

## GLOOKO STANDAARDCONTRACTBEPALINGEN

### AFDELING I

#### *Bepaling 1*

##### ***Doel en toepassingsgebied***

- (a) Het doel van deze standaardcontractbepalingen (hierna “de bepalingen” genoemd) is te zorgen voor de naleving van artikel 28, leden 3 en 4, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
- (b) De in bijlage I vermelde verwerkingsverantwoordelijken en verwerkers hebben met deze bepalingen ingestemd teneinde te zorgen voor de naleving van artikel 28, leden 3 en 4, van Verordening (EU) 2016/679 en/of artikel 29, leden 3 en 4, van Verordening (EU) 2018/1725.
- (c) Deze bepalingen zijn van toepassing indien is voldaan aan de vereisten vermeld in de Raamovereenkomst en op de verwerking van persoonsgegevens als gespecificeerd in bijlage II.
- (d) De bijlagen I tot en met IV maken integrerend deel uit van de bepalingen.
- (e) Deze bepalingen laten de verplichtingen die op de verwerkingsverantwoordelijke rusten krachtens Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 onverlet.
- (f) Deze bepalingen waarborgen op zichzelf niet de naleving van verplichtingen in verband met internationale doorgiften overeenkomstig hoofdstuk V van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.

#### *Bepaling 2*

##### ***Onveranderlijkheid van de bepalingen***

- (a) De partijen verbinden zich ertoe de bepalingen niet te wijzigen, tenzij om informatie aan de bijlagen toe te voegen of de daarin vervatte informatie bij te werken.
- (b) Dit belet de partijen niet om de in deze bepalingen neergelegde standaardcontractbepalingen op te nemen in een bredere overeenkomst, of om andere bepalingen of aanvullende waarborgen toe te voegen, mits deze niet direct of indirect in strijd zijn met de bepalingen of afbreuk doen aan de grondrechten of fundamentele vrijheden van betrokkenen.

#### *Bepaling 3*

##### ***Interpretatie***

- (a) Wanneer in deze bepalingen de termen worden gebruikt die zijn gedefinieerd in Verordening (EU) 2016/679 respectievelijk Verordening (EU) 2018/1725, hebben die termen dezelfde betekenis als in die verordening.
- (b) Deze bepalingen moeten worden gelezen en geïnterpreteerd in het licht van de

bepalingen van Verordening (EU) 2016/679 respectievelijk Verordening (EU) 2018/1725.

- (c) Deze bepalingen mogen niet worden geïnterpreteerd op een wijze die indruist tegen de rechten en verplichtingen waarin Verordening (EU) 2016/679/Verordening (EU) 2018/1725 voorziet of op een wijze die afbreuk doet aan de grondrechten of fundamentele vrijheden van de betrokkenen.

#### *Bepaling 4*

##### ***Hiërarchie***

In geval van tegenstrijdigheid tussen deze standaardcontractbepalingen en de bepalingen van gerelateerde overeenkomsten tussen de partijen die reeds bestaan op het tijdstip waarop met deze standaardcontractbepalingen wordt ingestemd of die na dat tijdstip worden gesloten, prevaleren deze standaardcontractbepalingen.

- (a) Elke entiteit die geen partij deze bepalingen is, kan, met instemming van alle partijen, te allen tijde tot deze bepalingen toetreden als verwerkingsverantwoordelijke of verwerker door de bijlagen in te vullen en bijlage I te ondertekenen.
- (b) Wanneer de in punt a) bedoelde bijlagen zijn ingevuld en ondertekend, wordt de toetredende partij als een partij bij deze bepalingen behandeld en heeft zij de rechten en verplichtingen van een verwerkingsverantwoordelijke of verwerker, al naar gelang zij in bijlage I is aangeduid.
- (c) Voor de toetredende entiteit vloeien uit deze bepalingen geen rechten of verplichtingen voort met betrekking tot de periode voordat zij partij werd.

#### *Bepaling 5 — Facultatief*

##### ***Docking-bepaling***

- (a) Elke entiteit die geen partij deze bepalingen is, kan, met instemming van alle partijen, te allen tijde tot deze bepalingen toetreden als verwerkingsverantwoordelijke of verwerker door de bijlagen in te vullen en bijlage I te ondertekenen.
- (b) Wanneer de in punt a) bedoelde bijlagen zijn ingevuld en ondertekend, wordt de toetredende partij als een partij bij deze bepalingen behandeld en heeft zij de rechten en verplichtingen van een verwerkingsverantwoordelijke of verwerker, al naar gelang zij in bijlage I is aangeduid.
- (c) Voor de toetredende entiteit vloeien uit deze bepalingen geen rechten of verplichtingen voort met betrekking tot de periode voordat zij partij werd.

## **AFDELING II - VERPLICHTINGEN VAN PARTIJEN**

#### *Bepaling 6*

##### ***Beschrijving van de verwerking(en)***

De bijzonderheden van de verwerkingen, en met name de categorieën persoonsgegevens en de doeleinden van de verwerking waarvoor de persoonsgegevens namens de verwerkingsverantwoordelijke worden verwerkt, zijn gespecificeerd in bijlage II.

## *Bepaling 7*

### **Verplichtingen van de partijen**

#### **7.1. Instructies**

- (a) De verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht. In dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij de wetgeving dit om gewichtige redenen van algemeen belang verbiedt. De verwerkingsverantwoordelijke kan ook tijdens de verwerking van persoonsgegevens steeds verdere instructies geven. Deze instructies worden altijd schriftelijk vastgelegd.
- (b) De verwerker stelt de verwerkingsverantwoordelijke onmiddellijk in kennis als de instructies van de verwerkingsverantwoordelijke naar het oordeel van de verwerker inbreuk maken op Verordening (EU) 2016/679/Verordening (EU) 2018/1725 of de toepasselijke gegevensbeschermingsbepalingen van de Unie of de lidstaten.

#### **7.2. Doelbinding**

De verwerker verwerkt de persoonsgegevens uitsluitend voor het specifieke doel of de specifieke doeleinden van de verwerking, zoals beschreven in bijlage II, tenzij hij verdere instructies van de verwerkingsverantwoordelijke krijgt.

#### **7.3. Doel van de verwerking van persoonsgegevens**

Verwerking door de verwerker vindt slechts plaats gedurende de in bijlage II vastgestelde tijdspanne.

#### **7.4. Beveiliging van de verwerking**

- (a) De verwerker treft ten minste de in bijlage III gespecificeerde technische en organisatorische maatregelen om de beveiliging van de persoonsgegevens te waarborgen. Dit houdt onder meer in dat de gegevens worden beschermd tegen een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot de gegevens, hetzij per ongeluk hetzij onrechtmatig (inbreuk in verband met persoonsgegevens). Bij de beoordeling van het passende beveiligingsniveau houden de partijen naar behoren rekening met de stand van de techniek, de uitvoeringskosten, de aard, de reikwijdte, de context en de doeleinden van de verwerking en de risico's voor de betrokkenen.
- (b) De verwerker verleent zijn personeel slechts toegang tot de persoonsgegevens die worden verwerkt voor zover dat strikt noodzakelijk is voor de uitvoering, het beheer en de monitoring van de overeenkomst. De verwerker waarborgt dat de tot het verwerken van de ontvangen persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

#### **7.5. Gevoelige gegevens**

Indien de verwerking betrekking heeft op persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap

van een vakbond blijken, of betrekking heeft op genetische gegevens of biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (hierna “gevoelige gegevens” genoemd), voorziet de verwerker in specifieke beperkingen en/of aanvullende waarborgen.

## **7.6. Documentatie en naleving**

- (a) De partijen kunnen aantonen dat aan deze bepalingen is voldaan.
- (b) De verwerker behandelt verzoeken van de verwerkingsverantwoordelijke inzake de verwerking van gegevens overeenkomstig deze bepalingen onverwijld en adequaat.
- (c) De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat is voldaan aan de in deze bepalingen vastgestelde verplichtingen die rechtstreeks voortvloeien uit Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725. Op verzoek van de verwerkingsverantwoordelijke staat de verwerker ook regelmatig, of indien er aanwijzingen van niet-naleving zijn, audits toe van de onder deze bepalingen vallende verwerkingsactiviteiten en draagt de verwerker aan die audits bij. Bij het nemen van een beslissing over een toetsing of audit kan de verwerkingsverantwoordelijke rekening houden met relevante certificeringen van de verwerker.
- (d) De verwerkingsverantwoordelijke kan ervoor kiezen de audit zelf uit te voeren of een onafhankelijke auditor daartoe opdracht te geven. De audits kunnen ook inspecties in de bedrijfsruimten of fysieke faciliteiten van de verwerker omvatten en worden, in voorkomend geval, tijdig aangekondigd.
- (e) De partijen stellen de in deze bepaling bedoelde informatie, met inbegrip van de resultaten van eventuele audits, op verzoek ter beschikking van de bevoegde toezichthoudende autoriteit/autoriteiten.

## **7.7. Gebruik van subverwerkers**

- (a) De verwerker heeft de algemene toestemming van de verwerkingsverantwoordelijke om subverwerkers in dienst te nemen die op een overeengekomen lijst staan. De verwerker stelt de verwerkingsverantwoordelijke ten minste dertig (30) dagen van tevoren specifiek schriftelijk in kennis van voorgenomen wijzigingen van die lijst door toevoeging of vervanging van subverwerkers, zodat de verwerkingsverantwoordelijke voldoende tijd heeft om vóór de indienstneming van de betrokken subverwerker(s) bezwaar te kunnen maken tegen dergelijke wijzigingen. De verwerker verstrekt de verwerkingsverantwoordelijke de informatie die nodig is om deze laatste in staat te stellen zijn recht van bezwaar uit te oefenen.
- (b) Wanneer de verwerker een subverwerker in dienst neemt voor de uitvoering van specifieke verwerkingen (namens de verwerkingsverantwoordelijke), doet hij dit door middel van een overeenkomst die de subverwerker in wezen dezelfde verplichtingen inzake gegevensbescherming oplegt als die welke op grond van deze bepalingen aan de verwerker worden opgelegd. De verwerker zorgt ervoor dat de subverwerker voldoet aan de verplichtingen die krachtens deze bepalingen en Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 op de verwerker rusten.
- (c) Op verzoek van de verwerkingsverantwoordelijke verstrekt de verwerker de verwerkingsverantwoordelijke een kopie van een dergelijke

subverwerkingsovereenkomst en van alle latere wijzigingen daarvan. Voor zover nodig ter bescherming van bedrijfsgeheimen of andere vertrouwelijke informatie, met inbegrip van persoonsgegevens, kan de verwerker de tekst van de overeenkomst bewerken alvorens de kopie te delen.

- (d) De verwerker blijft ten opzichte van de verwerkingsverantwoordelijke volledig verantwoordelijk voor de uitvoering van de verplichtingen van de subverwerker overeenkomstig zijn overeenkomst met de verwerker. De verwerker stelt de verwerkingsverantwoordelijke in kennis van elk verzuim van de subverwerker om zijn contractuele verplichtingen na te komen.
- (e) De verwerker komt, indien mogelijk, met de subverwerker een derdenbeding overeen waarbij — ingeval de verwerker feitelijk is verdwenen, rechtens is opgehouden te bestaan of insolvent is geworden — de verwerkingsverantwoordelijke het recht heeft de overeenkomst met de subverwerker te beëindigen en de subverwerker te gelasten de persoonsgegevens te wissen of terug te geven.

### **7.8. Internationale doorgiften**

- (a) Doorgifte van gegevens aan een derde land of een internationale organisatie door de verwerker geschiedt uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke of om te voldoen aan een specifieke eis uit hoofde van het Unierecht of het lidstatelijke recht waaraan de verwerker is onderworpen, en vindt plaats in overeenstemming met hoofdstuk V van Verordening (EU) 2016/679 of Verordening (EU) 2018/1725.
- (b) De verwerkingsverantwoordelijke stemt ermee in dat wanneer de verwerker overeenkomstig bepaling 7.7 een subverwerker in dienst neemt voor het uitvoeren van specifieke verwerkingen (namens de verwerkingsverantwoordelijke) en die verwerkingen een doorgifte van persoonsgegevens in de zin van hoofdstuk V van Verordening (EU) 2016/679 inhouden, de verwerker en de subverwerker de naleving van hoofdstuk V van Verordening (EU) 2016/679 kunnen waarborgen door gebruik te maken van standaardcontractbepalingen die door de Commissie zijn vastgesteld overeenkomstig artikel 46, lid 2, van Verordening (EU) 2016/679, mits aan de voorwaarden voor het gebruik van die standaardcontractbepalingen is voldaan.

#### *Bepaling 8*

##### ***Bijstand aan de verwerkingsverantwoordelijke***

- (a) De verwerker verwijst betrokkenen door naar de voor de verwerkingsverantwoordelijke, indien de verwerker een verzoek van een betrokkene ontvangt. De verwerker antwoordt niet zelf op het verzoek, tenzij de verwerkingsverantwoordelijke daartoe toestemming heeft gegeven.
- (b) De verwerker staat de verwerkingsverantwoordelijke bij bij het vervullen van zijn verplichtingen om te reageren op verzoeken van betrokkenen tot uitoefening van hun rechten, en houdt daarbij rekening met de aard van de verwerking. Bij het nakomen van zijn verplichtingen uit hoofde van de punten a) en b) volgt de verwerker de instructies van de verwerkingsverantwoordelijke.
- (c) De verwerker heeft niet alleen de verplichting de verwerkingsverantwoordelijke bij te staan overeenkomstig bepaling 8, punt b), maar staat de verwerkingsverantwoordelijke ook bij bij het waarborgen van de naleving van de volgende verplichtingen, waarbij

rekening wordt gehouden met de aard van de gegevensverwerking en de informatie waarover de verwerker beschikt:

- (1) de verplichting om een beoordeling uit te voeren van het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens (een “gegevensbeschermingseffectbeoordeling”) wanneer een bepaalde soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen;
  - (2) de verplichting om de bevoegde toezichthoudende autoriteit/autoriteiten voorafgaand aan de verwerking te raadplegen wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om dat risico te beperken;
  - (3) de verplichting om ervoor te zorgen dat persoonsgegevens accuraat en actueel zijn, door de verwerkingsverantwoordelijke onverwijld in te lichten wanneer de verwerker ervan kennis heeft gekregen dat de gegevens die hij verwerkt onjuist of achterhaald zijn;
  - (4) de verplichtingen in artikel 32 van Verordening (EU) 2016/679.
- (d) De partijen stellen in bijlage III de passende technische en organisatorische maatregelen vast op grond waarvan de verwerker de verwerkingsverantwoordelijke bij de toepassing van deze bepaling moet bijstaan, alsmede de omvang en de omvang van de vereiste bijstand.

#### *Bepaling 9*

##### ***Kennisgeving van een inbreuk in verband met persoonsgegevens***

In het geval van een inbreuk in verband met persoonsgegevens werkt de verwerker samen met de verwerkingsverantwoordelijke en staat hij hem bij opdat de verwerkingsverantwoordelijke kan voldoen aan zijn verplichtingen uit hoofde van de artikelen 33 en 34 van Verordening (EU) 2016/679 of de artikelen 34 en 35 van Verordening (EU) 2018/1725, indien van toepassing, waarbij rekening wordt gehouden met de aard van de verwerking en de informatie waarover de verwerker beschikt.

##### **9.1. Inbreuk in verband met gegevens die door de verwerkingsverantwoordelijke worden verwerkt**

In geval van een inbreuk in verband met persoonsgegevens die door de verwerkingsverantwoordelijke worden verwerkt, staat de verwerker de verwerkingsverantwoordelijke bij:

- (a) bij het zonder onnodige vertraging melden van de inbreuk in verband met persoonsgegevens aan de bevoegde toezichthoudende autoriteit/autoriteiten nadat de verwerkingsverantwoordelijke er kennis van heeft gekregen, indien relevant / (tenzij het onwaarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen);
- (b) bij het verkrijgen van onderstaande informatie die overeenkomstig artikel 33, lid 3, van Verordening (EU) 2016/679 in de kennisgeving van de verwerkingsverantwoordelijke moet worden vermeld en ten minste omvat:
  - (1) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder

vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

- (2) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- (3) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Indien en voor zover al deze informatie niet op hetzelfde moment kan worden verstrekt, bevat de oorspronkelijke kennisgeving de dan beschikbare informatie en wordt verdere informatie vervolgens onverwijld verstrekt zodra deze beschikbaar is;

- (c) bij het naleven, overeenkomstig artikel 34 van Verordening (EU) 2016/679, van de verplichting om de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee te delen, wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

## **9.2. Inbreuk in verband met gegevens die door de verwerker worden verwerkt**

In geval van een inbreuk in verband met persoonsgegevens die door de verwerker worden verwerkt, stelt de verwerker, nadat hij kennis heeft gekregen van de inbreuk, de verwerkingsverantwoordelijke daarvan onverwijld in kennis. Deze kennisgeving bevat ten minste:

- (a) een beschrijving van de aard van de inbreuk (waar mogelijk onder vermelding van de categorieën betrokkenen en gegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en gegevensregisters in kwestie);
- (b) de gegevens van een contactpunt waar meer informatie over de inbreuk in verband met persoonsgegevens kan worden verkregen;
- (c) de waarschijnlijke gevolgen van de inbreuk en de maatregelen die zijn genomen of worden voorgesteld om deze aan te pakken, onder meer om de mogelijke negatieve gevolgen ervan te beperken.

Indien en voor zover al deze informatie niet op hetzelfde moment kan worden verstrekt, bevat de oorspronkelijke kennisgeving de dan beschikbare informatie en wordt verdere informatie vervolgens onverwijld verstrekt zodra deze beschikbaar is.

De partijen vermelden in bijlage III alle andere elementen die door de verwerker moeten worden verstrekt wanneer hij de verwerkingsverantwoordelijke bijstaat bij de naleving van de verplichtingen van de verwerkingsverantwoordelijke uit hoofde van de artikelen 33 en 34 van Verordening (EU) 2016/679.

## **AFDELING III - SLOTBEPALINGEN**

### *Bepaling 10*

#### ***Niet-naleving van de bepalingen en beëindiging***

- (a) Onverminderd eventuele bepalingen van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 kan de verwerkingsverantwoordelijke, ingeval de verwerker zijn verplichtingen uit hoofde van deze bepalingen niet nakomt, de verwerker opdracht geven

de verwerking van persoonsgegevens op te schorten totdat deze aan deze bepalingen voldoet of de Raamovereenkomst wordt beëindigd. Wanneer de verwerker om welke reden dan ook niet aan deze bepalingen kan voldoen, stelt hij de verwerkingsverantwoordelijke daarvan onverwijld in kennis.

- (b) De verwerkingsverantwoordelijke heeft het recht de Raamovereenkomst te beëindigen voor zover deze de verwerking van persoonsgegevens overeenkomstig deze bepalingen betreft, indien:
- (4) de verwerkingsverantwoordelijke de verwerking van persoonsgegevens door de verwerker overeenkomstig punt a) heeft opgeschort en de naleving van deze bepalingen niet binnen een redelijke termijn en in elk geval binnen één maand na de opschorting wordt hervat;
  - (5) de verwerker deze bepalingen of zijn verplichtingen uit hoofde van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 wezenlijk of voortdurend schendt;
  - (6) de verwerker niet voldoet aan een bindend besluit van een bevoegde rechter of de bevoegde toezichthoudende autoriteit/autoriteiten met betrekking tot zijn verplichtingen uit hoofde van deze bepalingen of Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.
- (c) De verwerker heeft het recht de Raamovereenkomst op te zeggen voor zover het daarbij gaat om de verwerking van persoonsgegevens krachtens deze bepalingen, indien de verwerkingsverantwoordelijke, nadat de verwerker hem er overeenkomstig bepaling 7.1, punt b), van in kennis heeft gesteld dat zijn instructies inbreuk maken op de toepasselijke wettelijke vereisten, aandringt op naleving van de instructies.
- (d) Na de beëindiging van de Raamovereenkomst wist de verwerker, naar keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens die namens de verwerkingsverantwoordelijke zijn verwerkt en bevestigt hij tegenover de verwerkingsverantwoordelijke dat hij dit heeft gedaan, of zendt hij alle persoonsgegevens terug aan de verwerkingsverantwoordelijke en verwijdert hij bestaande kopieën, tenzij het Unierecht of het lidstatelijke recht de opslag van de persoonsgegevens voorschrijft. Indien de verwerkingsverantwoordelijke niet binnen dertig (30) dagen na de beëindiging van de Raamovereenkomst heeft verzocht om teruggave van alle persoonsgegevens die ten behoeve van de verwerkingsverantwoordelijke zijn verwerkt, heeft de verwerker het recht de persoonsgegevens naar eigen goeddunken te wissen. Totdat de gegevens zijn gewist of teruggeven, blijft de verwerker ervoor zorgen dat deze bepalingen worden nageleefd.



## **BIJLAGE I LIJST VAN PARTIJEN**

### **Verwerkingsverantwoordelijk(n):**

1. *De Klant (zoals geïdentificeerd in de Raamovereenkomst of het Bestelformulier)*

### **Verwerker(s)**

1. *Glooko AB (zoals geïdentificeerd in de Raamovereenkomst)*

## **BIJLAGE II BESCHRIJVING VAN DE VERWERKING**

*Categorieën betrokkenen van wie persoonsgegevens worden verwerkt*

- Geautoriseerde Gebruikers
- Patiënten

*Categorieën verwerkte persoonsgegevens*

Voor Geautoriseerde Gebruikers

- Algemene informatie (naam)
- Contactinformatie (e-mailadres, telefoonnummer)
- Gebruiksinformatie (gebruikersnaam, wachtwoord, toegangsrechten, auditlogs)

Voor Patiënten

- Algemene informatie (naam, geboortedatum, geslacht)
- Contactgegevens (postadres, e-mailadres, telefoonnummer)
- Gebruiksinformatie (gebruikersnaam, wachtwoord)
- Gezondheidsinformatie (diabetestype, jaar van diagnose diabetes, geschatte partus, streefbereik, gewicht, lengte, behandelingen)
- Apparaatinformatie (insulinepomp, glucosemeter en insulinepen serienummer(s), doses, koolhydraten, instellingen, alarmen)

*Verwerkte gevoelige gegevens (indien van toepassing) en toegepaste beperkingen of waarborgen die ten volle rekening houden met de aard van de gegevens en de betrokken risico's, zoals strikte doelbinding, toegangsbeperkingen (met inbegrip van toegang voor enkel personeel dat een gespecialiseerde opleiding heeft gevolgd), het bijhouden van een register inzake de toegang tot de gegevens, beperkingen voor verdere doorgifte of aanvullende beveiligingsmaatregelen.*

- Gegevens betreffende de gezondheid

Voor informatie over de uitgevoerde waarborgen, zie bijlage III

*Aard van de verwerking*

Het verzamelen, analyseren, visualiseren en anderszins verwerken van de persoonsgegevens in overeenstemming met de Raamovereenkomst.

*Doeleinde(n) waarvoor de persoonsgegevens namens de verwerkingsverantwoordelijke worden verwerkt*

Om de verwerkingsverantwoordelijke en zijn Geautoriseerde Gebruikers in staat te stellen de Software en andere Prestaties te gebruiken in overeenstemming met de Raamovereenkomst.

*Duur van de verwerking*

Voor de duur van de terbeschikkingstelling van de Software en andere Prestaties volgens de Raamovereenkomst.

*Voor verwerking door (sub)verwerkers, ook het voorwerp, de aard en de duur van de verwerking vermelden.*

Zie Bijlage IV

*Instructies in het kader van punt 7.8, onder a), van de clausules inzake internationale doorgiften*

De standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen in Bijlage V zijn van toepassing indien de verwerker persoonsgegevens doorgeeft buiten de Europese Economische Ruimte (“**EER**”), naar een land dat door de Europese Commissie niet is erkend als een land dat een passend niveau voor de bescherming van persoonsgegevens biedt.

### **BIJLAGE III TECHNISCHE EN ORGANISATORISCHE MAATREGELEN, MET INBEGRIJ VAN TECHNISCHE EN ORGANISATORISCHE MAATREGELEN OM DE BEVEILIGING VAN DE GEGEVENS TE WAARBORGEN**

1. Doel. Deze bijlage beschrijft het beveiligingsprogramma, de beveiligingscertificeringen en de technische en organisatorische maatregelen van Glooko om (a) persoonsgegevens die door de verwerker namens de verwerkingsverantwoordelijke worden verwerkt, te beschermen tegen ongeoorloofd gebruik, ongeoorloofde toegang, openbaarmaking of diefstal en (b) de Software. Naarmate veiligheidsrisico's veranderen en evolueren, blijft Glooko zijn beveiligingsprogramma en -strategie bijwerken om persoonsgegevens en de Software te beschermen. Glooko behoudt zich het recht voor om deze Bijlage van tijd tot tijd bij te werken; op voorwaarde echter dat een eventuele wijziging de algemene bescherming zoals uiteengezet in deze Bijlage niet wezenlijk zal verminderen.
2. Beveiligingsorganisatie en -programma. Glooko heeft een beveiligingsprogramma op basis van risicobeoordeling. Het kader voor het beveiligingsprogramma van Glooko omvat administratieve, organisatorische, technische en fysieke veiligheidsmaatregelen die redelijkerwijs zijn ontworpen om de Software en de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens te beschermen. Het beveiligingsprogramma van beoogt passend te zijn voor de aard van de Software en de omvang en complexiteit van de bedrijfsactiviteiten van Glooko. Glooko heeft een afzonderlijk team toegewijd aan informatiebeveiliging dat het beveiligingsprogramma van Glooko beheert. Dit team faciliteert en ondersteunt onafhankelijke audits en beoordelingen die door derden worden uitgevoerd. Glooko's beveiligingsraamwerk omvat programma's die betrekking hebben op: Beleid en Procedures, Activabeheer, Toegangsbeheer, Cryptografie, Fysieke Beveiliging, Operationele Beveiliging, Communicatiebeveiliging, Bedrijfscontinuïteitsbeveiliging, Beveiligingsmaatregelen omtrent Werknemers, Productbeveiliging, Beveiliging van Cloud- en Netwerkinfrastructuur, Beveiliging Compliance, Beveiliging van Derden, Vulnerability Management, en Beveiligingsmonitoring en Incidentrespons. Beveiliging wordt op het hoogste niveau van het bedrijf beheerd, waarbij de Security Officer van Glooko regelmatig met het uitvoerend management vergadert om problemen te bespreken en beveiligingsinitiatieven voor het hele bedrijf te coördineren. Het informatiebeveiligingsbeleid en de standaarden worden minstens jaarlijks herzien en goedgekeurd door het management en zijn beschikbaar voor alle werknemers van Glooko, zodat zij deze kunnen raadplegen.
3. Vertrouwelijkheid. Glooko heeft controle-instrumenten geïmplementeerd om de vertrouwelijkheid van persoonsgegevens te handhaven in overeenstemming met de Raamovereenkomst. Alle werknemers en ingehuurd personeel van Glooko zijn gebonden aan het interne beleid van Glooko met betrekking tot het handhaven van de vertrouwelijkheid van persoonsgegevens en zijn contractueel verplicht om deze verplichtingen na te leven.
4. Beveiligingsmaatregelen omtrent werknemers
  - a. Achtergrondcontroles van werknemers. Glooko voert achtergrondcontroles uit op alle nieuwe werknemers op het moment van werving, in overeenstemming met de toepasselijke lokale wetgeving. Glooko controleert momenteel de opleiding en eerdere banen van een nieuwe werknemer en voert referentiechecks uit. Indien toegestaan door de toepasselijke wetgeving, kan Glooko ook strafrechtelijke, krediet-, immigratie- en veiligheidscontroles uitvoeren, afhankelijk van de aard en de reikwijdte van de functie van een nieuwe werknemer.
  - b. Opleiding van werknemers. Ten minste één (1) keer per jaar moeten alle

medewerkers van Glooko een beveiligings- en privacytraining volgen die het beveiligingsbeleid van Glooko, de beste beveiligingspraktijken en de privacybeginselen behandelt. Werknemers die met verlof zijn, kunnen extra tijd krijgen om deze jaarlijkse training te voltooien. Glooko's aan beveiliging toegewijde team voert ook phishing bewustwordingscampagnes uit en communiceert opkomende bedreigingen aan de werknemers.

5. Beheer van derden-leveranciers

- a. Leveranciersbeoordeling. Glooko kan externe leveranciers gebruiken om de Software te leveren. Glooko voert een op beveiligingsrisico's gebaseerde beoordeling van potentiële leveranciers uit alvorens met hen samen te werken om te valideren of zij aan de beveiligingsvereisten van Glooko voldoen. Glooko beoordeelt periodiek elke leverancier in het licht van de beveiligings- en bedrijfscontinuïteitsnormen van Glooko, met inbegrip van het soort toegang en de classificatie van gegevens waartoe toegang wordt verkregen (indien van toepassing), maatregelen die nodig zijn om gegevens te beschermen, en wettelijke/reglementaire vereisten. Glooko zorgt ervoor dat persoonsgegevens worden geretourneerd en/of verwijderd aan het einde van een leveranciersrelatie.
- b. Leveranciersovereenkomsten. Glooko sluit schriftelijke overeenkomsten met al haar leveranciers die vertrouwelijkheids-, privacy- en beveiligingsverplichtingen bevatten die een passend niveau van bescherming bieden voor de persoonsgegevens die deze leveranciers kunnen verwerken.

6. Architectuur, firewalls en scheiding van gegevens. Alle netwerktoegang tussen productiehosts wordt beperkt, waarbij firewalls worden gebruikt om alleen geautoriseerde diensten interactie in het productienetwerk toe te staan. Firewalls worden gebruikt om de netwerksegregatie tussen verschillende beveiligingszones in de productie- en bedrijfsomgevingen te beheren. Glooko scheidt zijn databases op logische wijze. De Glooko API's zijn ontworpen en gebouwd om alleen toegang van en naar de respectievelijke afzenders te identificeren en toe te staan. Deze controles voorkomen dat klanten toegang hebben tot gegevens van andere klanten.

7. Fysieke beveiliging. De datacenters waar de Software wordt gehost, worden zowel aan de terreingrenzen als bij de ingangen van het gebouw streng gecontroleerd door professioneel beveiligingspersoneel dat gebruik maakt van videobewaking, inbraakdetectiesystemen en andere elektronische middelen. Ononderbroken stroomvoorzieningen en on-site generatoren zijn beschikbaar om back-up stroom te leveren in het geval van een stroomstoring. Bovendien hebben het hoofdkantoor en de kantoorruimten van Glooko een fysiek beveiligingsprogramma dat bezoekers, ingangen en algemene kantoorbeveiliging beheert.

8. Beveiliging door ontwerp. Glooko volgt de principes van beveiliging door ontwerp wanneer het de Software ontwerpt. Glooko past ook de Glooko Software Development Lifecycle (SDLC) standaard toe om talrijke activiteiten gerelateerd aan beveiliging voor de Software uit te voeren in de verschillende fasen van de productcreatie levenscyclus, van het verzamelen van de vereisten en het productontwerp tot de uitrol van het product.

9. Toegang controlemaatregelen

- a. Toegang verlenen. Om het risico op blootstelling aan gegevens te minimaliseren, volgt Glooko de principes van de minste privileges door middel van een toegangscontrolemodel op teambasis bij het verlenen van toegang tot het

systeem. Personeel van Glooko heeft toegang tot persoonsgegevens op basis van hun functie, rol en verantwoordelijkheden, en dergelijke toegang moet worden goedgekeurd door de manager van de werknemer. De toegang van een werknemer tot persoonsgegevens wordt verwijderd bij beëindiging van het dienstverband. Voordat een ingenieur toegang krijgt tot de productieomgeving, moet de toegang worden goedgekeurd door het management en de ingenieur is verplicht om interne trainingen te voltooien voor dergelijke toegang, waaronder trainingen over de systemen van het betreffende team. Glooko logt hoog risico acties en veranderingen in de productie omgeving. Glooko maakt gebruik van automatische systemen om elke afwijking van interne technische standaarden te identificeren die zou kunnen duiden op afwijkende/ongeautoriseerde activiteit om binnen enkele minuten na een configuratiewijziging een waarschuwing te geven.

- b. Wachtwoord controle. Wanneer een Geautoriseerde Gebruiker inlogt op zijn account, heeft Glooko de inloggegevens van de gebruiker voordat deze worden opgeslagen. Klanten kunnen ook eisen dat de Geautoriseerde Gebruikers een extra beveiligingslaag toevoegen aan hun account door gebruik te maken van twee-factor authenticatie (2FA).
10. Change management. Glooko heeft een formeel proces voor change management dat wordt gevolgd om wijzigingen in de productieomgeving voor de Software te beheren, met inbegrip van wijzigingen in de onderliggende software, toepassingen en systemen. Elke wijziging wordt zorgvuldig herzien en geëvalueerd in een testomgeving alvorens te worden geïmplementeerd in de productieomgeving voor de Software. Alle wijzigingen, inclusief de evaluatie van de wijzigingen in een testomgeving, worden gedocumenteerd met behulp van een formeel, controleerbaar registratiesysteem. Voor wijzigingen met een hoog risico is goedkeuring vereist van de juiste organisatorische belanghebbenden. Er worden ook plannen en procedures geïmplementeerd voor het geval een doorgevoerde wijziging moet worden teruggedraaid om de beveiliging van de Software te waarborgen.
11. Encryptie. Voor de Software geldt dat (a) de databases waarin persoonsgegevens worden opgeslagen, worden versleuteld met behulp van de Advanced Encryption Standard en (b) persoonsgegevens worden versleuteld bij de doorgifte tussen de softwaretoepassing van de Klant en de Software met behulp van TLS v1.2
12. Vulnerability management. Glooko handhaaft controles en beleidslijnen ter beperking van het risico van kwetsbaarheden in de beveiliging om een evenwicht te vinden tussen risico en de bedrijfs-/operationele vereisten. Glooko gebruikt een tool van een derde partij om regelmatig kwetsbaarheidsscans uit te voeren om de kwetsbaarheden in Glooko's cloudinfrastructuur en bedrijfssystemen te beoordelen.
13. Penetratietesten. Glooko voert penetratietesten uit en doet een beroep op onafhankelijke derde partijen om penetratietesten op applicatieniveau uit te voeren. Gedetecteerde beveiligingsbedreigingen en kwetsbaarheden worden geprioriteerd, getriaged en verholpen.
14. Beheer van beveiligingsincidenten. Glooko heeft een beleid voor het beheer van beveiligingsincidenten. Glooko's Security Incident Response Team (T-SIRT) beoordeelt alle relevante beveiligingsbedreigingen en kwetsbaarheden en stelt gepaste herstel- en beperkingsacties op. Glooko bewaart zijn relevante beveiligingslogboeken.
15. Weerbaarheid en continuïteit van de software. De Software maakt gebruik van een verscheidenheid aan hulpmiddelen en mechanismen om een hoge beschikbaarheid en

weerbaarheid te bereiken. Voor de Software strekt de infrastructuur van Glooko zich uit over meerdere onafhankelijk beschikbare zones in verschillende geografische regio's die fysiek van elkaar gescheiden zijn. Glooko maakt ook gebruik van gespecialiseerde tools die de serverprestaties, gegevens en verkeersbelasting binnen elke beschikbaarheidszone en colocation-datacenter bewaken. Als suboptimale serverprestaties of overbelaste capaciteit wordt gedetecteerd op een server binnen een beschikbaarheidszone of colocation datacenter, verhogen deze gespecialiseerde tools de capaciteit of verschuiven ze het verkeer om de suboptimale serverprestaties of overbelaste capaciteit te verlichten. Glooko wordt ook onmiddellijk op de hoogte gebracht in het geval van suboptimale serverprestaties of overbelaste capaciteit.

16. Back-ups en herstel. Glooko maakt regelmatig back-ups van persoonsgegevens. Persoonsgegevens waarvan een back-up wordt gemaakt, worden overvloedig bewaard in meerdere beschikbaarheidszones en versleuteld tijdens het transport en in rust met behulp van Advanced Encryption Standards.

#### **BIJLAGE IV LIJST VAN SUBVERWERKERS**

De verwerkingsverantwoordelijke heeft toestemming gegeven voor uitbesteding aan de volgende subverwerkers:

1. Naam: Amazon Web Services EMEA

SARL adres: 38 Avenue John F. Kennedy, L-1855, Luxemburg

*Beschrijving van de verwerking (met inbegrip van een duidelijke afbakening van de verantwoordelijkheden ingeval er toestemming is voor uitbesteding aan meerdere subverwerkers):*

Cloud dienstverlener

2 . Naam: Cegedim SA

Adres: 137 rue d'Aguesseau, 92100 Boulogne-Billancourt, Frankrijk

Beschrijving van de verwerking (met inbegrip van een duidelijke afbakening van de verantwoordelijkheden ingeval er toestemming is voor uitbesteding aan meerdere subverwerkers):  
Cloud dienstverlener (kan gebruikt worden voor Klanten die zich in Frankrijk bevinden)

3 . Naam: Pictime Groupe

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

Beschrijving van de verwerking (met inbegrip van een duidelijke afbakening van de verantwoordelijkheden ingeval er toestemming is voor uitbesteding aan meerdere subverwerkers):  
gecertificeerde host voor gezondheidsgegevens (kan gebruikt worden voor Klanten die zich in Frankrijk en Duitsland bevinden)



**BIJLAGE V: STANDAARDCONTRACTBEPALINGEN VOOR DE DOORGIFTE VAN PERSOONSGEGEVENS  
NAAR DERDE LANDEN**

*Bepaling 1*

***Doel en toepassingsgebied***

- (a) Deze standaardcontractbepalingen hebben tot doel de naleving van de in Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (AVG, algemene verordening gegevensbescherming) <sup>1</sup> bepaalde vereisten te garanderen voor de doorgifte van persoonsgegevens naar een derde land.
- (b) De partijen:
- (i) de natuurlijke of rechtspersonen en de overheidsinstellingen, -organen en -instanties (hierna “entiteiten” genoemd) die de in bijlage I.A bedoelde persoonsgegevens doorgeven (“gegevensexporteur”); en
  - (ii) de entiteiten in een derde land die de persoonsgegevens van de gegevensexporteur ontvangen, direct of indirect via een andere entiteit die ook partij is bij deze bepalingen, zoals opgenomen in bijlage I.A (hierna “gegevensimporteur” genoemd)
- zijn deze standaardcontractbepalingen (hierna: “bepalingen” genoemd) overeengekomen.
- (c) Deze bepalingen zijn van toepassing op de doorgifte van persoonsgegevens zoals opgenomen in bijlage Annex I.B.
- (d) Het aanhangsel bij deze bepalingen dat de daarin genoemde bijlagen bevat, maakt integraal deel uit van deze bepalingen.

*Bepaling 2*

***Effect en onveranderlijkheid van de bepalingen***

- (a) In deze bepalingen worden passende waarborgen vastgesteld, met inbegrip van afdwingbare rechten van betrokkenen en doeltreffende rechtsmiddelen, overeenkomstig artikel 46, lid 1, en artikel 46, lid 2, punt c), van Verordening (EU) 2016/679 alsook, met

---

<sup>1</sup> Wanneer de gegevensexporteur een onder Verordening (EU) 2016/679 vallende verwerker is die namens een instelling of orgaan van de Unie optreedt als verwerkingsverantwoordelijke, garandeert de toepassing van deze bepalingen bij het in dienst nemen van een andere verwerker (subverwerker) die niet onder Verordening (EU) 2016/679 valt ook de naleving van artikel 29, lid 4, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39), voor zover deze bepalingen en de verplichtingen inzake gegevensbescherming zoals opgenomen in de overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker overeenkomstig artikel 29, lid 3, van Verordening (EU) 2018/1725 op één lijn zijn gebracht. Dat is met name het geval wanneer de verwerkingsverantwoordelijke en de verwerker zich baseren op de in Besluit [...] opgenomen standaardcontractbepalingen.

betrekking tot gegevensdoorgiften van verwerkingsverantwoordelijken aan verwerkers en/of van verwerkers aan verwerkers, standaardcontractbepalingen overeenkomstig artikel 28, lid 7, van Verordening (EU) 2016/679, mits deze niet worden gewijzigd, behalve om de geschikte module(s) te selecteren of om informatie in het aanhangsel toe te voegen of te wijzigen. Dit houdt niet in dat de partijen de in deze bepalingen neergelegde standaardcontractbepalingen niet in een bredere overeenkomst mogen opnemen en/of andere bepalingen of extra waarborgen mogen toevoegen, mits deze niet direct of indirect in tegenspraak zijn met deze bepalingen en geen afbreuk doen aan de grondrechten of de fundamentele vrijheden van de betrokkenen.

- (b) Deze bepalingen doen geen afbreuk aan de krachtens Verordening (EU) 2016/679 op de gegevensexporteur rustende verplichtingen.

### *Bepaling 3*

#### ***Derde-begunstigden***

- (a) Betrokkenen mogen zich als derde-begunstigden op deze bepalingen beroepen en deze doen gelden tegen de gegevensexporteur en/of de gegevensimporteur, met de volgende uitzonderingen:

- (i) Bepaling 1, bepaling 2, bepaling 3, bepaling 6, bepaling 7;
- (ii) Bepaling 8 - module een: Bepaling 8.5, punt e) en bepaling 8.9, punt b); Module twee: Bepaling 8.1, punt b), bepaling 8.9, punten a), c), d) en e); Module drie: Bepaling 8.1, punten a), c) en d) en bepaling 8.9, punten a), c), d), e), f) en g); Module vier: Bepaling 8.1, punt b) en bepaling 8.3, punt b);
- (iii) Bepaling 9 - module twee: Bepaling 9, punten a), c), d) en e); Module drie: Bepaling 9, punten a), c), d) en e);
- (iv) Bepaling 12 - module een: Bepaling 12, punten a) en d); Modulen twee en drie: Bepaling 12, punten a), d) en f);
- (v) Bepaling 13;
- (vi) Bepaling 15.1, punten c), d) en e);
- (vii) Bepaling 16, punt e);
- (viii) Bepaling 18 - modulen een, twee en drie: Bepaling 18, punten a) en b); Module vier: Clause 18.

- (b) Punt a) doet geen afbreuk aan de rechten van betrokkenen krachtens Verordening (EU) 2016/679.

### *Bepaling 4*

#### ***Interpretatie***

- (a) Wanneer in deze bepalingen in Verordening (EU) 2016/679 gedefinieerde termen worden gebruikt, hebben die termen dezelfde betekenis als in die verordening.
- (b) Deze bepalingen worden gelezen en geïnterpreteerd in het licht van de bepalingen van Verordening (EU) 2016/679.
- (c) Deze bepalingen worden niet geïnterpreteerd op een wijze die in tegenspraak is met de in Verordening (EU) 2016/679 vastgestelde rechten en verplichtingen.

#### *Bepaling 5*

##### ***Hiërarchie***

In geval van tegenspraak tussen deze bepalingen en de bepalingen van aanverwante overeenkomsten tussen de partijen die bestonden ten tijde van het overeenkomen van deze bepalingen of die daarna werden gesloten, hebben deze bepalingen voorrang.

#### *Clause 6*

##### ***Beschrijving van de doorgifte(n)***

De details van de doorgifte(n), en in het bijzonder de categorieën van persoonsgegevens die worden doorgegeven en het doel waarvoor zij worden doorgegeven, worden in bijlage I.B nader gespecificeerd.

#### *Bepaling 7 - Facultatief*

##### ***Docking-bepaling***

*Niet van toepassing*

## **AFDELING II – VERPLICHTINGEN VAN DE PARTIJEN**

#### *Bepaling 8*

##### ***Waarborgen inzake gegevensbescherming***

De gegevensexporteur garandeert dat hij redelijke inspanningen heeft geleverd om te bepalen of de gegevensimporteur, door de uitvoering van passende technische en organisatorische maatregelen, in staat is zijn verplichtingen uit hoofde van deze bepalingen na te komen.

### **8.1 Instructies**

- (a) De gegevensexporteur verwerkt de persoonsgegevens uitsluitend op basis van schriftelijke instructies van de gegevensimporteur die als zijn verwerkingsverantwoordelijke optreedt.

- (b) De gegevensexporteur brengt de gegevensimporteur onmiddellijk op de hoogte indien hij niet in staat is die instructies op te volgen, onder meer als die instructies in tegenspraak zijn met Verordening (EU) 2016/679 of andere wetgeving inzake gegevensbescherming van de Unie of de desbetreffende lidstaat.
- (c) De gegevensimporteur onthoudt zich van acties die de gegevensexporteur zouden verhinderen om zijn verplichtingen op grond van Verordening (EU) 2016/679 na te komen, ook in het kader van de indienstneming van een andere verwerker of met betrekking tot samenwerking met bevoegde toezichthoudende autoriteiten.
- (d) Na afloop van de verrichting van de verwerkingsdiensten wist de gegevensexporteur, naargelang de wens van de gegevensimporteur, alle namens de gegevensimporteur verwerkte persoonsgegevens en verzekert hij de gegevensimporteur ervan dat hij dat heeft gedaan, of geeft hij de gegevensimporteur alle namens hem verwerkte persoonsgegevens terug en verwijdert hij bestaande kopieën.

## **8.2 Beveiliging van de verwerking**

- (a) De partijen nemen passende technische en organisatorische maatregelen om de beveiliging van de gegevens te waarborgen, ook tijdens de toezending en met inbegrip van bescherming tegen een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking of toegang (hierna “inbreuk in verband met persoonsgegevens” genoemd). Bij het beoordelen van het passende beveiligingsniveau houden zij naar behoren rekening met de stand van de techniek, de uitvoeringskosten, de aard van de persoonsgegevens<sup>2</sup>, de aard, reikwijdte, context en doeleinden van de verwerking, en met de risico’s die de verwerking met zich meebrengt voor de betrokkenen, en nemen zij in het bijzonder het gebruik van versleuteling of pseudonimisering in overweging, onder andere tijdens de toezending, indien het doel van de verwerking op die manier kan worden verwezenlijkt.
- (b) De gegevensexporteur verleent bijstand aan de gegevensimporteur om passende beveiliging van de gegevens overeenkomstig punt a) te waarborgen. Bij een inbreuk in verband met persoonsgegevens met betrekking tot de krachtens deze bepalingen door de gegevensexporteur verwerkte persoonsgegevens, stelt de gegevensexporteur de gegevensimporteur onverwijld in kennis nadat hij er kennis van heeft genomen, en staat hij de gegevensimporteur bij met het aanpakken van de inbreuk.
- (c) De gegevensexporteur waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

## **8.3 Documentatie en naleving**

- (a) De partijen moeten de naleving van deze bepalingen kunnen aantonen.

---

<sup>2</sup> Hieronder valt ook de vraag of de doorgifte en verdere verwerking persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens of biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten omvatten.

- (b) De gegevensexporteur stelt de gegevensimporteur alle informatie ter beschikking die nodig is om de naleving van zijn verplichtingen uit hoofde van deze bepalingen aan te tonen en om audits mogelijk te maken en eraan bij te dragen.

#### *Bepaling 9*

##### **Gebruik van subverwerkers**

*Niet van toepassing*

#### *Bepaling 10*

##### **De rechten van betrokkenen**

De partijen staan elkaar bij met het beantwoorden van vragen en het afhandelen van verzoeken van betrokkenen op grond van het lokale recht dat op de gegevensimporteur van toepassing is of, voor gegevensverwerking door de gegevensexporteur in de Europese Unie, op grond van Verordening (EU) 2016/679.

#### *Bepaling 11*

##### **Verhaal**

- (a) De gegevensimporteur brengt betrokkenen via een individuele mededeling of op zijn website, in een transparant en gemakkelijk toegankelijk formaat, op de hoogte van een contactpunt dat gemachtigd is om klachten af te handelen. Hij handelt klachten die hij van een betrokkene ontvangt onverwijld af.

#### *Bepaling 12*

##### **Aansprakelijkheid**

- (a) Elke partij is ten aanzien van de andere partij(en) aansprakelijk voor schade die hij de andere partij(en) berokkent door inbreuken op deze bepalingen.
- (b) Elke partij is ten aanzien van de betrokkene aansprakelijk, en de betrokkene heeft het recht een vergoeding te verkrijgen, voor materiële of immateriële schade die de partij aan de betrokkene berokkent door de rechten ten behoeve van derden uit hoofde van deze bepalingen te schenden. Dit doet geen afbreuk aan de aansprakelijkheid van de gegevensexporteur op grond van Verordening (EU) 2016/679.
- (c) Wanneer meerdere partijen verantwoordelijk zijn voor schade die als gevolg van schendingen van deze bepalingen aan de betrokkene is berokkend, zijn alle verantwoordelijke partijen hoofdelijk aansprakelijk en heeft de betrokkene het recht om voor de rechter een procedure tegen deze partijen in te stellen.

- (d) De partijen komen overeen dat als een van de partijen op grond van punt c) aansprakelijk wordt gesteld, deze partij het recht heeft om op de andere partij(en) het deel van de schadevergoeding te verhalen dat overeenkomt met zijn/hun deel van de aansprakelijkheid voor de schade.
- (e) De gegevensimporteur mag zich niet op het gedrag van een verwerker of subverwerker beroepen om zich aan zijn eigen aansprakelijkheid te onttrekken.

*Bepaling 13*

***Toezicht***

*Niet van toepassing*

**AFDELING III – LOKALE WETTEN EN VERPLICHTINGEN IN GEVAL VAN TOEGANG DOOR OVERHEIDSINSTANTIES**

*Bepaling 14*

***Lokale wetten en praktijken met gevolgen voor de naleving van de bepalingen***

*Niet van toepassing*

*Bepaling 15*

***Verplichtingen van de gegevensimporteur in geval van toegang door overheidsinstanties***

*Niet van toepassing*

**AFDELING IV — SLOTBEPALINGEN**

*Bepaling 16*

***Niet-naleving van de bepalingen en beëindiging***

- (a) De gegevensimporteur stelt de gegevensexporteur onverwijld in kennis indien hij om wat voor reden dan ook niet in staat is deze bepalingen na te leven.
- (b) Indien de gegevensimporteur inbreuk maakt op deze bepalingen of niet in staat is deze bepalingen na te leven, schort de gegevensexporteur de doorgifte van persoonsgegevens aan de gegevensimporteur op totdat de naleving weer wordt gewaarborgd of totdat de overeenkomst wordt beëindigd. Dit doet geen afbreuk aan bepaling 14, punt f).

- (c) De gegevensexporteur heeft het recht de overeenkomst te beëindigen, voor zover die betrekking heeft op de verwerking van persoonsgegevens uit hoofde van deze bepalingen, wanneer:
- (i) de gegevensexporteur de doorgifte van persoonsgegevens naar de gegevensimporteur overeenkomstig punt b) heeft opgeschort en de bepalingen niet binnen een redelijke termijn en in elk geval binnen één maand na de opschorting weer worden nageleefd;
  - (ii) de gegevensimporteur in belangrijke en voortdurende mate inbreuk maakt op deze bepalingen; of
  - (iii) de gegevensimporteur zich niet aan een bindend besluit van een bevoegd gerecht of een bevoegde autoriteit met betrekking tot zijn verplichtingen uit hoofde van deze bepalingen houdt.

In deze gevallen stelt hij de bevoegde toezichthoudende autoriteit in kennis van die niet-naleving. Wanneer meer dan twee partijen bij de overeenkomst zijn betrokken, mag de gegevensexporteur zijn recht om de overeenkomst te beëindigen alleen uitoefenen met betrekking tot de betrokken partij, tenzij anderszins door de partijen is overeengekomen.

- (d) Door de gegevensexporteur in de Europese Unie verzamelde persoonsgegevens die voordat de overeenkomst werd beëindigd waren doorgegeven overeenkomstig punt c) worden onmiddellijk volledig gewist, met inbegrip van eventuele kopieën daarvan. De gegevensimporteur verzekert de gegevensexporteur ervan dat de gegevens zijn gewist. Totdat de gegevens zijn gewist of teruggezonden, blijft de gegevensimporteur ervoor zorgen dat aan deze bepalingen wordt voldaan. In geval van lokaal recht dat op de gegevensimporteur van toepassing is en op basis waarvan teruggave of wissing van de doorgegeven persoonsgegevens verboden is, garandeert de gegevensimporteur dat hij deze bepalingen zal blijven naleven en de gegevens alleen zal verwerken voor zover en zolang dat naar dat lokaal recht is vereist.
- (e) Elk van de partijen kan haar toestemming om aan deze bepalingen gebonden te zijn, intrekken wanneer (i) de Europese Commissie een besluit overeenkomstig artikel 45, lid 3, van Verordening (EU) 2016/679 neemt dat betrekking heeft op de doorgifte van persoonsgegevens waarop deze bepalingen van toepassing zijn; of (ii) Verordening (EU) 2016/679 onderdeel wordt van het rechtskader van het land waarnaar de persoonsgegevens worden doorgegeven. Dit doet geen afbreuk aan andere verplichtingen die van toepassing zijn op de desbetreffende verwerking op grond van Verordening (EU) 2016/679.

#### *Bepaling 17*

#### **Toepasselijk recht**

Deze bepalingen worden geregeld door het recht van een land dat rechten ten behoeve van derden toestaat. De partijen komen overeen dat dit het recht van het land zoals gespecificeerd in de Raamovereenkomst is.

*Bepaling 18*

***Forum- en jurisdictiekeuze***

Uit deze bepalingen voortvloeiende geschillen worden beslecht door de gerechten van het land zoals gespecificeerd in de Raamovereenkomst.



## AANHANGSEL

### BIJLAGE I

#### **A. LIJST VAN PARTIJEN**

**Gegevensexporteur(s):** *[Identiteit en contactgegevens van de gegevensexporteur(s) en, in voorkomend geval, van zijn/hun functionaris voor gegevensbescherming en/of de vertegenwoordiger in de Europese Unie]*

1. Naam: De Glooko entiteit zoals gespecificeerd in de Raamovereenkomst

Adres: Zoals gespecificeerd in de Raamovereenkomst

Naam, functie en contactgegevens van de contactpersoon: Jesper Forster, functionaris voor gegevensbescherming. Glooko AB, Nellickevägen 20B412 63 Gothenburg, Zweden. Email: dpo@glooko.com

Activiteiten in verband met de overeenkomstig deze bepalingen doorgegeven gegevens: Het leveren van de Prestaties zoals gespecificeerd in het toepasselijke Bestelformulier.

Handtekening en datum: Zoals gespecificeerd in het toepasselijke Bestelformulier in overeenstemming met de Raamovereenkomst

Rol (verwerkingsverantwoordelijke/verwerker): Verwerker

**Gegevensimporteur(s):** *[Identiteit en contactgegevens van de gegevensimporteur(s), met inbegrip van eventuele contactpersonen die verantwoordelijk zijn voor gegevensbescherming]*

1. Naam: Klant (zoals gespecificeerd in het toepasselijke Bestelformulier)

Adres: Adres van de Klant (zoals gespecificeerd in het toepasselijke Bestelformulier)

Naam, functie en contactgegevens van de contactpersoon: Adres van de Klant (zoals gespecificeerd in het toepasselijke Bestelformulier)

Activiteiten in verband met de overeenkomstig deze bepalingen doorgegeven gegevens: Ontvangst van de Prestaties zoals gespecificeerd in het toepasselijke Bestelformulier

Handtekening en datum: Zoals gespecificeerd in het toepasselijke Bestelformulier in overeenstemming met de Raamovereenkomst

Rol (verwerkingsverantwoordelijke/verwerker): Verwerkingsverantwoordelijke

#### **B. BESCHRIJVING VAN DOORGIFTE**

*Categorieën van betrokkenen wier persoonsgegevens worden doorgegeven*

- Geautoriseerde Gebruikers van de Klant

- Patiënten

### *Categorieën van doorgegeven persoonsgegevens*

#### Geautoriseerde Gebruikers van de Klant

- Algemene informatie (naam)
- Contactgegevens (e-mail adres, telefoonnummer)
- Gebruiksgegevens (gebruikersnaam, wachtwoord, toegangsrechten, audit logs)

#### Patiënten

- Algemene informatie (naam, geboortedatum, geslacht)
- Contactgegevens (adres, e-mail adres, telefoonnummer)
- Gebruiksgegevens (gebruikersnaam, wachtwoord)
- Gezondheidsgegevens (diabetes type, jaar van diabetes diagnose, geschatte bevallingsdatum, streefbereik, gewicht, lengte, behandelingen)
- Apparaatinformatie (insulinepomp, glucosemeter en insulinepen serienummer(s), doses, koolhydraten, instellingen, alarmen)

*Gevoelige gegevens die worden doorgegeven (indien van toepassing) en toegepaste beperkingen of waarborgen waarmee ten volle rekening wordt gehouden met de aard van de gegevens en de bijbehorende risico's, zoals strikte beperking van het doel, toegangsbeperkingen (waaronder uitsluitend toegang voor personeelsleden die een gespecialiseerde opleiding hebben gevolgd), het in een register bijhouden van toegang tot de gegevens, beperkingen voor verdere doorgiften, of bijkomende beveiligingsmaatregelen.*

- Gezondheidsgegevens (diabetes type, jaar van diabetes diagnose, geschatte bevallingsdatum, streefbereik, gewicht, lengte, behandelingen)

Toegangsbeperkingen voor personeel op een "need-to-know"-basis (voor zowel de verwerker als de verwerkingsverantwoordelijke)

Registratie van toegang tot de gegevens

Versleuteling van de gegevens in doorvoer en in rust

*De frequentie van de doorgifte (bv. of de gegevens eenmalig of continu worden doorgegeven).*

De persoonsgegevens worden opgeslagen door de verwerker, maar kunnen te allen tijde worden geraadpleegd door de verwerkingsverantwoordelijke (indien bijvoorbeeld de te leveren Prestaties bestaan uit software als een dienst). In die gevallen kunnen de persoonsgegevens worden geacht te zijn doorgegeven van de EER naar een derde land.

*Aard van de verwerking*

Het maken van berekeningen op basis van persoonsgegevens, uploaden, analyseren, visualiseren, doorgeven en anderszins verwerken van persoonsgegevens om Geautoriseerde Gebruikers in staat te stellen de Prestaties te gebruiken.

*Doeleind(en) van de gegevensdoorgifte en verdere verwerking*

Het doel van de gegevensoverdracht is om de Klant in staat te stellen de Prestaties te gebruiken.

*De periode gedurende welke de persoonsgegevens zullen worden bewaard, of indien dat niet mogelijk is, de criteria om die termijn te bepalen*

De Verwerking is niet beperkt in tijd en wordt uitgevoerd zolang de Prestaties worden geleverd of totdat de toepasselijke gegevensverwerkingsovereenkomst wordt beëindigd.

*Voor doorgiften aan (sub-)verwerkers ook het onderwerp, de aard en de duur van de verwerking opgeven*

Niet van toepassing.

### **C. BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT**

*De bevoegde toezichhoudende autoriteiten identificeren in overeenstemming met bepaling 13*

Niet van toepassing.

### **BIJLAGE II - TECHNISCHE EN ORGANISATORISCHE MAATREGELEN WAARONDER TECHNISCHE EN ORGANISATORISCHE MAATREGELEN OM DE BEVEILIGING VAN DE GEGEVENS TE WAARBORGEN**

Niet van toepassing.

### **BIJLAGE III – LIJST VAN SUBVERWERKERS**

Niet van toepassing.