CLÁUSULAS CONTRACTUALES TIPO DE GLOOKO

SECCIÓN I

Cláusula 1

Finalidad y ámbito de aplicación

a) La finalidad de las presentes cláusulas contractuales tipo (en lo sucesivo, «pliego de cláusulas») es garantizar que se cumpla el artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

b) Los responsables y encargados del tratamiento enumerados en el anexo I han dado su consentimiento a vincularse por el presente pliego de cláusulas a fin de garantizar el cumplimiento del artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 y/o del artículo 29, apartados 3 y 4, del Reglamento (UE) 2018/1725.

c) El presente pliego de cláusulas se aplica si las condiciones indicadas en el Acuerdo Marco se cumplen y al tratamiento de datos personales especificado en el anexo II.

d) Los anexos I a IV forman parte del pliego.

e) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el responsable en virtud del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

f) El presente pliego de cláusulas no garantiza por sí mismo el cumplimiento de las obligaciones relativas a las transferencias internacionales contempladas en el capítulo V del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

Cláusula 2

Invariabilidad del pliego de cláusulas

a) Las partes se comprometen a no modificar el pliego de cláusulas, excepto para añadir o actualizar información en los anexos.

b) Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, el pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

Cláusula 3

Interpretación

a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679 o en el Reglamento (UE) 2018/1725, se entiende que tienen el mismo significado que en el Reglamento correspondiente.

b)El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

c)No se podrán realizar interpretaciones del presente pliego de cláusulas que entren en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679 y el Reglamento (UE) 2018/1725 y/o que perjudiquen los derechos o libertades fundamentales de los interesados.

Cláusula 4

Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 5 (opcional)

Cláusula de incorporación

a)Cualquier entidad que no sea parte en el presente pliego de cláusulas podrá, previo consentimiento de todas las partes, adherirse al presente pliego de cláusulas en cualquier momento, ya sea como responsable o como encargado, cumplimentando los anexos y firmando el anexo I.

b)Una vez se hayan cumplimentado y firmado los anexos a que se refiere la letra a), la entidad que se adhiera será tratada como parte en el presente pliego de cláusulas y tendrá los derechos y obligaciones de un responsable o encargado, según la categoría en la que se haya inscrito en el anexo I.

c)La entidad que se adhiera no adquirirá derechos y obligaciones del presente pliego de cláusulas derivados del período anterior a la adhesión.

SECCIÓN II - OBLIGACIONES DE LAS PARTES

Cláusula 6

Descripción del tratamiento o tratamientos

En el anexo II se especifican los pormenores de las operaciones de tratamiento y, en particular, las categorías de datos personales y los fines para los que se tratan los datos personales por cuenta del responsable.

Cláusula 7

Obligaciones de las partes

7.1. Instrucciones

a) El encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado. En tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. El responsable también podrá dar instrucciones ulteriores en cualquier momento del período de tratamiento de los datos personales. Dichas instrucciones deberán estar siempre documentadas.

b) El encargado informará inmediatamente al responsable si las instrucciones dadas por el responsable infringen, a juicio del encargado, el Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 o las disposiciones aplicables del Derecho de la Unión o de los Estados miembros en materia de protección de datos.

7.2. Limitación de la finalidad

El encargado tratará los datos personales únicamente para los fines específicos del tratamiento indicados en el anexo II, salvo cuando siga instrucciones adicionales del responsable.

7.3. Duración del tratamiento de datos personales

El tratamiento por parte del encargado solo se realizará durante el período especificado en el anexo II.

7.4. Seguridad del tratamiento

a) El encargado aplicará, como mínimo, las medidas técnicas y organizativas especificadas en el anexo III para garantizar la seguridad de los datos personales. Una de estas medidas podrá consistir en la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos («violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados.

b) El encargado solo concederá acceso a los datos personales tratados a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. El encargado garantizará que las personas autorizadas para tratar

los datos personales recibidos se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

7.5. Datos sensibles

Si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales («datos sensibles»), el encargado aplicará restricciones específicas y/o garantías adicionales.

7.6. Documentación y cumplimiento

a) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas.

b) El encargado resolverá con presteza y de forma adecuada las consultas del responsable relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

c) El encargado pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y que deriven directamente del Reglamento (UE) 2016/679 y del Reglamento (UE) 2018/1725. A instancia del responsable, el encargado permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el responsable podrá tener en cuenta las certificaciones pertinentes que obren en poder del encargado.

d) El responsable podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías también podrán consistir en inspecciones de los locales o instalaciones físicas del encargado y, cuando proceda, realizarse con un preaviso razonable.

e) Las partes pondrán a disposición de las autoridades de control competentes, a instancia de estas, la información a que se refiere la presente cláusula y, en particular, los resultados de las auditorías.

7.7. Recurso a subencargados

a) El encargado cuenta con una autorización general del responsable para contratar a subencargados que figuren en una lista acordada. El encargado informará al responsable específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos treinta (30) días de antelación, de modo que el responsable tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El encargado del tratamiento proporcionará al responsable la información necesaria para que pueda ejercer su derecho a formular objeción.

b) Cuando el encargado contrate a un subencargado para llevar a cabo actividades de tratamiento específicas (por cuenta del responsable), lo hará por medio de un contrato que imponga al subencargado, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al encargado en virtud del presente pliego de cláusulas. El encargado se asegurará de que el subencargado cumpla las obligaciones a las que esté sujeto en virtud del presente pliego de cláusulas y del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

c) El encargado proporcionará al responsable, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea

necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el encargado podrá expurgar el texto del contrato antes de compartir la copia.

d)El encargado seguirá siendo plenamente responsable ante el responsable del cumplimiento de las obligaciones que imponga al subencargado su contrato con el encargado. El encargado notificará al responsable los incumplimientos por parte del subencargado de las obligaciones que le atribuya dicho contrato.

e)El encargado, cuando sea posible, pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el encargado desaparezca de facto, cese de existir jurídicamente o sea insolvente, el responsable tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

7.8. Transferencias internacionales

a)Las transferencias de datos a un tercer país o a una organización internacional por parte del encargado solo podrán realizarse siguiendo instrucciones documentadas del responsable o en virtud de una exigencia expresa del Derecho de la Unión o del Estado miembro al que esté sujeto el encargado; se llevarán a cabo de conformidad con el capítulo V del Reglamento (UE) 2016/679 o del Reglamento (UE) 2018/1725.

b)El responsable se aviene a que, cuando el encargado recurra a un subencargado de conformidad con la cláusula 7.7 para llevar a cabo actividades de tratamiento específicas (por cuenta del responsable) y dichas actividades conlleven una transferencia de datos personales en el sentido del capítulo V del Reglamento (UE) 2016/679, el encargado y el subencargado puedan garantizar el cumplimiento del capítulo V del Reglamento (UE) 2016/679 utilizando cláusulas contractuales tipo adoptadas por la Comisión, con arreglo al artículo 46, apartado 2, del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones para la utilización de dichas cláusulas contractuales tipo.

Cláusula 8

Ayuda al responsable del tratamiento

a)El encargado indicará a los interesados que se pongan en contacto con el responsable, en caso de que el encargado reciba una solicitud de los interesados. No responderá a dicha solicitud por sí mismo, a menos que el responsable le haya autorizado a hacerlo.

b)El encargado ayudará al responsable a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos de los interesados teniendo en cuenta la naturaleza del tratamiento. En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el encargado cumplirá las instrucciones del responsable.

c)Además de la obligación del encargado de ayudar al responsable en virtud de la cláusula 8, letra b), el encargado también ayudará al responsable a garantizar el cumplimiento de las obligaciones siguientes teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el encargado:

1)la obligación de realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales («evaluación de impacto») cuando sea probable que un tipo de tratamiento suponga un alto riesgo para los derechos y libertades de las personas físicas;

2)la obligación de consultar a las autoridades de control competentes antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo;

3)la obligación de garantizar que los datos personales sean exactos y estén actualizados, informando sin demora al responsable si el encargado descubre que los datos personales que está tratando son inexactos o han quedado obsoletos;

4) las obligaciones contempladas en el artículo 32 del Reglamento (UE) 2016/679.

d)Las partes establecerán en el anexo III medidas técnicas y organizativas apropiadas que obliguen al encargado a ayudar al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

Cláusula 9

Notificación de violaciones de la seguridad de los datos personales

En caso de violación de la seguridad de los datos personales, el encargado colaborará con el responsable y le ayudará a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del Reglamento (UE) 2016/679 o los artículos 34 y 35 del Reglamento (UE) 2018/1725, en su caso, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el encargado.

9.1. Violación de la seguridad de datos personales tratados por el responsable

En caso de violación de la seguridad de los datos personales en relación con los datos tratados por el responsable, el encargado ayudará al responsable en lo siguiente.

a)Notificar la violación de la seguridad de los datos personales a las autoridades de control competentes sin dilación indebida una vez tenga constancia de ella, si procede (a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas).

b)Recabar la información siguiente, que, de conformidad con el artículo 33, apartado 3, del Reglamento (UE) 2016/679, deberá figurar en la notificación del responsable, que debe incluir como mínimo:

1)la naturaleza de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

2)las consecuencias probables de la violación de la seguridad de los datos personales;

3)las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

c)Cumplir, con arreglo al artículo 34 del Reglamento (UE) 2016/679, la obligación de comunicar sin dilación indebida al interesado la violación de la seguridad de los datos personales cuando sea probable que la violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas.

9.2. Violación de la seguridad de datos personales tratados por el encargado

En caso de violación de la seguridad de datos personales tratados por el encargado, este lo notificará al responsable sin dilación indebida una vez que el encargado tenga constancia de ella. Dicha notificación deberá incluir como mínimo:

a) una descripción de la naturaleza de la violación de la seguridad (inclusive, cuando sea posible, las categorías y el número aproximado de interesados y de registros de datos afectados);

b) los datos de un punto de contacto en el que pueda obtenerse más información sobre la violación de la seguridad de los datos personales;

c) sus consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

Las partes establecerán en el anexo III los demás elementos que deberá aportar el encargado cuando ayude al responsable a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del Reglamento (UE) 2016/679.

SECCIÓN III - DISPOSICIONES FINALES

Cláusula 10

Incumplimiento de las cláusulas y resolución del contrato

a) Sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725, en caso de que el encargado del tratamiento incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el responsable podrá ordenar al encargado que suspenda el tratamiento de datos personales hasta que este vuelva a dar cumplimiento al presente pliego de cláusulas, o resolver el Acuerdo Marco. El encargado informará con presteza al responsable en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

b) El responsable estará facultado para resolver el Acuerdo Marco en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

1) el tratamiento de datos personales por parte del encargado haya sido suspendido por el responsable con arreglo a la letra a) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

2) el encargado incumpla de manera sustancial o persistente el presente pliego de cláusulas o las obligaciones que le atribuye el Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725;

3) el encargado incumpla una resolución vinculante de un órgano jurisdiccional competente o de las autoridades de control competentes en relación con las obligaciones que les atribuye el presente pliego de cláusulas, el Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725.

c) El encargado estará facultado para resolver el Acuerdo Marco en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando, tras haber informado al responsable de que sus instrucciones infringen los requisitos jurídicos exigidos por la cláusula 7.1, letra b), el responsable insiste en que se sigan dichas instrucciones.

d) Tras la resolución del Acuerdo Marco, el encargado suprimirá, a petición del responsable, todos los datos personales tratados por cuenta del responsable y acreditará al responsable que lo ha hecho, o devolverá todos los datos personales al responsable y suprimirá las copias existentes, a menos que el Derecho de la Unión o de los Estados miembros exija el almacenamiento de los datos personales. En caso de que el responsable no haya solicitado que todos los datos personales tratados por cuenta del responsable se devuelvan, dentro de los treinta (30) días siguientes a la terminación del Acuerdo Marco, el encargado podrá, a su entera discreción, eliminar los datos personales. Hasta que se destruyan o devuelvan los datos, el encargado seguirá garantizando el cumplimiento con el presente pliego de cláusulas.

ANEXO I LISTA DE PARTES

Responsable(s):

1. *El Cliente (según se identifica en el Acuerdo Marco o Formulario de Pedido)*

Encargado(s):

1. *Glooko AB (según se identifica en el Acuerdo Marco)*

ANEXO II: DESCRIPCIÓN DEL TRATAMIENTO

Categorías de interesados cuyos datos personales se tratan

- Usuarios Autorizados
- Pacientes

Categorías de datos personales tratados

Para Usuarios Autorizados

- Información general (nombre)
- Datos de contacto (dirección de correo electrónico, número de teléfono)
- Información de uso (nombre de usuario, contraseña, derechos de acceso, registros de auditoría (logs))

Para Pacientes

- Información general (nombre, fecha de nacimiento, género)
- Datos de contacto (dirección postal, dirección de correo electrónico, número de teléfono)
- Información de uso (nombre de usuario, contraseña)
- Datos de salud (tipo de diabetes, año de diagnóstico de la diabetes, fecha estimada para dar a luz, rango objetivo, peso, altura, tratamientos)
- Información del dispositivo (número(s) de serie de la bomba de insulina, del medidor de glucosa y de la pluma de insulina, dosis, carbohidratos, ajustes, alarmas)

Datos sensibles tratados (si procede) y restricciones o garantías aplicadas que tengan plenamente en cuenta la naturaleza de los datos y los riesgos que entrañan, como, por ejemplo, la limitación estricta de la finalidad, restricciones de acceso (incluido el acceso exclusivo del personal que haya hecho un curso especializado), un registro del acceso a los datos, restricciones a transferencias ulteriores o medidas de seguridad adicionales.

- Datos relativos a la salud

Para información acerca de las garantías implementadas, véase el Anexo III

Naturaleza del tratamiento

Recabar, analizar, visualizar y tratar de otro modo los datos personales de conformidad con el Acuerdo Marco.

Finalidad(es) del tratamiento de los datos personales por cuenta del responsable del tratamiento

Para permitir al responsable y sus Usuarios Autorizados utilizar el Software y otros Entregables de conformidad con el Acuerdo Marco.

Duración del tratamiento

Mientras dure la prestación del Software y otros Entregables de conformidad con el Acuerdo Marco.

En caso de tratamiento por parte de (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento

Véase el Anexo IV

Instrucciones bajo el apartado 7.8 a) de las Cláusulas relativas a transferencias internacionales

Las cláusulas contractuales tipo para transferencias internacionales (las "**CCT**") del Anexo V serán de aplicación si el encargado transfiere datos personales fuera del EEE, a un país no reconocido por la Comisión Europea como país que garantiza un nivel adecuado de protección a los datos personales.

ANEXO III MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

1. Finalidad. Este Anexo describe el programa de seguridad de Glooko, las certificaciones de seguridad y las medidas técnicas y organizativas para proteger (a) los datos personales tratados por el encargado del tratamiento en nombre del responsable del tratamiento contra el uso, el acceso y la divulgación no autorizados o el robo y (b) el Software. A medida que las amenazas a la seguridad cambian y evolucionan, Glooko continúa actualizando su programa y estrategia de seguridad para ayudar a proteger los datos personales y el Software. Por tanto, Glooko se reserva el derecho a actualizar este Anexo cada cierto tiempo; siempre y cuando las actualizaciones no reduzcan materialmente las medidas de protección generales establecidas en este Anexo.

2. Organización y Programa de Seguridad. Glooko mantiene un programa de seguridad basado en la evaluación de riesgos. El marco del programa de seguridad de Glooko incluye garantías administrativas, organizativas, técnicas y físicas razonablemente diseñadas para proteger el Software y la confidencialidad, integridad y disponibilidad de los datos personales. El programa de seguridad de Glooko pretende ser adecuado a la naturaleza del Software y al tamaño y complejidad de las operaciones comerciales de Glooko. Glooko tiene un equipo de seguridad de la información independiente y especializado que gestiona el programa de seguridad de Glooko. Este equipo facilita y apoya las auditorías y evaluaciones independientes realizadas por terceros. El marco de seguridad de Glooko incluye programas que cubren: Políticas y Procedimientos, Gestión de Activos, Gestión de Accesos, Criptografía, Seguridad Física, Seguridad de las Operaciones, Seguridad de las Comunicaciones, Seguridad de la Continuidad del Negocio, Seguridad de las Personas, Seguridad de los Productos, Seguridad de la Nube y de la Infraestructura de la Red, Cumplimiento de la Seguridad, Seguridad de Terceros, Gestión de Vulnerabilidades y Monitorización de la Seguridad y Respuesta a Incidentes. La seguridad se gestiona al más alto nivel de la empresa, y el responsable de seguridad (*Security Officer*) de Glooko se reúne regularmente con la dirección ejecutiva para debatir los problemas y coordinar las iniciativas de seguridad de toda la empresa. Las políticas y normas de seguridad de la información son revisadas y aprobadas por la dirección al menos una vez al año y se ponen a disposición de todos los empleados de Glooko para su conocimiento.

3. Confidencialidad. Glooko cuenta con controles para mantener la confidencialidad de los datos personales de acuerdo con el Acuerdo Marco. Todos los empleados de Glooko y el personal contratado están sujetos a las políticas internas de Glooko relativas al mantenimiento de la confidencialidad de los datos personales y están obligados contractualmente a cumplir con estas obligaciones.

4. Seguridad de las Personas

    a. Comprobación de los Antecedentes de los Empleados. Glooko realiza comprobaciones de antecedentes de todos los nuevos empleados en el momento de la contratación de acuerdo con las leyes locales aplicables. Actualmente, Glooko verifica la educación y el empleo anterior de los nuevos empleados y realiza comprobaciones de referencias. Cuando la ley aplicable lo permita, Glooko también puede realizar comprobaciones de antecedentes penales, crediticios, de inmigración y de seguridad, dependiendo de la naturaleza y el alcance de la función del nuevo empleado.

    b. Formación de los Empleados. Al menos una (1) vez al año, todos los empleados de Glooko deben completar una formación sobre seguridad y privacidad que cubra las políticas de seguridad de Glooko, las mejores prácticas de seguridad y los principios de privacidad. Los empleados que se encuentren de permiso/excedencia pueden disponer de tiempo adicional para completar esta formación anual. El equipo de seguridad de Glooko también realiza campañas de concienciación sobre *phishing* e informa sobre nuevas amenazas a los empleados.

5. Gestión de Proveedores Externos

   a. Evaluación de Proveedores. Glooko puede utilizar proveedores externos para proporcionar el Software. Glooko lleva a cabo una evaluación de riesgos de seguridad de los posibles proveedores antes de trabajar con ellos para validar que cumplen con los requisitos de seguridad de Glooko. Glooko revisa periódicamente a cada proveedor atendiendo a los estándares de seguridad y continuidad del negocio de Glooko, incluyendo el tipo de acceso y la clasificación de los datos a los que se accede (si los hay), los controles necesarios para proteger los datos y los requisitos legales/regulatorios. Glooko se asegura de que los datos personales sean devueltos y/o eliminados al final de la relación con el proveedor.

   b. Acuerdos con Proveedores. Glooko celebra acuerdos por escrito con todos sus proveedores que incluyen obligaciones de confidencialidad, privacidad y seguridad que proporcionan un nivel adecuado de protección de los datos personales que estos proveedores puedan tratar.

6. Arquitectura, Cortafuegos y Segregación de Datos. Todo acceso a la red entre los hosts de producción está restringido, utilizando cortafuegos para permitir que sólo los servicios autorizados interactúen en la red de producción. Los cortafuegos se utilizan para gestionar la segregación de la red entre las diferentes zonas de seguridad en los entornos de producción y corporativos. Glooko separa lógicamente sus bases de datos. Las APIs de Glooko están diseñadas y construidas para identificar y permitir el acceso sólo a y desde los respectivos remitentes. Estos controles evitan que los clientes tengan acceso a los datos de otros clientes.

7. Seguridad Física. Los centros de datos que albergan el Software están estrictamente controlados, tanto en el perímetro como en los puntos de entrada al edificio, por personal de seguridad profesional que utiliza videovigilancia, sistemas de detección de intrusos y otros medios electrónicos. Se dispone de sistemas de alimentación ininterrumpida y generadores in situ para proporcionar energía de reserva en caso de fallo eléctrico. Además, la sede y las oficinas de Glooko cuentan con un programa de seguridad física que gestiona las visitas, las entradas al edificio y la seguridad general de las oficinas.

8. Seguridad desde el Diseño. Glooko sigue los principios de seguridad desde el diseño cuando diseña el Software. Glooko también aplica el estándar del Ciclo de Vida de Desarrollo de Software (SDLC por sus siglas en inglés) de Glooko para llevar a cabo numerosas actividades relacionadas con la seguridad del Software a través de las diferentes fases del ciclo de vida de la creación del producto, desde la recopilación de requisitos y el diseño del producto hasta el despliegue del mismo.

9. Control de Accesos

   a. Concesión de Acceso. Para minimizar el riesgo de exposición de los datos, Glooko sigue principios de privilegios mínimos a través de un modelo de control de acceso basado en el equipo cuando se proporciona el acceso al sistema. El personal de Glooko está autorizado a acceder a los datos personales en función de su trabajo, rol y responsabilidades, y dicho acceso requiere la aprobación del jefe del empleado. El acceso de un empleado a los datos personales se retira al terminar su empleo. Antes de conceder a un ingeniero acceso al entorno de producción, el acceso debe ser aprobado por la dirección y el ingeniero está obligado a completar las formaciones internas para dicho acceso, incluyendo las formaciones en los sistemas del equipo correspondiente. Glooko registra las acciones y los cambios de alto riesgo en el entorno de producción. Glooko aprovecha la automatización para identificar cualquier desviación de las normas técnicas internas que pueda indicar una actividad anómala/no autorizada para lanzar una alerta a los pocos minutos de un cambio de configuración.

   b. Control de Contraseñas. Cuando un Usuario Autorizado se conecta a su cuenta, Glooko hace un hash de las credenciales del usuario antes de almacenarlas. Los clientes también pueden requerir a sus Usuarios Autorizados que añadan otra capa de seguridad a su cuenta utilizando la autenticación de dos factores (2FA por sus siglas en inglés).

10. Gestión de Cambios. Glooko tiene un proceso formal de gestión de cambios que sigue para administrar los cambios en el entorno de producción del Software, incluyendo cualquier cambio en su software, aplicaciones y sistemas subyacentes. Cada cambio es cuidadosamente revisado y evaluado en un entorno de prueba antes de ser desplegado en el entorno de producción para el Software. Todos los cambios, incluida la evaluación de los cambios en un entorno de prueba, se documentan mediante un sistema de registro formal y auditable. Los *stakeholders* competentes de la organización deberán aprobar el despliegue de los cambios de alto riesgo. También se implementan planes y procedimientos en caso de que sea necesario revertir un cambio ya desplegado para preservar la seguridad del software.

11. Cifrado. Para el Software, (a) las bases de datos que almacenan datos personales están encriptadas utilizando el Estándar de Encriptación Avanzada (AES por sus siglas en inglés) y (b) los datos personales están encriptados cuando están en tránsito entre la aplicación de software del Cliente y el Software utilizando TLS v1.2.

12. Gestión de Vulnerabilidades. Glooko mantiene controles y políticas para mitigar el riesgo de vulnerabilidades de seguridad con el fin de alcanzar el equilibrio entre el riesgo y las necesidades empresariales/operativas. Glooko utiliza una herramienta de terceros para realizar periódicamente escaneos de vulnerabilidades y así evaluar las vulnerabilidades en la infraestructura de la nube de Glooko y los sistemas corporativos.

13. Pruebas de Penetración. Glooko realiza pruebas de penetración y contrata a terceras entidades independientes para realizar pruebas de penetración a nivel de aplicación. Las amenazas de seguridad y las vulnerabilidades que se detectan son priorizadas, clasificadas y remediadas.

14. Gestión de Incidentes de Seguridad. Glooko mantiene políticas de gestión de incidentes de seguridad. El Equipo de Respuesta a Incidentes de Seguridad de Glooko (T-SIRT) evalúa todas las amenazas y vulnerabilidades de seguridad relevantes y establece las acciones de corrección y mitigación apropiadas. Glooko conserva sus registros de seguridad pertinentes.

15. Resiliencia y Continuidad del Software. El Software utiliza una variedad de herramientas y mecanismos para lograr una alta disponibilidad y resiliencia. Para el Software, la infraestructura de Glooko abarca múltiples zonas de disponibilidad independientes a efectos de incidencias en regiones geográficas físicamente separadas entre sí. Glooko también utiliza herramientas especializadas que supervisan el rendimiento de los servidores, los datos y la capacidad de carga de tráfico dentro de cada zona de disponibilidad y centro de datos coubicado (*colocation data center*). Si se detecta un rendimiento subóptimo del servidor o una capacidad sobrecargada en un servidor dentro de una zona de disponibilidad o centro de datos coubicado, estas herramientas especializadas aumentan la capacidad o cambian el tráfico para aliviar cualquier rendimiento subóptimo del servidor o sobrecarga de capacidad. Glooko también es notificado inmediatamente en el caso de cualquier rendimiento subóptimo del servidor o capacidad sobrecargada.

16. Copias de Seguridad y Recuperación. Glooko realiza copias de seguridad periódicas de los datos personales. Los datos personales de los que se hace una copia de seguridad se conservan de forma duplicada (redundante) en múltiples zonas de disponibilidad y se encriptan en tránsito y en reposo utilizando Estándares Avanzados de Encriptación.

ANEXO IV: LISTA DE SUBENCARGADOS DEL TRATAMIENTO

El responsable ha autorizado que se recurra a los subencargados siguientes:

1. **Nombre**: Amazon Web Services EMEA SARL

Dirección: 38 Avenue John F. Kennedy, L-1855, Luxemburgo

Descripción del tratamiento (incluida una delimitación bien definida de las responsabilidades si se autoriza a varios subencargados): Proveedor de servicios de cloud (nube)

2. **Nombre**: Cegedim SA

Dirección: 137 rue d'Aguesseau, 92100 Boulogne-Billancourt, Francia

Descripción del tratamiento (incluyendo una clara delimitación de responsabilidades en caso de que estén autorizados varios subencargados): proveedor de servicios de cloud (nube) (puede ser utilizado para Clientes ubicados en Francia)

3. **Nombre**: Pictime Groupe

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

Descripción del tratamiento (incluyendo una clara delimitación de responsabilidades en caso de que estén autorizados varios subencargados): Host de datos sanitarios certificado (puede ser utilizado para Clientes ubicados en Francia y Alemania)

ANEXO V: CLÁUSULAS CONTRACTUALES TIPO PARA TRANSFERENCIAS INTERNACIONALES (LAS "CCT")

Cláusula 1

Finalidad y ámbito de aplicación

a) La finalidad de estas cláusulas contractuales tipo es garantizar que se cumplan los requisitos que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), exige para la transferencia de datos personales a un tercer país.

b) Las partes:

(i). la(s) persona(s) física(s) o jurídica(s), autoridad(es) pública(s), servicio(s) u organismo(s) (en lo sucesivo, «entidad» o «entidades») que va(n) a transferir los datos personales, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «exportador de datos»), y

(ii). la(s) entidad(es) en un tercer país que va(n) a recibir los datos personales del exportador de datos directamente o indirectamente por medio de otra entidad que también sea parte en el presente pliego de cláusulas, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «importador de datos»),

han pactado las presentes cláusulas contractuales tipo (en lo sucesivo, «pliego de cláusulas»).

c) El presente pliego de cláusulas se aplica a la transferencia de datos personales especificada en el anexo I.B.

d) El apéndice del presente pliego de cláusulas, que contiene los anexos que se citan en estas, forman parte del pliego.

Cláusula 2

Efecto e invariabilidad de las cláusulas

a) El presente pliego de cláusulas establece garantías adecuadas, incluidos derechos exigibles de los interesados y acciones judiciales eficaces, de conformidad con el artículo 46, apartado 1, y el artículo 46, apartado 2, letra c), del Reglamento (UE) 2016/679 y, en relación con las transferencias de datos de responsables a encargados o de encargados a otros encargados, de conformidad con las cláusulas contractuales tipo a que se refiere el artículo 28, apartado 7, del Reglamento (UE) 2016/679 siempre que no se modifiquen, salvo para seleccionar el módulo o módulos adecuados o para añadir o actualizar información del apéndice. Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, al presente pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

b) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el exportador de datos en virtud del Reglamento (UE) 2016/679.

Cláusula 3

Terceros beneficiarios

a) Los interesados podrán invocar, como terceros beneficiarios, el presente pliego de cláusulas contra el exportador y/o el importador de datos y exigirles su cumplimiento, con las excepciones siguientes.

i) Cláusulas 1, 2, 3, 6 y 7.

ii) Cláusula 8: [módulo uno] cláusula 8.5, letra e), y cláusula 8.9, letra b); [módulo dos] cláusula 8.1, letra b), y cláusula 8.9, letras a), c), d) y e); [módulo tres] cláusula 8.1, letras a), c) y d), y cláusula 8.9, letras a), c), d), e), f) y g); [módulo cuatro] cláusula 8.1, letra b), y cláusula 8.3, letra b).

iii) Cláusula 9: [módulo dos] cláusula 9, letras a), c), d) y e); [módulo tres] cláusula 9, letras a), c), d) y e).

iv) Cláusula 12: [módulo uno] cláusula 12, letras a) y d); [módulos dos y tres] cláusula 12, letras a), d) y f).

v) Cláusula 13.

vi) Cláusula 15.1, letras c), d) y e).

vii) Cláusula 16, letra e).

viii) Cláusula 18: [módulos uno, dos y tres] cláusula 18, letras a) y b); [módulo cuatro] cláusula 18.

b) Lo dispuesto en la letra a) se entiende sin perjuicio de los derechos que el Reglamento (UE) 2016/679 otorga a los interesados.

Cláusula 4

Interpretación

a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679, se entiende que tienen el mismo significado que en dicho Reglamento.

b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679.

c) El presente pliego de cláusulas no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679.

Cláusula 5

Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 6

Descripción de la transferencia o transferencias

Los datos de la transferencia o transferencias y, en particular, las categorías de datos personales que se transfieren y los fines para los que se transfieren se especifican en el anexo I.B.

Cláusula 7 (opcional)

Cláusula de incorporación

No aplicable

SECCIÓN II: OBLIGACIONES DE LAS PARTES

Cláusula 8

Garantías en materia de protección de datos

El exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el importador de datos puede, aplicando medidas técnicas y organizativas adecuadas, cumplir las obligaciones que le atribuye el presente pliego de cláusulas.

8.1. Instrucciones

a) El exportador de datos solo tratará los datos personales siguiendo instrucciones documentadas del importador de datos que actúe como su responsable.

b) El exportador de datos informará inmediatamente al importador de datos si no puede seguir dichas instrucciones, especialmente si dichas instrucciones infringen el Reglamento (UE) 2016/679 u otro instrumento normativo del Derecho de la Unión o del Estado miembro en materia de protección de datos.

c) El importador de datos no obrará de forma que pueda impedir al exportador de datos cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679 y, en particular, en el marco del subtratamiento o de la cooperación con las autoridades de control competentes.

d) Una vez se hayan prestado los servicios de tratamiento, el exportador de datos suprimirá, a petición del importador de datos, todos los datos personales tratados por cuenta del importador de datos y acreditará al importador de datos que lo ha hecho, o devolverá al

importador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes.

8.2. Seguridad del tratamiento

a) Las partes aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, especialmente durante la transferencia; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza de los datos personales, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados, y considerarán, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento.

b) El exportador de datos ayudará al importador de datos a garantizar una seguridad adecuada de los datos de conformidad con la letra a). En caso de violación de la seguridad de los datos personales tratados por el exportador de datos en virtud del presente pliego de cláusulas, el exportador de datos lo notificará sin dilación indebida al importador de datos, una vez que tenga conocimiento de ello, y le ayudará a poner remedio a la violación de la seguridad.

c) El exportador de datos garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

8.3. Documentación y cumplimiento

a) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas.

b) El exportador de datos pondrá a disposición del importador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones que le atribuye el presente pliego de cláusulas y permitirá y contribuirá a las auditorías.

Cláusula 9

Recurso a subencargados

No aplicable

Cláusula 10

Derechos del interesado

Las partes se prestarán ayuda recíproca para responder a las consultas y solicitudes de los interesados en virtud del Derecho doméstico aplicable al importador de datos o, respecto del tratamiento de datos por parte del exportador de datos en la Unión, en virtud del Reglamento (UE) 2016/679.

Cláusula 11

Reparación

a) El importador de datos informará a los interesados, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará con presteza las reclamaciones que reciba de los interesados.

Cláusula 12

Responsabilidad

a) Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.

b) Cada parte será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que la parte ocasione al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Ello se entiende sin perjuicio de la responsabilidad que le atribuye el Reglamento (UE) 2016/679 al exportador de datos.

c) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.

d) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra c), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.

e) El importador de datos no puede alegar la conducta de un encargado o subencargado del tratamiento para eludir su propia responsabilidad.

Cláusula 13

Supervisión

No aplicable

SECCIÓN III: DERECHO DEL PAÍS Y OBLIGACIONES EN CASO DE ACCESO POR PARTE DE LAS AUTORIDADES PÚBLICAS

Cláusula 14

Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

No aplicable

Cláusula 15

Obligaciones del importador de datos en caso de acceso por parte de las autoridades públicas

No aplicable

SECCIÓN IV: DISPOSICIONES FINALES

Cláusula 16

Incumplimiento de las Cláusulas y resolución del contrato

a) El importador de datos informará con presteza al exportador de datos en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

b) En caso de que el importador de datos incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos suspenderá la transferencia de datos personales al importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato. Lo anterior se entiende sin perjuicio de la cláusula 14, letra f).

c) El exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

   i) el exportador de datos haya suspendido la transferencia de datos personales al importador de datos con arreglo a la letra b) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

   ii) el importador de datos vulnere de manera sustancial o persistente el presente pliego de cláusulas; o

   iii) el importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o autoridad de control competente en relación con las obligaciones que le atribuye el presente pliego de cláusulas.

   En este supuesto, informará a la autoridad de supervisión competente de su incumplimiento. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa.

d) Los datos personales recopilados por el exportador de datos en la UE que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán destruirse en su totalidad inmediatamente, así como cualquier copia de estos. El importador de datos acreditará la destrucción de los datos al exportador de datos. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales transferidos, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país.

e) Ninguna de las partes podrá revocar su consentimiento a quedar vinculada por el presente pliego de cláusulas si: i) la Comisión Europea adopta una decisión de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679 que regule la transferencia de datos personales a los que se aplique el presente pliego de cláusulas; o ii) el Reglamento (UE) 2016/679 pasa a formar parte del ordenamiento jurídico del país al que se transfieren los datos personales. Ello se entiende sin perjuicio de otras responsabilidades que sean de aplicación al tratamiento en cuestión en virtud del Reglamento (UE) 2016/679.

Cláusula 17

Derecho aplicable

El presente pliego de cláusulas se regirá por el Derecho de un país que contemple los derechos de los terceros beneficiarios. Las partes acuerdan que sea el Derecho del país según se indique en el Acuerdo Marco.

Cláusula 18

Elección del foro y jurisdicción

Cualquier controversia derivada del presente pliego de cláusulas será resuelta judicialmente en el país según se indique en el Acuerdo Marco.

APÉNDICE

ANEXO I

A. LISTA DE PARTES

Exportador(es) de datos: [Identidad y datos de contacto del exportador o exportadores de datos y, en su caso, del delegado de protección de datos de este o estos y/o del representante en la Unión Europea]

1.**Nombre**: La entidad Glooko señalada en el Acuerdo Marco.

Dirección: La indicada en el Acuerdo Marco.

Nombre, cargo y datos de contacto de la persona de contacto: Jesper Forster, Delegado de Protección de Datos. Glooko AB, Nellickevägen 20B412 63 Gothenburg, Suecia. Email: dpo@glooko.com.

Actividades relacionadas con los datos transferidos en virtud del presente pliego de cláusulas: Facilitar los Entregables especificados en el Formulario de Pedido.

Firma y fecha: La indicada en el Formulario de Pedido correspondiente según el Acuerdo Marco.

Función (responsable/encargado): Encargado.

Importador(es) de datos: [Identidad y datos de contacto del importador o importadores de datos, incluida cualquier persona de contacto responsable de la protección de los datos]

1.**Nombre**: el Cliente (según se señala en el Formulario de Pedido aplicable)

Dirección: la dirección del Cliente (según se señala en el Formulario de Pedido aplicable)

Nombre, cargo y datos de contacto de la persona de contacto: la dirección del Cliente (según se señala en el Formulario de Pedido aplicable)

Actividades relacionadas con los datos transferidos en virtud del presente pliego de cláusulas: Recibir los Entregables especificados en el Formulario de Pedido aplicable.

Firma y fecha: La indicada en el Formulario de Pedido correspondiente según el Acuerdo Marco.

Función (responsable/encargado): Responsable.

B. DESCRIPCIÓN DE LA TRANSFERENCIA

Categorías de interesados cuyos datos personales se transfieren

- Usuarios Autorizados del Cliente
- Pacientes

Categorías de datos personales transferidos

Para Usuarios Autorizados del Cliente

- Información general (nombre)
- Datos de contacto (dirección de correo electrónico, número de teléfono)
- Información de uso (nombre de usuario, contraseña, derechos de acceso, registros de auditoría (logs))

Para Pacientes

- Información general (nombre, fecha de nacimiento, género)
- Datos de contacto (dirección postal, dirección de correo electrónico, número de teléfono)
- Información de uso (nombre de usuario, contraseña)
- Datos de salud (tipo de diabetes, año de diagnóstico de la diabetes, fecha estimada para dar a luz, rango objetivo, peso, altura, tratamientos)
- Información del dispositivo (número(s) de serie de la bomba de insulina, del medidor de glucosa y de la pluma de insulina, dosis, carbohidratos, ajustes, alarmas)

Datos sensibles transferidos (si procede) y restricciones o garantías aplicadas que tengan plenamente en cuenta la naturaleza de los datos y los riesgos que entrañan, como, por ejemplo, la limitación estricta de la finalidad, restricciones de acceso (incluido el acceso exclusivo del personal que haya hecho un curso especializado), un registro del acceso a los datos, restricciones a transferencias ulteriores o medidas de seguridad adicionales

- Datos relativos a la salud (tipo de diabetes, año de diagnóstico de la diabetes, fecha estimada para dar a luz, rango objetivo, peso, altura, tratamientos).

Restricciones de acceso al personal sobre el principio de "necesidad de conocer" (tanto para el encargado como el responsable).

Se grabará un registro de accesos a los datos.

Encriptación de los datos en tránsito y en reposo.

La frecuencia de la transferencia (por ejemplo, si los datos se transfieren de una vez o de forma periódica)

Los datos personales los almacena el encargado pero el responsable puede acceder a ellos en todo momento (si, por ejemplo, los Entregables consisten en un software como servicio [*software as a service*]). Los datos personales pueden en estos casos considerarse transferidos del EEE a terceros países.

Naturaleza del tratamiento

Cargar (upload), computar, analizar, visualizar, transferir y de otro modo tratar datos personales para permitir a los Usuarios Autorizados utilizar los Entregables.

Finalidad(es) de la transferencia y posterior tratamiento de los datos

La finalidad de la transferencia de datos es permitir al Cliente hacer uso de los Entregables.

El plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo

El Tratamiento no tiene un plazo definido y se llevará a cabo mientras los Entregables se pongan a disposición o hasta que el contrato de encargo de tratamiento aplicable se termine.

En caso de transferencia a (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento

No aplicable.

C. AUTORIDAD DE CONTROL COMPETENTE

Indíquese la autoridad o autoridades de control competentes de conformidad con la cláusula 13

No aplicable.

ANEXO II

MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

No aplicable.

ANEXO III:

LISTA DE SUBENCARGADOS DEL TRATAMIENTO

No aplicable.