PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679[1]

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	**Personuppgiftsbiträde**
Region Västmanland	Glooko AB
Organisationsnummer	**Organisationsnummer**
232100-0172	556668-4675
Postadress	**Postadress**
Regionhuset, 721 89 Västerås	Nellickevägen 20, 412 63 Göteborg
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**
Namn: E-post: Tfn:	Nick van der Meer nick.vandermeer@glooko.com
Kontaktperson för parternas samarbete om dataskydd	**Kontaktpersoner för parternas samarbete om dataskydd**
Namn: *Moon Carlbring* E-post: *dataskyddsombudet@regionvastmanland.se* Tfn: *021-173 00 00*	Kontaktuppgifter till dataskyddsombud: dpo@glooko.com
Personuppgiftsbiträdesavtal gäller för följande affärsavtal	
Orderformulär (se definition i punkten 2 DEFINITIONER nedan)	

[1] Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

2. DEFINITIONER

Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

Behandling	En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den Behandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.
Logg	Logg är resultatet av Loggning.
Orderformulär	Orderformulär som beskrivs i detta personuppgiftsbiträdesavtal avser varje orderformulär, avseende beställning av analysverktyget Glooko, för enskild klinik som beställande enhet och användare för analysverktyget Glooko inom Region Västmanland.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.

Registrerad	Fysisk person vars Personuppgifter Behandlas.
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).
Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3. BAKGRUND OCH SYFTE

3.1 Med detta Personuppgiftsbiträdesavtal jämte Instruktioner och en eventuell förteckning över Underbiträden (nedan gemensamt "PUB-avtalet") reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad stadgas i artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679 ("Dataskyddsförordningen").

3.2 När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet "Orderformulär" i PUB-avtalet.

3.3 Hänvisningar i PUB-avtalet till nationell eller unionsrättslig lagstiftning, avser vid var tid tillämpliga bestämmelser.

4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

4.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen, se Bilaga 1.

4.3. Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner angivna i Bilaga 1.

5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner så att Personuppgiftsbiträdet och eventuellt Underbiträde kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Orderformulär i förekommande fall.

5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig att säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 i Dataskyddsförordningen fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner.

6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder, se Bilaga 1, som krävs enligt Dataskyddslagstiftningen för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

8. SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

8.2. Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.

8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3.h i Dataskyddsförordningen.

9.2 Personuppgiftsbiträdet ska minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation som visar att Personuppgiftsbiträdet har erforderliga tredjeparts certifikat på plats, samt göra all relevant nödvändig information tillgänglig och svara på frågor avseende Personuppgiftsbiträdet verksamhet, med undantag för den information som Personuppgiftsbiträdet är begränsad att lämna ut, som behövs för att kunna granska Personuppgiftsbiträdets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2–9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt punkten 9 i PUB-avtalet.

10. HANTERING AV RÄTTELSER OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella Personuppgiften som ett led i processen för rättelse eller radering.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka försämrar säkerheten kring Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad stadgas om meddelanden i punkten 19 i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11. PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1.c i Dataskyddsförordningen.

11.2 Personuppgiftbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda obehörig Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincident, vilken Personuppgiftbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå, tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

Beskrivningen ska redogöra för:

1. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
2. de sannolika konsekvenserna av Personuppgiftsincidenten, och
3. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftincidentens potentiella negativa effekter.

11.4 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkten 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12. UNDERBITRÄDE

12.1 Personuppgiftsbiträdet äger rätt att anlita den eller de Underbiträden som framgår av bilagd förteckning över Underbiträden, se Bilaga 2.

12.2 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt avtal med Underbiträdet som reglerar Behandlingen som Underbiträdet utför å en Personuppgiftsansvariges vägnar samt att endast anlita Underbiträden som ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddsförordningen. I fråga om dataskydd ska avtalet ålägga Underbiträdet samma skyldigheter som åläggs Personuppgiftsbiträdet i detta PUB-avtal.

12.3 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige.

12.4 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden.

12.5 När Personuppgiftsbiträdet avser att anlita ett nytt eller ersätta ett befintligt Underbiträde ska Personuppgiftsbiträdet säkerställa Underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

1. Underbiträdets namn, organisationsnummer och säte (adress och land),
2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
3. var Personuppgifterna ska behandlas.

12.6 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.5 invända mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde och att, med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkten 17.4.

12.7 När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om att det upphör med att anlita Underbiträdet.

12.8 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Behandling av Underbiträdets Behandling av Personuppgifter enligt punkten 12.2. I den mån det är nödvändigt för att skydda företagshemligheter eller annan sekretessbelagd information, inklusive personuppgifter, har Personuppgiftsbiträdet rätt att sekretessmarkera sådana delar av avtalet innan Personuppgiftsbiträdet översänder en kopia av avtalet till den Personuppgiftsansvarige.

13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger rätt att behandla begränsad mängd Personuppgifter till Tredje land för Behandling (enbart för teknisk support och för regulatoriska syften). Sådan behandling ska vara begränsad till endast den nödvändiga minsta mängden Personuppgifter, för en begränsad tidsperiod och ska aldrig medföra en permanent överföring eller lagring av Personuppgifter i ett sådant Tredje Land.

13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkten 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten, under detta PUB-avtal, ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad sägs i Orderformulär gäller detta PUB-avtal, punkterna 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

14.5 Personuppgiftsbiträdets ansvar gentemot Personuppgiftsansvarig för skador, kostnader och utlägg ska maximalt uppgå till de belopp som Personuppgiftsbiträdet har erhållit för Orderformulär under vilket skadan har uppkommit under de tolv månader som föregått händelsen som lett till skadan. Personuppgiftsbiträdet och dess aktieägare, närstående bolag, ledning, chefer, anställda och andra ombud ska inte vara ansvariga inför Personuppgiftsansvarig, Auktoriserade användare eller någon tredje part för indirekt, tillfällig, särskild skada eller följdskada (inbegripet advokatarvoden och förlorade intäkter) som härrör från eller har uppstått i samband med detta PUB-avtal. Detta inbegriper bland annat skada, smärta och lidande som en person kan drabbas av, känslomässigt lidande samt förlust av inkomst, intäkter, affärsverksamhet, förmodade besparingar, användning, goodwill eller data, förseningar eller avbrott i driften eller avbrott i överföringskommunikationen, förlust av anslutning, avbrott i nätverk eller system, otillgänglighet hos eller drift i kombination med en tredje parts nätverk eller system. Detta gäller oavsett huruvida situationen har uppstått genom en skadegrundande händelse (inbegripet vårdslöshet), avtalsbrott eller på annat sätt, även om den kunnat förutses och även om Personuppgiftsbiträdet informerats om risken för sådan skada.

15. LAGVAL OCH TVISTLÖSNING

15.1 För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol.

16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

16.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tillsvidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

17.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

17.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

17.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet och/eller Instruktioner ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

17.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.6, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan.

18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

18.1 Vid uppsägning av PUB-avtalet ska den Personuppgiftsansvarige utan onödigt dröjsmål begära att Personuppgiftsbiträdet överlämnar samtliga Personuppgifter till den Personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

18.2 Överlämning och radering enligt PUB-avtalet, punkten 18.1, ska vara utförda senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt detta PUB-avtal, punkten 16.1.

18.3 Behandling som utförs av Personuppgiftsbiträdet efter den tidpunkt som stadgas i punkten 18.2 är att betrakta som en otillåten Behandling.

18.4 Bestämmelser om sekretess/tystnadsplikt i punkten 8 enligt detta PUB-avtal ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

19.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas till respektive parts kontaktperson för PUB-avtalet.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande Behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

19.3 Meddelanden inom ramen för PUB-avtalet och Instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

20. KONTAKTPERSONER

20.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.

20.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.

21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

21.1 Varje part ansvarar för att de uppgifter som anges i punkten 1 i PUB-avtalet alltid är aktuella. Ändring av uppgifter i punkten 1 ska meddelas skriftligen enligt punkten 19.1 i PUB-avtalet.

22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt tecknande eller i pappersformat för tecknande med penna. Om PUB-avtalet tillhandahålls i digitalt format utgår punkter 22.2–22.3.

22.2 Den Personuppgiftsansvariges undertecknande av PUB-avtalet

Ort Datum

Västerås 18 feb 25

Undertecknande

Namnförtydligande

22.3 Personuppgiftsbiträdets undertecknande av PUB-avtalet

Ort Datum

January 31, 2025

Undertecknande

MARK BEUCLER

Namnförtydligande

Bilaga 1. Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående Instruktion:

1. Ändamål, föremålet och arten

Ändamålet är att tillhandahålla god, patientsäker och effektiv diabetesvård till användare enligt Socialstyrelsens nationella riktlinje för Diabetesvård.

- Möjliggöra för patienter att bedriva god egenvård.
- Möjliggöra för vårdpersonalen att vägleda och utbilda patienterna för egenvård.
- Leverantör ska ge teknisk support för de diabetestekniska produkter som leverantören tillhandahåller för den personuppgiftsansvarige.

Föremålet för Personuppgiftsbiträdets behandling av Personuppgifter åt den Personuppgiftsansvarige är att:
Behandling av Personuppgifter åt den Personuppgiftsansvarige i samband med att Personuppgiftsbiträdet tillhandahåller en webbaserad "data management" tjänst till sjukvårdspersonal för hantera data från produkter som används av personer med diabetes på uppdrag av den Personuppgiftsansvarige. Behandlingen av Personuppgifterna är delvis eller helt automatiserad.

Personuppgiftsbiträdet ska behandla personuppgifter för följande ändamål

- För att göra det möjligt att tillhandahålla Tjänsterna enligt beskrivningen i detta Personuppgiftsbiträdesavtal och Orderformulär, inklusive:
  -Leverera tjänsten som en molntjänst
  (För patienter: Behandling av personuppgifter om den registrerade och att göra dessa uppgifter fjärråtkomliga för personer som har fått behörighet av Personuppgiftsansvarige.
  För vårdpersonal: Behandling av personuppgifter om den registrerade inom ramen för användningen av produkterna och Tjänsterna.)
  -Utföra tekniskt underhåll och säkerhetskopiering
  -Användarstatistik med syfte att fakturera och utveckla applikationer
  -Utvärdering av prestanda och användning av Tjänsterna samt utrustning, teknik och infrastruktur som krävs för deras tillhandahållande samt av produkterna, bland annat identifiera områden för förbättring som kan bidra till Tjänsternas, produkternas och patientbehandlingarnas säkerhet och kvalitet, exempelvis:
  (1) Skapa och utvärdera aggregerade data avseende produktinställningar, produktprestanda och kliniska data för produkterna, möjlighet till proaktiv optimering av utbildning och information till vårdpersonal med fokus på optimal patientbehandling.
  (2) Skapa och utvärdera aggregerade data erhållna från incidentrespons, felsökning och teknisk support för Personuppgiftsansvarige och patienterna för att förbättra Tjänsterna och relaterad utbildning för Personuppgiftsansvarige och patienterna.
  (3) Skapa och utvärdera data avseende överföringar för att proaktivt kunna optimera utbildning och information för Personuppgiftsansvarige och patienterna.

-Samla in, analysera, visualisera och på annat sätt behandla Personuppgifterna i enlighet med Orderformulär och detta Personuppgiftsbiträdesavtal

- Utvärdera, analysera och rapportera om insamlande personuppgifter på begäran av Personuppgiftsansvarig.

-Vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för Behandlade Personuppgifter, vilket kan inkludera pseudonymisering, anonymisering och kryptering.

- Efterkomma rimliga begäranden från behörig brottsbekämpande personal eller representanter, rättsliga myndigheter, offentliga myndigheter eller organ, inklusive behöriga dataskyddsmyndigheter, varvid behandlingen begränsas till miniminivån för att uppfylla begäran. Personuppgiftsbiträde kommer i vilket fall att underrätta Personuppgiftsansvarig om en sådan begäran, förutom om förhandsanmälan inte är tillåten på grund av skyldighet till sekretess som åläggs Personuppgiftsbiträdet enligt tillämplig lag eller av begärande person, representant, myndighet eller organ.

- Säkerställa att Tjänsterna samt produkter, teknik och infrastruktur som krävs för att tillhandahålla dessa fungerar i enlighet med Orderformulär och detta Personuppgiftsbiträdesavtal, bland annat genom regelbundet underhåll, incidentrespons, felsökning och teknisk support för Personuppgiftsansvarige och de registrerade, inklusive patienter.

2. Behandlingen omfattar följande typer av Personuppgifter

Patientens personuppgifter:
-Allmän information (Förnamn, efternamn, födelsedatum, kön)
-Kontaktinformation (postadress, e-postadress, telefonnummer, mobiltelefonnummer, födelsenummer, patientdata, apparatdata och hälsodata.
-Hälsoinformation (diabetestyp, år för diabetesdiagnos, beräknat förlossningsdatum, målintervall, vikt, längd, behandling)
-Enhetsinformation (insulinpump, glukosmätare och insulinpennas serienummer, doser, kolhydrater, inställningar, larm)

Personuppgiftsansvariges anställdas och konsulters personuppgifter:
-Allmän information (Förnamn, efternamn), inloggningsuppgifter
- Kontaktinformation (e-postadress, telefonnummer)
-Användarinformation (användarnamn, lösenord, åtkomsträttigheter, ändringsloggar)

3. Behandlingen omfattar kategorier av Registrerade

Personuppgifter i systemet utgörs av:

- Patienter
- Personuppgiftsansvariges anställda och konsulter och vårdgivare som benämns som Auktoriserad användare som finns i Orderformulär.

4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

Alla hanteringskrav är tillämpliga för Personuppgiftsbiträdet och möjliga underbiträden.

Personuppgiftsbiträdet ska ha nödvändiga rutiner/instruktioner för anställda och användare måste finnas och användas.

Personuppgiftsbiträdets anställda måste ingå och följa ett sekretessavtal för att skydda den registrerades personuppgifter.

Personuppgiftsbiträdets anställda måste ha genomgått utbildning i GDPR och ha en förståelse för det.

Personuppgiftsbiträdets anställda måste få tydliga instruktioner så att de vet hur de ska hantera en personuppgiftsincident.

Personuppgiftsbiträdets anställda måste ha genomgått träning inom IT-säkerhet.

Personuppgiftsbiträdets anställda inom supporten hanterar personuppgifter endast om det är nödvändigt baserat på lägsta behörighet.

Personuppgiftsbiträdets anställda aktivitet i databasen måste loggas och vara uppkopplade via en säker inloggning i databasen.

Loggning av personuppgiftsbiträdets anställdas aktivitet måste göras regelbundet och kontrolleras minst en gång om året.

Personuppgifterna måste loggas separat från personuppgifter som Personuppgiftsbiträdet behandlar på uppdrag av någon annan än den Personuppgiftsansvarige.

Personuppgiftsbiträdet ska ha dokumenterade förfaranden för att skydda systemet mot virus, trojaner och andra former av digitala intrång. Enbart program som formellt är godkända inom bolaget skall användas i systemmiljön.

Personuppgiftsbiträdet ska logga och förhindra alla försök till intrång.

Personuppgiftsbiträdet ska ha återkommande säkerhetskopiering av personuppgifter och databas måste genomföras. På liknande sätt, ska kontroller av säkerhetskopior och säkerhetskopior verifieras enligt rutiner.

Personuppgiftsbiträdet skall säkerställa att login till tjänsten görs genom antingen tvåfaktorsautentisering (2FA) eller genom att använda den Personuppgiftsansvariges egna Single Sign-On (SSO).

Personuppgiftsbiträdet måste ge information som är nödvändig på individnivå för att den Personuppgiftsansvarige ska kunna fullgöra den registrerades rättigheter. Till exempel i form av ett registerutdrag.

5. Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

Personuppgiftsbiträdet ska ha krypteringsprotokoll i lagring enligt AES256 eller motsvarande som godkänns av den Personuppgiftsansvarige.
Personuppgiftsbiträdet ska ha krypteringsprotokoll för överföring som enligt TLS v1.2 eller högre, alternativt likvärdigt krypteringsprotokoll som Personuppgiftsansvarige bedömer vara godkänd.

Personuppgiftsbiträdet ska redogöra skriftligt i bilaga 3 tekniska och organisatoriska säkerhetsåtgärder som ska godkännas av Personuppgiftsansvarig i samband med tecknande av personuppgiftsbiträdesavtal.

6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem

Personuppgiftsbiträdet ska ansvara för att:
Personuppgiftsbiträdet ska ha minimal tillgång till personuppgifter. Aktivitet ska loggas hos användarna för att kunna granskas vid ett senare tillfälle om det är nödvändigt. Loggarna ska åtminstone innehålla följande information:

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient (vilken typ av aktivitet; originalvärde och nya värdet),
2. det av loggarna framgår vid vilken organisatoriska enhet åtgärderna vidtagits (vem (användare) har utfört),
3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits (datum, tid och tidsperiod),
4. användarens och patientens identitet framgår av loggarna (vem (användare) och vilken patient),
5. loggarna sparas minst fem år för att möjliggöra kontroll av åtkomsten till uppgifter om en patient

Personuppgiftsbiträdet ska tillhandahålla på begäran av Personuppgiftsansvarig loggutdrag enligt ovanstående kriterier.

7. Lokalisering och överföring av Personuppgifter till Tredje land

- Personuppgifterna ska hanteras och lagras inom EU/EES i enlighet med p. 13.1 i PUB-avtalet. Vid de fall där Personuppgifterna ska behandlas enligt p. 13.2 ska ett av nedanstående kriterier uppfyllas:
- Leverantören ska ha ett av Integritetsskyddsmyndigheten eller annan tillsynsmyndighet inom EU godkänt BCR (Binding corporate rules)

- Om leverantören är registrerad och lokaliserad i ett land som EU-kommissionen godkänt som ett land med adekvata skyddsnivå ska SCC (Standard contractual clauses som är framtagen av EU-kommissionen) tecknas med samtliga biträden i tredjeland där det är relevant.

- Tredjelandsöverföring som uppkommer i samband med nyttjande av underbiträde ska biträdet tillse att lämpliga skyddsåtgärder vidtas enligt artikel 46 allmänna dataskyddsförordningen och enligt EDPBs riktlinjer om säkerhetsåtgärder.

- Tredjelandsöverföring till USA som av EU-kommissionen har bedömts ha adekvat skyddsnivå enligt artikel 45 ska vara anslutna och certifierade mot Data Privacy Framework, personuppgiftsbiträde och personuppgiftsunderbiträden ska uppvisa certifieringsdokumenten.

8. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/biträdena

Personuppgiftsbiträdets interna information och IT säkerhetsarbete måste baseras på ISO27000, ISO27001 and ISO27002, vilket också gäller för eventuella underbiträden.

När nya/uppdaterade funktioner lanseras i molntjänsten ska följande göras:

-Följa upp säkerhetskrav
-Funktionstester så att inga fel hitta i programmet vid driftsättning
-Produktionsdata är inte tillåtet att använda under testning
-Uppdatering av operativa dokument och användardokument. Detta görs innan ett säkerhetsgodkännande kan ges och driften kan påbörjas.

Interna säkerhetsgranskningar måste göras periodvis dock minst en gång om året. Interna aktiviteter som förbättrar säkerheten och omständigheterna kring informationen måste göras kontinuerligt och omfattande.

Bilaga 2. Personuppgiftsbiträdets biträdesförhållande vid avtalstecknandet.

Biträdet ska vid de fall det är aktuellt ange ifall personuppgiftsbiträdet ingår i en koncern, om ja redogör bolagsuppgifter för koncernen.

Biträdet ska vid de fall det är aktuellt ange vilka underbiträden bolaget anlitar som kommer behandla eller ta del av personuppgiftsansvariges personuppgifter.

Inom parentes anges de länder där respektive bolag är etablerat och från vilka personal kan komma att behandla personuppgifter.

Behandla supportärenden, samtal och andra supportförfrågningar från den personuppgiftsansvarige.

☐	Det finns inga underleverantörer vid avtalets ingående	
1	**Namn och geografisk belägenhet**	Glooko Inc., 579 University Avenue, Palo Alto, CA 94301, USA, DUNS 078605143 (ingår i samma koncern som Glooko AB)
	Personuppgifter som behandlas	Se punkt 2 i Bilaga 1
	Roll i dataprocessen	För regulatoriska krav och teknisk support
2	**Namn och geografisk belägenhet**	Amazon Web Services Ireland (AWS), One Burlington Plaza, Burlington Road, Ballsbridge, Dublin 4, Ireland Lokalisering: Dublin, Irland och Frankfurt, Tyskland.
	Personuppgifter som behandlas	Se punkt 2 i Bilaga 1
	Roll i dataprocessen	Leverantör av molntjänst
3	**Namn och geografisk belägenhet**	
	Personuppgifter som behandlas	
	Roll i dataprocessen	

Bilaga 3. TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INBEGRIPET TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA DATASÄKERHETEN.

1. Syfte. Detta 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.

Versionshantering				
Dokument	Version	Datum	Ändringar	Ansvarig
Avtal	1.2.1	2020-01-02	17.4	PR (SKR)
Bilaga 1	1.2	2019-10-25	Borttag av 'Mall för förteckning över Underbiträden vid PUB-avtalets ingående	PR (SKR)
Bilaga 2	1.1	2021-05-05	Tillägg, Biträdesförhållanden Redogör ifall biträdet ingår i en koncern	MC (RV)