GLOOKO Standardvertragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten sofern die Voraussetzungen des Rahmenvertrags erfüllt sind sowie für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a)Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b)Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II

PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden

Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens dreißig (30) Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart, soweit möglich, mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter wird die betroffene Personen darauf verweisen, den Verantwortlichen zu kontaktieren, sofern der Auftragsverarbeiter einen Antrag von einer betroffenen Person erhält. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der

Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Rahmenvertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Rahmenvertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Rahmenvertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom

Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Rahmenvertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Sofern der Verantwortliche nicht innerhalb von dreißig (30) Tagen nach Beendigung des Rahmenvertrags verlangt hat, dass die im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten zurückgegeben werden, ist der Auftragsverarbeiter in seinem alleinigen Ermessen berechtigt, die personenbezogenen Daten zu löschen. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I

Liste der Parteien

Verantwortliche(r):

1. *Der Kunde (wie im Rahmenvertrag oder dem Bestellformular bezeichnet)*

Auftragsverarbeiter:

1. *Glooko AB (wie im Rahmenvertrag bezeichnet)*

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Autorisierte Benutzer
- Patienten

Kategorien personenbezogener Daten, die verarbeitet werden

Für Autorisierte Benutzer

- Allgemeine Informationen (Name)
- Kontaktinformationen (E-Mailadresse, Telefonnummer)
- Nutzungsinformationen (Benutzername, Passwort, Zugangsrechte, Audit Logs)

Für Patienten

- Allgemeine Informationen (Name, Geburtsdatum)
- Kontaktinformationen (Postadresse, E-Mailadresse, Telefonnummer)
- Nutzungsinformationen (Benutzername, Passwort)
- Gesundheitsinformationen (Diabetes Typ, Jahr der Diabetes Diagnose, erwarteter Partus, Zielbereich, Gewicht, Größe, Behandlungen)
- Geräteinformationen (Seriennummer(n) der Insulinpumpe(n), des Blutzuckermessgeräts und Insulinstifts, Dosierungen, Kohlenhydrate, Einstellungen, Alarme)

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

- Gesundheitsdaten

Für Informationen zu den implementierten Schutzmaßnahmen siehe Anhang III

Art der Verarbeitung

Erhebung, Analyse, Visualisierung und sonstige Verarbeitung der personenbezogenen Daten gemäß dem Rahmenvertrag.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Um dem Verantwortlichen und seinen Autorisierten Benutzern zu ermöglichen, die Software und andere Leistungen gemäß dem Rahmenvertrag zu nutzen.

Dauer der Verarbeitung

Für die Dauer der Bereitstellung der Software und andere Leistungen gemäß dem Rahmenertrag.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Siehe Anhang IV

Anweisungen gemäß Abschnitt 7.8 a) der Klauseln in Bezug auf internationale Datenübermittlungen

Die Standardvertragsklauseln für internationale Datenübermittlungen (die „**SCCs**“) in Anhang V finden Anwendung, wenn der Auftragsverarbeiter personenbezogene Daten in ein Land außerhalb der EU übermittelt, das von der Europäischen Kommission nicht als Land anerkannt wird, welches ein angemessenes Schutzniveau für personenbezogene Daten bietet.

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

1. Zweck. Dieser Anhang beschreibt das Sicherheitsprogramm, die Sicherheitszertifizierungen sowie die technischen und organisatorischen Maßnahmen von Glooko zum Schutz (a) personenbezogener Daten, die vom Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet werden, vor unbefugter Nutzung, unbefugtem Zugang, unbefugter Offenlegung oder unbefugtem Diebstahl und (b) der Software. Da sich die Sicherheitsbedrohungen verändern und weiterentwickeln, aktualisiert Glooko ständig sein Sicherheitsprogramm und seine Strategie, um personenbezogene Daten und die Software zu schützen. Daher behält sich Glooko das Recht vor, diesen Anhang von Zeit zu Zeit zu aktualisieren, vorausgesetzt, dass eine Aktualisierung den in diesem Anhang dargelegten Gesamtschutz nicht wesentlich verringert.

2. Sicherheitsorganisation und -programm. Glooko unterhält ein Sicherheitsprogramm mit Risikobewertung. Der Rahmen für das Sicherheitsprogramm von Glooko umfasst administrative, organisatorische, technische und physische Schutzmaßnahmen, die angemessen sind, um die Software und die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten zu schützen. Das Sicherheitsprogramm von Glooko soll der Art der Software sowie der Größe und Komplexität des Geschäftsbetriebs von Glooko angemessen sein. Glooko hat ein separates und engagiertes Informationssicherheitsteam, das das Sicherheitsprogramm von Glooko verwaltet. Dieses Team erleichtert und unterstützt unabhängige Audits und Bewertungen, die von Dritten durchgeführt werden. Der Sicherheitsrahmen von Glooko umfasst Programme, die Folgendes abdecken: Richtlinien und Verfahren, Asset Management, Zugangsmanagement, Kryptografie, physische Sicherheit, Betriebssicherheit, Kommunikationssicherheit, Sicherheit der Geschäftskontinuität, Personalsicherheit, Produktsicherheit, Sicherheit der Cloud- und Netzwerkinfrastruktur, Sicherheits-Compliance, Sicherheit von Drittanbietern, Schwachstellenmanagement sowie Sicherheitsüberwachung und Reaktion auf Vorfälle. Die Sicherheit wird auf den höchsten Ebenen des Unternehmens verwaltet. Der Sicherheitsbeauftragte von Glooko trifft sich regelmäßig mit der Geschäftsleitung, um Belange zu besprechen und unternehmensweite Sicherheitsinitiativen zu koordinieren. Die Richtlinien und Standards für die Informationssicherheit werden mindestens einmal jährlich von der Geschäftsleitung überprüft und genehmigt und allen Glooko-Mitarbeitern als Referenz zur Verfügung gestellt.

3. Vertraulichkeit. Glooko verfügt über Kontrollen zur Wahrung der Vertraulichkeit personenbezogener Daten in Übereinstimmung mit dem Rahmenvertrag. Alle Mitarbeiter von Glooko und Vertragspersonal sind an die internen Richtlinien von Glooko zur Wahrung der Vertraulichkeit personenbezogener Daten gebunden und vertraglich zur Einhaltung dieser Verpflichtungen verpflichtet.

4. Personelle Sicherheit

a. Mitarbeiter-Hintergrundüberprüfungen. Glooko führt bei allen neuen Mitarbeitern zum Zeitpunkt der Einstellung Hintergrundüberprüfungen in Übereinstimmung mit den geltenden lokalen Gesetzen durch. Glooko prüft derzeit die Ausbildung und frühere Beschäftigung eines neuen Mitarbeiters und führt Referenzprüfungen durch. Soweit nach geltendem Recht zulässig, kann Glooko je nach Art und Umfang der Rolle eines neuen Mitarbeiters auch Strafrechts-, Kredit-, Einwanderungs- und Sicherheitsüberprüfungen durchführen.

b. Mitarbeiterschulung. Mindestens einmal (1) pro Jahr müssen alle Glooko-Mitarbeiter eine Sicherheits- und Datenschutzschulung absolvieren, in der die Sicherheitsrichtlinien von Glooko, bewährte Sicherheitsverfahren und Datenschutzgrundsätze behandelt werden. Mitarbeiter, die beurlaubt sind, können zusätzliche Zeit haben, um diese jährliche Schulung zu absolvieren. Das engagierte Sicherheitsteam von Glooko führt auch Kampagnen zur Sensibilisierung für Phishing durch und informiert die Mitarbeiter über neue Bedrohungen.

5. Verwaltung von Drittanbietern

a. Bewertung des Anbieters. Glooko kann für die Bereitstellung der Software auf Drittanbieter zurückgreifen. Glooko führt eine auf Sicherheitsrisiken basierende Bewertung potenzieller Anbieter durch, bevor es mit ihnen zusammenarbeitet, um sicherzustellen, dass sie die Sicherheitsanforderungen von Glooko erfüllen. Glooko überprüft regelmäßig jeden Anbieter im Hinblick auf die Sicherheits- und Geschäftskontinuitätsstandards von Glooko, einschließlich der Art des Zugangs und der Klassifizierung der Daten, auf die zugegriffen wird (falls zutreffend), der zum Schutz der Daten erforderlichen Kontrollen und der gesetzlichen/regulatorischen Anforderungen. Glooko stellt sicher, dass personenbezogene Daten bei Beendigung einer Anbieterbeziehung zurückgegeben und/oder gelöscht werden.

b. Vereinbarungen mit Anbietern. Glooko schließt mit allen seinen Anbietern schriftliche Vereinbarungen ab, die Vertraulichkeits-, Datenschutz- und Sicherheitsverpflichtungen beinhalten, die ein angemessenes Schutzniveau für personenbezogene Daten bieten, die diese Anbieter verarbeiten können.

6. Architektur, Firewalls und Datentrennung. Der gesamte Netzzugang zwischen den Produktionshosts wird durch Firewalls eingeschränkt, damit nur autorisierte Dienste im Produktionsnetz interagieren können. Firewalls werden eingesetzt, um die Netzwerktrennung zwischen verschiedenen Sicherheitszonen in der Produktions- und Unternehmensumgebung zu verwalten. Glooko trennt seine Datenbanken logisch voneinander. Die Glooko-APIs sind so konzipiert und aufgebaut, dass sie den Zugang nur zu und von den jeweiligen Absendern zulassen. Diese Kontrollen verhindern, dass Kunden Zugang zu den Daten anderer Kunden haben.

7. Physische Sicherheit. Die Rechenzentren, in denen die Software gehostet wird, werden sowohl an den Außengrenzen als auch an den Gebäudeeingängen durch professionelles Sicherheitspersonal mit Hilfe von Videoüberwachung, Einbruchmeldeanlagen und anderen elektronischen Mitteln streng kontrolliert. Unterbrechungsfreie Stromversorgungen und Generatoren vor Ort stehen zur Verfügung, um im Falle eines Stromausfalls eine Notstromversorgung zu gewährleisten. Darüber hinaus verfügen der Hauptsitz und die Büroräume von Glooko über ein physisches Sicherheitsprogramm, das Besucher, Gebäudeeingänge und die allgemeine Bürosicherheit verwaltet.

8. Sicherheit durch Design. Glooko folgt bei der Entwicklung der Software den Grundsätzen des "Security by Design". Glooko wendet außerdem den Glooko-Standard für den Softwareentwicklungszyklus (SDLC) an, um zahlreiche sicherheitsrelevante Aktivitäten für die Software in verschiedenen Phasen des Produktentwicklungszyklus durchzuführen, von der Anforderungserfassung und dem Produktdesign bis hin zur Produktbereitstellung.

9. Zugangskontrollen

a. Bereitstellung des Zugangs. Um das Risiko der Datenexposition zu minimieren, folgt Glooko bei der Bereitstellung des Systemzugangs den Prinzipien des geringsten Privilegs durch ein teambasiertes Zugangskontrollmodell. Die Mitarbeiter von Glooko sind autorisiert, auf personenbezogene Daten zuzugreifen, basierend auf ihrer Funktion, Rolle und Verantwortung, und ein solcher Zugang erfordert die Genehmigung des Vorgesetzten des Mitarbeiters. Der Zugang eines Mitarbeiters zu personenbezogene Daten wird bei Beendigung

des Arbeitsverhältnisses entfernt. Bevor ein Ingenieur Zugang zur Produktionsumgebung erhält, muss der Zugang von der Geschäftsleitung genehmigt werden und der Ingenieur muss für diesen Zugang interne Schulungen absolvieren, einschließlich Schulungen zu den Systemen des betreffenden Teams. Glooko protokolliert risikoreiche Handlungen und Änderungen in der Produktionsumgebung. Glooko nutzt die Automatisierung, um jede Abweichung von internen technischen Standards zu identifizieren, die auf anomale/unautorisierte Aktivitäten hinweisen könnte, um innerhalb von Minuten nach einer Konfigurationsänderung einen Alarm auszulösen.

b. Passwort-Kontrollen. Wenn sich ein Autorisierter Benutzer bei seinem Konto anmeldet, verschlüsselt Glooko die Anmeldedaten des Benutzers, bevor sie gespeichert werden. Kunden können von ihren Autorisierten Benutzern auch verlangen, dass sie eine weitere Sicherheitsebene zu ihrem Konto hinzufügen, indem sie eine Zwei-Faktor-Authentifizierung (2FA) verwenden.

10. Änderungsmanagement. Glooko verfügt über einen formellen Change-Management-Prozess, um Änderungen an der Produktionsumgebung für die Software zu verwalten, einschließlich aller Änderungen an der zugrunde liegenden Software, den Anwendungen und Systemen. Jede Änderung wird in einer Testumgebung sorgfältig geprüft und bewertet, bevor sie in der Produktionsumgebung für die Software eingesetzt wird. Alle Änderungen, einschließlich der Bewertung der Änderungen in einer Testumgebung, werden mithilfe eines formellen, überprüfbaren Aufzeichnungssystems dokumentiert. Für risikoreiche Änderungen ist die Zustimmung der zuständigen Stellen erforderlich. Es werden auch Pläne und Verfahren für den Fall implementiert, dass eine eingesetzte Änderung zurückgenommen werden muss, um die Sicherheit der Software zu gewährleisten.

11. Verschlüsselung. Für die Software werden (a) die Datenbanken, in denen personenbezogene Daten gespeichert sind, mit dem Advanced Encryption Standard verschlüsselt und (b) personenbezogene Daten bei der Übertragung zwischen der Softwareanwendung des Kunden und der Software mit TLS v1.2 verschlüsselt.

12. Schwachstellen-Management. Glooko unterhält Kontrollen und Richtlinien zur Minderung des Risikos von Sicherheitslücken, um ein Gleichgewicht zwischen dem Risiko und den geschäftlichen/betrieblichen Anforderungen herzustellen. Glooko nutzt ein Tool eines Drittanbieters, um regelmäßig Schwachstellen-Scans durchzuführen, um Schwachstellen in der Cloud-Infrastruktur und den Unternehmenssystemen von Glooko zu bewerten.

13. Penetrationstests. Glooko führt Penetrationstests durch und beauftragt unabhängige Drittunternehmen mit der Durchführung von Penetrationstests auf Anwendungsebene. Erkannte Sicherheitsbedrohungen und Schwachstellen werden priorisiert, bewertet und behoben.

14. Management von Sicherheitsvorfällen. Glooko unterhält Richtlinien für das Management von Sicherheitsvorfällen. Das Security Incident Response Team (T-SIRT) von Glooko bewertet alle relevanten Sicherheitsbedrohungen und Schwachstellen und legt geeignete Abhilfe- und Schadensminimierungsmaßnahmen fest. Glooko bewahrt seine einschlägigen Sicherheitsprotokolle auf.

15. Ausfallsicherheit und Softwarekontinuität. Die Software nutzt eine Vielzahl von Tools und Mechanismen, um eine hohe Verfügbarkeit und Ausfallsicherheit zu erreichen. Für die Software erstreckt sich die Infrastruktur von Glooko über mehrere fehlerunabhängige Verfügbarkeitszonen in geografischen Regionen, die physisch voneinander getrennt sind. Glooko setzt außerdem spezielle Tools ein, die die Serverleistung, die Daten und die Verkehrslastkapazität innerhalb jeder Verfügbarkeitszone und jedes Colocation-Rechenzentrums überwachen. Wenn auf einem Server innerhalb einer Verfügbarkeitszone oder eines Colocation-Rechenzentrums eine suboptimale Serverleistung oder eine überlastete

Kapazität festgestellt wird, erhöhen diese spezialisierten Tools die Kapazität oder verlagern den Datenverkehr, um eine suboptimale Serverleistung oder eine Kapazitätsüberlastung zu beheben. Glooko wird im Falle einer suboptimalen Serverleistung oder überlasteten Kapazität ebenfalls sofort benachrichtigt.

16. Backups und Wiederherstellung. Glooko führt regelmäßige Backups von personenbezogenen Daten durch. Personenbezogene Daten, die gesichert werden, werden redundant über mehrere Verfügbarkeitszonen aufbewahrt und während der Übertragung und im Ruhezustand mit Advanced Encryption Standards verschlüsselt.

ANHANG IV

Liste der Unterauftragsverarbeiter

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: Amazon Web Services EMEA SARL

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

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): Cloud Service Anbieter

2. Name: Cegedim SA

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

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): Cloud Service Anbieter (kann für Kunden, die in Frankreich ansässig sind, genutzt werden)

3. Name: Pictime Groupe

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

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): Zertifizierter Gesundheitsdaten-Host (kann für Kunden, die in Frankreich und Deutschland ansässig sind, genutzt werden)

ANHANG V: STANDARDVERTRAGSKLAUSELN FÜR INTERNATIONALE DATENÜBERMITTLUNGEN (DIE "SCCS")

Klausel 1

Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[1] bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

(b) Die Parteien:

(i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)"), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur"), und

(ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur")

haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.

(d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

(a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien

---

[1] Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der der Verordnung (EU) 2016/679 unterliegt und der im Auftrag eines Organs oder einer Einrichtung der Union als Verantwortlicher handelt, so gewährleistet der Rückgriff auf diese Klauseln bei der Beauftragung eines anderen Auftragsverarbeiters (Unterauftragsverarbeitung), der nicht unter die Verordnung (EU) 2016/679 fällt, ebenfalls die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39), insofern als diese Klauseln und die gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegten Datenschutzpflichten angeglichen sind. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die im Beschluss 2021/915 enthaltenen Standardvertragsklauseln stützen.

hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

(b)Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3

Drittbegünstigte

(a)Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:

(i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7;

(ii)Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b;

(iii)Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e;

(iv)Klausel 12 — Modul eins: Klausel 12 Buchstaben a und d Module zwei und drei: Klausel 12 Buchstaben a, d und f

(v) Klausel 13;

(vi) Klausel 15.1(c), (d) und (e);

(vii) Klausel 16(e);

(viii)Klausel 18 – Module eins, zwei und drei Klausel 18 Buchstaben a und b Modul vier: Klausel 18.

(b)Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4

Auslegung

(a)Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.

(b)Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

(c)Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln.

Klausel 6

Beschreibung der Datenübermittlung(en)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Klausel 7 – fakultativ

Kopplungsklausel

Nicht anwendbar

Abschnitt II – Pflichten der Parteien

Klausel 8

Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur — durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

8.1 Weisungen

(a) Der Datenexporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenimporteurs, der als sein Verantwortlicher fungiert.

(b) Der Datenexporteur unterrichtet den Datenimporteur unverzüglich, wenn er die betreffenden Weisungen nicht befolgen kann, u. a. wenn eine solche Weisung gegen die Verordnung (EU) 2016/679 oder andere Datenschutzvorschriften der Union oder eines Mitgliedstaats verstößt.

(c) Der Datenimporteur sieht von jeglicher Handlung ab, die den Datenexporteur an der Erfüllung seiner Pflichten gemäß der Verordnung (EU) 2016/679 hindern würde, einschließlich im Zusammenhang mit Unterverarbeitungen oder der Zusammenarbeit mit den zuständigen Aufsichtsbehörden.

(d) Nach Wahl des Datenimporteurs löscht der Datenexporteur nach Beendigung der Datenverarbeitungsdienste alle im Auftrag des Datenimporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenimporteur, dass dies erfolgt ist, oder gibt dem Datenimporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien.

8.2 Sicherheit der Verarbeitung

(a) Die Parteien treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten, auch während der Übermittlung, sowie den Schutz vor einer Verletzung

der Sicherheit zu gewährleisten, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art der personenbezogenen Daten[2], der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung und ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Übermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

(b) Der Datenexporteur unterstützt den Datenimporteur bei der Gewährleistung einer angemessenen Sicherheit der Daten gemäß Buchstabe a. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Datenexporteur gemäß diesen Klauseln verarbeiteten personenbezogenen Daten meldet der Datenexporteur dem Datenimporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde, und unterstützt den Datenimporteur bei der Behebung der Verletzung.

(c) Der Datenexporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.3 Dokumentation und Einhaltung der Klauseln

(a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

(b) Der Datenexporteur stellt dem Datenimporteur alle Informationen zur Verfügung, die für den Nachweis der Einhaltung seiner Pflichten gemäß diesen Klauseln erforderlich sind, und ermöglicht Prüfungen und trägt zu diesen bei.

Klausel 9

Einsatz von Unterauftragsverarbeitern

Nicht anwendbar

Klausel 10

Rechte betroffener Personen

Die Parteien unterstützen sich gegenseitig bei der Beantwortung von Anfragen und Anträgen, die von betroffenen Personen gemäß den für den Datenimporteur geltenden lokalen Rechtsvorschriften oder — bei der Datenverarbeitung durch den Datenexporteur in der Union — gemäß der Verordnung (EU) 2016/679 gestellt werden.

Klausel 11

---

[2] Hierzu zählt, ob die Übermittlung und Weiterverarbeitung personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen oder Straftaten enthalten.

Rechtsbehelf

(a)Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält

Klausel 12

Haftung

(a)Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

(b)Jede Partei haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den die Partei der betroffenen Person verursacht, indem sie deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs gemäß der Verordnung (EU) 2016/679.

(c)Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

(d)Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe c haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

(e)Der Datenimporteur kann sich nicht auf das Verhalten eines Auftragsverarbeiters oder Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung zu entziehen.

Klausel 13

Aufsicht

Nicht anwendbar

Abschnitt III – LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

Nicht anwendbar

Klausel 15

Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

Nicht anwendbar

Abschnitt IV – Schlussbestimmungen

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

(a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe f.

(c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn:

(i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

(ii) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

(iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

(d) Von dem in der EU ansässigen Datenexporteur erhobene personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen unverzüglich vollständig gelöscht werden, einschließlich aller Kopien. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

(e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die

personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/67 gelten.

Klausel 17

Anwendbares Recht

Diese Klauseln unterliegen dem Recht eines Landes, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das im Rahmenvertrag bestimmte Recht ist.

Klausel 18

Gerichtsstand und Zuständigkeit

Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten beigelegt, die im Rahmenvertrag angegeben sind.

ANLAGE

ANHANG I

A. LISTE DER PARTEIEN

Datenexporteur(e): [Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union]

1. Name: Die Glooko Gesellschaft wie im Rahmenvertrag angegeben

   Anschrift: Wie im Rahmenvertrag angegeben

   Name, Funktion und Kontaktdaten der Kontaktperson: Jesper Forster, Datenschutzbeauftragter. Glooko AB, Nellickevägen 20B412 63 Göteborg, Schweden. E-mail: dpo@glooko.com

   Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Bereitstellung der zu erbringenden Leistungen wie im anwendbaren Bestellformular beschrieben

   Unterschrift und Datum: Wie im Bestellformular gemäß dem Rahmenvertrag angegeben

   Rolle (Verantwortlicher/Auftragsverarbeiter): Auftragsverarbeiter

   …

2.

Datenimporteur(e):[Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson]

1. Name: Kunde (wie in dem anwendbaren Bestellformular angegeben)

   Anschrift: Adresse des Kunden (wie in dem anwendbaren Bestellformular angegeben)

   Name, Funktion und Kontaktdaten der Kontaktperson: Adresse des Kunden (wie in dem anwendbaren Bestellformular angegeben)

   Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Erhalt der Leistungen wie in dem anwendbaren Bestellformular angegeben

   Unterschrift und Datum: Wie im Bestellformular gemäß dem Rahmenvertrag angegeben

   Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

   …

2.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

- Die Autorisierten Benutzer des Kunden
- Patienten

Kategorien der übermittelten personenbezogenen Daten

<u>Autorisierte Benutzer des Kunden</u>

- Grundsätzliche Informationen (Name)
- Kontaktdaten (E-Mail-Adresse, Telefonnummer)
- Nutzungsdaten (Benutzername, Passwort, Zugriffsrechte, Audit Logs)

Patienten

- Grundsätzliche Informationen (Name, Geburtsdatum, Geschlecht)
- Kontaktdaten (Postadresse, E-Mail-Adresse, Telefonnummer)
- Nutzungsdaten (Benutzername, Passwort)
- Gesundheitsinformationen (Diabetes Typ, Jahr der Diabetes Diagnose, geschätzter Partus, Zielbereich, Gewicht, Körpergröße, Behandlungen)
- Geräteinformation (Insulinpumpe, Seriennummer(n) von Blutzuckermessgerät und Insulinpen, Dosen, Kohlenhydrate, Einstellungen, Alarme)

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen.

- Gesundheitsinformationen (Diabetes Typ, Jahr der Diabetes Diagnose, geschätzter Partus, Zielbereich, Gewicht, Körpergröße, Behandlungen)

Zugangsbeschränkungen für das Personal auf Grundlage eines Need-to-Know Prinzips (sowohl für den Auftragsverarbeiter als auch den Verantwortlichen)

Der Zugriff auf die Daten wird protokolliert

Transportverschlüsselung und Verschlüsselung von gespeicherten Daten

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)

Die personenbezogenen Daten werden von dem Auftragsverarbeiter gespeichert, jedoch kann der Verantwortliche jederzeit auf diese Zugreifen (z.B., wenn die Leistungen in einer Software as a Service bestehen). Personenbezogene Daten können dann ebenfalls als aus dem EWR in ein Drittland übermittelt gelten.

Art der Verarbeitung

Personenbezogene Daten hochladen, berechnen, analysieren, visualisieren, übermitteln und in sonstiger Weise verarbeiten, um den Autorisierten Benutzern die Nutzung der Leistungen zu ermöglichen.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Der Zweck der Datenübermittlung besteht darin, den Kunden die Nutzung der Leistungen zu ermöglichen.

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Die Verarbeitung ist zeitlich unbeschränkt und soll solange erfolgen, wie die Leistungen bereitgestellt werden oder bis der anwendbare Auftragsverarbeitungsvertrag beendet wird.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben

Nicht anwendbar

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13

Nicht anwendbar

ANHANG II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Nicht anwendbar

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

Nicht anwendbar