består av programvara som en tjänst). Personuppgifter kan i dessa fall anses överförda från EES till ett tredjeland.

Behandlingens karaktär

Ladda upp, kalkylera, analysera, visualisera, överföra och på annat sätt behandla personuppgifter för att möjliggöra för Auktoriserade Användare att använda Produkterna.

Ändamålet/ändamålen med överföringen av uppgifter och den efterföljande behandlingen

Ändamålet med överföringen av uppgifter är att möjliggöra för Klienten att använda Produkterna.

Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period

Behandlingen är inte tidsbegränsad och ska utföras så länge som Produkterna tillhandahålls eller tills tillämpligt avtal avseende behandling av personuppgifter sägs upp.

Vid överföringar till personuppgiftsbiträden/underentreprenörer, ange även föremålet för behandlingen liksom dess karaktär och varaktighet

Inte tillämpligt

C. BEHÖRIG TILLSYNSMYNDIGHET

Ange den eller de behöriga tillsynsmyndigheterna i enlighet med klausul 13

Inte tillämpligt

BILAGA II

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INKLUSIVE TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA UPPGIFTERNAS SÄKERHET

Inte tillämpligt

BILAGA III

FÖRTECKNING ÖVER UNDERENTREPRENÖRER

Inte tillämpligt