



Clauses contractuelles types de GLOOKO

SECTION I

Clause 1

Objet et champ d'application

- a) Les présentes clauses contractuelles types (ci-après les «clauses») ont pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- b) Les responsables du traitement et les sous-traitants énumérés à l'annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 et/ou des dispositions de l'article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725.
- c) Les présentes clauses s'appliquent, si les exigences énoncées dans le Contrat-cadre sont remplies, au traitement des données à caractère personnel tel que décrit à l'annexe II.
- d) Les annexes I à IV font partie intégrante des clauses.
- e) Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
- f) Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

Clause 2

Invariabilité des clauses

- a) Les parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent.
- b) Les parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Clause 3

Interprétation

- a) Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 ou dans le règlement (UE) 2018/1725 figurent dans les clauses, ils s'entendent comme dans le règlement en question.
- b) Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et du règlement (UE) 2018/1725 respectivement.
- c) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 / le règlement (UE) 2018/1725 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

Hierarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

Clause 5 — Facultative

Clause d'amarrage

- a) Toute entité qui n'est pas partie aux présentes clauses peut, avec l'accord de toutes les parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l'annexe I.
- b) Une fois que les annexes mentionnées au point a) sont complétées et signées, l'entité adhérente est considérée comme une partie aux présentes clauses et jouit des droits et est soumise aux obligations d'un responsable du traitement ou d'un sous-traitant, conformément à sa désignation à l'annexe I.
- c) Les présentes clauses ne créent pour la partie adhérente aucun droit ni aucune obligation pour la période précédant l'adhésion.

SECTION II

OBLIGATIONS DES PARTIES

Clause 6

Description du ou des traitements

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l'annexe II.

Clause 7

Obligations des parties

7.1. Instructions

- a) Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.
- b) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 / du règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

7.2. Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du



traitement, telles que définies à l'annexe II, sauf instruction complémentaire du responsable du traitement.

7.3. Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'annexe II.

7.4. Sécurité du traitement

- a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.
- b) Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

7.5. Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

7.6. Documentation et conformité

- a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.
- b) Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.
- c) Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.
- d) Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.
- e) Les parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause,

y compris les résultats de tout audit.

7.7. Recours à des sous-traitants ultérieurs

- a) Le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins trente (30) jours à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.
- b) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
- c) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.
- d) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
- e) Le sous-traitant, lorsque cela est possible, convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

7.8. Transferts internationaux

- a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.
- b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

Assistance au responsable du traitement

- a) Le sous-traitant indique aux personnes concernées de contacter le responsable du traitement, si le sous-traitant reçoit une demande de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait autorisé.
- b) Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.
- c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant:
 - 1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel («analyse d'impact relative à la protection des données») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;
 - 2) l'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque;
 - 3) l'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes;
 - 4) les obligations prévues à l'article 32 du règlement (UE) 2016/679.
- d) Les parties définissent à l'annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

Clause 9

Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 ou des articles 34 et 35 du règlement (UE) 2018/1725, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

9.1. Violation de données en rapport avec des données traitées par le responsable du traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement:

- a) aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques);
- b) aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins:
 - 1) la nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
 - 2) les conséquences probables de la violation de données à caractère personnel;
 - 3) les mesures prises ou les mesures que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais;

- c) aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

9.2. Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins:

- a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés);
- b) les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel;
- c) ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les parties définissent à l'annexe III tous les autres éléments que le sous-traitant doit communiquer lorsqu'il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679.

Clause 10

Non-respect des clauses et résiliation

- a) Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le Contrat-cadre soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.
 - b) Le responsable du traitement est en droit de résilier le Contrat-cadre dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si:
 - 1) le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;
 - 2) le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725;
 - 3) le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
 - c) Le sous-traitant est en droit de résilier le Contrat-cadre dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.
 - d) À la suite de la résiliation du Contrat-cadre, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Si le responsable du traitement n'a pas demandé la restitution de toutes les données à caractère personnel traitées pour son compte dans un délai de trente (30) jours à compter de la résiliation du Contrat-cadre, le sous-traitant a le droit, à sa seule discrétion, de supprimer les données à caractère personnel. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.
-



ANNEXE I

Liste des parties

Responsable(s) du traitement:

1. Le Client (tel qu'identifié dans le Contrat-cadre ou le Bon de commande)

Sous-traitant(s):

1. Glooko AB (tel qu'identifié dans le Contrat-cadre)

—



ANNEXE II

Description du traitement

Catégories de personnes concernées dont les données à caractère personnel sont traitées

- Utilisateurs autorisés
- Patients

Catégories de données à caractère personnel traitées

Pour les Utilisateurs autorisés

- Informations générales (nom)
- Informations de contact (adresse email, numéro de téléphone)
- Informations sur l'utilisation (nom d'utilisateur, mot de passe, droits d'accès, logs d'audits)

Pour les Patients

- Informations générales (nom, date de naissance, sexe)
- Informations de contact (adresse postale, adresse email, numéro de téléphone)
- Informations sur l'utilisation (nom d'utilisateur, mot de passe)
- Données de santé (type de diabète, année de diagnostic du diabète, partus estimé, fourchette cible, poids, taille, traitements)
- Informations sur les appareils (numéro(s) de série de la pompe à insuline, du glucomètre et du stylo à insuline, doses, glucides, paramètres, alarmes)

Les données sensibles traitées (le cas échéant) et les limitations ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, tels que, par exemple, la limitation stricte de la finalité, les restrictions des accès (y compris l'accès réservé uniquement au personnel ayant suivi une formation spécialisée), la tenue d'un registre de l'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

- Données concernant la santé

Pour les informations concernant les mesures de protection mises en œuvre, voir l'annexe III.

Nature du traitement

Collecte, analyse, visualisation et autres traitements des données à caractère personnel conformément au Contrat-cadre.

Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement

Permettre au responsable du traitement et à ses Utilisateurs autorisés d'utiliser le Logiciel et les autres Produits Livrables conformément au Contrat-cadre.

Durée du traitement

Pour la durée de la mise à disposition du Logiciel et des autres Produits Livrables conformément au Contrat-cadre.



Pour le traitement par les sous-traitants (ultérieurs), préciser également l'objet, la nature et la durée du traitement.

Voir Annexe IV

Instructions au titre de la section 7.8 a) des Clauses relatives aux transferts internationaux

Les clauses contractuelles types pour les transferts internationaux (les "CCT") de l'annexe V s'appliqueront si le sous-traitant transfère des données à caractère personnel en dehors de l'EEE, vers un pays non reconnu par la Commission européenne comme assurant un niveau de protection adéquat des données à caractère personnel.

—



ANNEXE III

Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données

1. Objectif. La présente Annexe décrit le programme de sécurité, les certifications de sécurité et les mesures techniques et organisationnelles de Glooko visant à protéger (a) les données personnelles traitées par le sous-traitant pour le compte du responsable du traitement contre toute utilisation, tout accès, toute divulgation non autorisés ou tout vol et (b) le Logiciel. Au fur et à mesure que les menaces à la sécurité changent et évoluent, Glooko continue à mettre à jour son programme et sa stratégie de sécurité pour aider à protéger les données personnelles et le Logiciel. À ce titre, Glooko se réserve le droit de mettre à jour la présente Annexe à tout moment ; à condition, toutefois, qu'aucune mise à jour ne réduise de manière significative les protections globales énoncées dans la présente Annexe.
2. Organisation et Programme de sécurité. Glooko maintient un programme de sécurité fondé sur l'évaluation des risques. Le cadre du programme de sécurité de Glooko comprend des mesures de protection administratives, organisationnelles, techniques et physiques raisonnablement conçues pour protéger le Logiciel et la confidentialité, l'intégrité et la disponibilité des données personnelles. Le programme de sécurité de Glooko est conçu pour être adapté à la nature du Logiciel ainsi qu'à la taille et à la complexité des opérations commerciales de Glooko. Glooko dispose d'une équipe de sécurité de l'information distincte et dédiée qui gère le programme de sécurité de Glooko. Cette équipe facilite et vient au soutien des audits et évaluations indépendants réalisés par des tiers. Le cadre de sécurité de Glooko comprend des programmes couvrant : les Politiques et Procédures, la Gestion d'Actifs, la Gestion des Accès, la Cryptographie, la Sécurité Physique, la Sécurité Opérationnelle, la Sécurité des Communications, la Sécurité de la Continuité des Activités, la Sécurité des Personnes, la Sécurité des Produits, la Sécurité des Infrastructures de Cloud et de Réseau, la Conformité en matière de Sécurité, la Sécurité des Tiers, la Gestion des Vulnérabilités, ainsi que le Contrôle de la Sécurité et la Réaction aux Incidents. La sécurité est gérée aux plus hauts niveaux de l'entreprise, le Responsable de la Sécurité de Glooko rencontrant régulièrement la direction pour discuter des problèmes et coordonner les initiatives de sécurité à l'échelle de l'entreprise. Les politiques et normes de sécurité de l'information sont revues et approuvées par la direction au moins une fois par an et sont mises à la disposition de tous les employés de Glooko pour qu'ils puissent s'y référer.
3. Confidentialité. Glooko a mis en place des contrôles pour maintenir la confidentialité des données personnelles conformément au Contrat-Cadre. Tous les employés et le personnel sous contrat de Glooko sont liés par les politiques internes de Glooko concernant le maintien de la confidentialité des données personnelles et sont contractuellement tenus de respecter ces obligations.
4. Sécurité des Personnes
 - a. Vérification des Antécédents des Employés. Glooko vérifie les antécédents de tous les nouveaux employés au moment de l'embauche, conformément aux lois locales applicables. Glooko vérifie actuellement la formation et les emplois précédents d'un nouvel employé et effectue des vérifications des références. Lorsque la loi applicable l'autorise, Glooko peut également effectuer des vérifications des antécédents criminels, de crédit, d'immigration et de sécurité en fonction de la nature et de l'étendue du rôle du nouvel employé.



- b. Formation des Employés. Au moins une (1) fois par an, tous les employés de Glooko doivent suivre une formation sur la sécurité et la confidentialité qui couvre les politiques de sécurité de Glooko, les meilleures pratiques de sécurité et les principes de confidentialité. Les employés en congé peuvent disposer d'un délai supplémentaire pour suivre cette formation annuelle. L'équipe de sécurité dédiée de Glooko mène également des campagnes de sensibilisation au phishing et communique les menaces émergentes aux employés.
5. Gestion des Prestataires Tiers
 - a. Évaluation des Prestataires. Glooko peut faire appel à des prestataires tiers pour fournir le Logiciel. Avant de travailler avec des prestataires potentiels, Glooko procède à une évaluation des risques de sécurité de ces derniers afin de s'assurer qu'ils répondent aux exigences de sécurité de Glooko. Glooko examine périodiquement chaque prestataire à la lumière des normes de sécurité et de continuité des activités de Glooko, y compris concernant le type d'accès et la classification des données accessibles (le cas échéant), les contrôles nécessaires pour protéger les données et les exigences légales/réglementaires. Glooko s'assure que les données personnelles sont restituées et/ou supprimées à la fin de la relation avec un prestataire.
 - b. Accords avec les Prestataire. Glooko conclut des accords écrits avec tous ses prestataires, lesquels incluent des obligations de confidentialité, de protection de la vie privée et de sécurité qui assurent un niveau approprié de protection des données personnelles que ces prestataires peuvent traiter.
6. Architecture, Pare-feu et Ségrégation des Données. Tous les accès au réseau entre les hôtes de production sont limités, en utilisant des pare-feux pour permettre aux seuls services autorisés d'interagir dans le réseau de production. Les pare-feux sont utilisés pour gérer la ségrégation du réseau entre les différentes zones de sécurité dans les environnements de production et d'entreprise. Glooko sépare logiquement ses bases de données. Les API de Glooko sont conçues et construites pour identifier et autoriser l'accès uniquement vers et depuis les expéditeurs respectifs. Ces contrôles empêchent les clients d'avoir accès aux données d'autres clients.
7. Sécurité Physique. Les centres de données qui hébergent le Logiciel sont strictement contrôlés, tant au niveau du périmètre que des points d'entrée des bâtiments, par un personnel de sécurité professionnel utilisant la vidéosurveillance, des systèmes de détection d'intrusion et d'autres moyens électroniques. Des alimentations sans interruption et des générateurs sur site sont disponibles pour fournir une alimentation de secours en cas de panne électrique. De plus, le siège et les bureaux de Glooko disposent d'un programme de sécurité physique qui gère les visiteurs, les entrées du bâtiment et la sécurité générale des bureaux.
8. Sécurité dès la Conception. Glooko suit les principes de sécurité dès la conception lors de la conception du Logiciel. Glooko applique également le standard *Software Development Lifecycle (SDLC)* afin d'effectuer de nombreuses activités liées à la sécurité du Logiciel au cours des différentes phases du cycle de vie de création du produit, depuis la collecte des exigences et la conception du produit jusqu'à son déploiement.
9. Contrôles des Accès
 - a. Octroi d'Accès. Afin de minimiser le risque d'exposition des données, Glooko suit les principes du moindre privilège par le biais d'un modèle de contrôle d'accès par équipe lors de l'octroi de l'accès au système. Le personnel de Glooko est autorisé à accéder aux données personnelles en fonction chacun de



sa fonction, de son rôle et de ses responsabilités, et cet accès nécessite la validation du responsable de l'employé. L'accès d'un employé aux données personnelles est supprimé dès lors qu'il cesse sa fonction. Avant qu'un ingénieur ne soit autorisé à accéder à l'environnement de production, l'accès doit être approuvé par la direction et l'ingénieur est tenu de suivre des formations internes pour cet accès, y compris des formations sur les systèmes de l'équipe concernée. Glooko consigne les actions et les modifications à haut risque dans l'environnement de production. Glooko s'appuie sur l'automatisation pour identifier tout écart par rapport aux normes techniques internes qui pourrait indiquer une activité anormale/non autorisée afin de déclencher une alerte dans les minutes qui suivent un changement de configuration.

- b. Contrôle des Mots de Passe. Lorsqu'un Utilisateur Autorisé se connecte à son compte, Glooko hache les informations d'identification de l'utilisateur avant de les stocker. Les Clients peuvent également demander à leurs Utilisateurs autorisés d'ajouter une autre couche de sécurité à leur compte en utilisant une authentification à deux facteurs (2FA).
10. Gestion des Modifications. Glooko dispose d'un processus formel de gestion des modifications qu'il suit pour administrer les modifications apportées à l'environnement de production du Logiciel, y compris toute modification de ses logiciels sous-jacents, applications et systèmes. Chaque modification est soigneusement examinée et évaluée dans un environnement de test avant d'être déployée dans l'environnement de production du Logiciel. Toutes les modifications, y compris l'évaluation des modifications dans un environnement de test, sont documentées à l'aide d'un système d'enregistrement formel et vérifiable. L'approbation du déploiement des changements à haut risque est requise de la part des parties prenantes organisationnelles pertinentes. Des plans et des procédures sont également mis en œuvre dans le cas où une modification déployée doit être annulée pour préserver la sécurité du logiciel.
11. Chiffrement. Pour le Logiciel, (a) les bases de données qui stockent les données personnelles sont chiffrées en utilisant les *Advanced Encryption Standard* et (b) les données personnelles sont chiffrées lorsqu'elles transitent entre l'application logicielle du Client et le Logiciel en utilisant TLS v1.2.
12. Gestion des Vulnérabilités. Glooko maintient des contrôles et des politiques pour atténuer le risque de vulnérabilités de sécurité afin d'équilibrer le risque et les exigences commerciales/opérationnelles. Glooko utilise un outil tiers pour effectuer régulièrement des analyses de vulnérabilité afin d'évaluer les vulnérabilités de l'infrastructure cloud et des systèmes d'entreprise de Glooko.
13. Tests de Pénétration. Glooko effectue des tests de pénétration et engage des entités tierces indépendantes pour effectuer des tests de pénétration au niveau des applications. Les menaces de sécurité et les vulnérabilités détectées sont classées par ordre de priorité, triées et corrigées.
14. Gestion des Incidents de Sécurité. Glooko maintient des politiques de gestion des incidents de sécurité. L'Equipe de Réponse aux Incidents de Sécurité de Glooko (T-SIRT) évalue toutes les menaces et les vulnérabilités de sécurité pertinentes et établit des actions de remédiation et d'atténuation appropriées. Glooko conserve ses registres de sécurité pertinents.
15. Résilience et Continuité du Logiciel. Le Logiciels utilise une variété d'outils et de mécanismes pour atteindre une disponibilité et une résilience élevées. Pour le Logiciel, l'infrastructure de Glooko s'étend sur plusieurs zones de disponibilité indépendantes des pannes dans des régions géographiques physiquement séparées les unes des autres.



Glooko utilise également des outils spécialisés qui contrôlent les performances des serveurs, les données et la capacité de charge du trafic dans chaque zone de disponibilité et centre de données de colocation. Si des performances de serveur suboptimales ou une capacité surchargée sont détectées sur un serveur au sein d'une zone de disponibilité ou d'un centre de données de colocation, ces outils spécialisés augmentent la capacité ou déplacent le trafic pour soulager une performance de serveur suboptimale ou une surcharge de capacité. Glooko est également immédiatement informé en cas de performance suboptimale d'un serveur ou d'une surcharge de capacité.

16. Sauvegardes et Récupération. Glooko effectue des sauvegardes régulières des données personnelles. Les données personnelles qui sont sauvegardées sont conservées de manière redondante dans plusieurs zones de disponibilité et chiffrées en transit et au repos à l'aide des *Advanced Encryption Standards*.



ANNEXE IV

Liste de sous-traitants ultérieurs

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants:

1. Nom: Amazon Web Services EMEA SARL

Adresse: 38 avenue John F. Kennedy, L1855, Luxembourg

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés): Fournisseur de services Cloud

2. Nom : Cegedim SA

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

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés): Fournisseur de services Cloud (peut être utilisé pour les Clients situés en France)

3. Nom: Pictime Groupe

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

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés): Hébergeur de Données de Santé (peut être utilisé pour les Clients situés en France et en Allemagne)

Clause Contractuelles Types pour les Transferts Internationaux (CCT)

SECTION I

Clause 1

Finalités et champ d'application

- (a) Les présentes clauses contractuelles types visent à garantir le respect des exigences du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)¹ en cas de transfert de données à caractère personnel vers un pays tiers.
- (b) Les parties:
- (i) la ou les personnes physiques ou morales, la ou les autorités publiques, la ou les agences ou autre(s) organisme(s) (ci-après la ou les «entités») qui transfèrent les données à caractère personnel, mentionnés à l'annexe I.A. (ci-après l'«exportateur de données»), et
 - (ii) la ou les entités d'un pays tiers qui reçoivent les données à caractère personnel de l'exportateur de données, directement ou indirectement par l'intermédiaire d'une autre entité également partie aux présentes clauses, mentionnées à l'annexe I.A. (ci-après l'«importateur de données»)
- sont convenues des présentes clauses contractuelles types (ci-après les «clauses»).
- (c) Les présentes clauses s'appliquent au transfert de données à caractère personnel précisé à l'annexe I.B.
- (d) L'appendice aux présentes clauses, qui contient les annexes qui y sont mentionnées, fait partie intégrante des présentes clauses.

Clause 2

Effet et invariabilité des clauses

- (a) Les présentes clauses établissent des garanties appropriées, notamment des droits opposables pour la personne concernée et des voies de droit effectives, en vertu de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679 et, en ce qui concerne les transferts de données de responsables du traitement à sous-traitants et/ou de sous-traitants à sous-traitants, des clauses contractuelles types en vertu de l'article 28, paragraphe 7, du règlement (UE) 2016/679, à condition qu'elles ne soient pas modifiées, sauf pour sélectionner le ou les modules appropriés ou pour ajouter ou mettre à jour des informations dans l'appendice. Cela n'empêche pas les parties d'inclure les clauses contractuelles types prévues dans les présentes clauses dans un contrat plus large et/ou d'ajouter d'autres clauses ou des

¹ Si l'exportateur de données est un sous-traitant soumis au règlement (UE) 2016/679 agissant pour le compte d'une institution ou d'un organe de l'Union en tant que responsable du traitement, le recours aux présentes clauses lors du recrutement d'un autre sous-traitant (sous-traitance ultérieure) qui n'est pas soumis au règlement (UE) 2016/679 garantit également le respect de l'article 29, paragraphe 4, du règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39), dans la mesure où les présentes clauses et les obligations en matière de protection des données fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément à l'article 29, paragraphe 3, du règlement (UE) 2018/1725 sont alignées. Ce sera en particulier le cas lorsque le responsable du traitement et le sous-traitant se fondent sur les clauses contractuelles types qui figurent dans la décision [...].



garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les présentes clauses et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

- (b) Les présentes clauses sont sans préjudice des obligations auxquelles l'exportateur de données est soumis en vertu du règlement (UE) 2016/679.

Clause 3

Tiers bénéficiaires

- (a) Les personnes concernées peuvent invoquer et faire appliquer les présentes clauses, en tant que tiers bénéficiaires, contre l'exportateur et/ou l'importateur de données, avec les exceptions suivantes:
 - (i) clause 1, clause 2, clause 3, clause 6, clause 7;
 - (ii) clause 8 - module 1: clause 8.5, paragraphe e), et clause 8.9, paragraphe b); module 2: clause 8.1, paragraphe b), clause 8.9, paragraphes a), c), d) et e); module 3: clause 8.1, paragraphes a), c) et d) et clause 8.9, paragraphes a), c), d), e), f) et g); module 4: clause 8.1, paragraphe b), et clause 8.3, paragraphe b);
 - (iii) clause 9 - module 2: clause 9, paragraphes a), c), d) et e); module 3: clause 9, paragraphes a) c), d) et e);
 - (iv) clause 12 - module 1: clause 12, paragraphes a) et d); modules 2 et 3: clause 12, paragraphes a), d) et f);
 - (v) clause 13;
 - (vi) clause 15.1, paragraphes c), d) et e);
 - (vii) clause 16, paragraphe e);
 - (viii) clause 18 - modules 1, 2 et 3: clause 18, paragraphes a) et b); module 4: clause 18.
- (b) Le paragraphe a) est sans préjudice des droits des personnes concernées au titre du règlement (UE) 2016/679.

Clause 4

Interprétation

- (a) Lorsque les présentes clauses utilisent des termes définis dans le règlement (UE) 2016/679, ceux-ci ont la même signification que dans ledit règlement.
- (b) Les présentes clauses sont lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.
- (c) Les présentes clauses ne sont pas interprétées dans un sens contraire aux droits et obligations prévus dans le règlement (UE) 2016/679.

Clause 5

Hierarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes entre les parties existant au moment où les présentes clauses sont convenues, ou souscrites par la suite, les présentes clauses prévalent.



Clause 6

Description du ou des transferts

Les détails du ou des transferts, en particulier les catégories de données à caractère personnel qui sont transférées et la ou les finalités pour lesquelles elles le sont, sont précisés à l'annexe I.B.

Clause 7 - Facultative

Clause d'adhésion

Non applicable

SECTION II – OBLIGATIONS DES PARTIES

Clause 8

Garanties en matière de protection des données

L'exportateur de données garantit qu'il a entrepris des démarches raisonnables pour s'assurer que l'importateur de données est à même, par la mise en œuvre de mesures techniques et organisationnelles appropriées, de satisfaire aux obligations qui lui incombent en vertu des présentes clauses.

8.1 Instructions

- (a) L'exportateur de données ne traite les données à caractère personnel que sur instructions documentées de l'importateur de données agissant en tant que son responsable du traitement.
- (b) S'il n'est pas en mesure de suivre ces instructions, notamment si elles constituent une violation du règlement (UE) 2016/679 ou d'autres dispositions législatives de l'Union ou d'un État membre en matière de protection des données, l'exportateur de données en informe immédiatement l'importateur de données.
- (c) L'importateur de données s'abstient de tout acte susceptible d'empêcher l'exportateur de données de s'acquitter des obligations qui lui incombent en vertu du règlement (UE) 2016/679, notamment dans le cadre d'une sous-traitance ultérieure ou en ce qui concerne la coopération avec les autorités de contrôle compétentes.
- (d) Au terme de la prestation des services de traitement, l'exportateur de données, à la convenance de l'importateur de données, efface toutes les données à caractère personnel traitées pour le compte de ce dernier et lui en apporte la preuve, ou lui restitue toutes les données à caractère personnel traitées pour son compte et efface les copies existantes.

8.2 Sécurité du traitement

- (a) Les parties mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, notamment pendant la transmission, et pour les protéger d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé (ci-après la «violation de données à caractère personnel»). Lors de l'évaluation du niveau de sécurité approprié, elles tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre, de la nature des données à caractère personnel², de la nature, de la portée, du

² Il s'agit notamment de savoir si le transfert et le traitement ultérieur portent sur des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données



contexte et de la ou des finalités du traitement ainsi que des risques inhérents au traitement pour les personnes concernées, et envisagent en particulier de recourir au chiffrement ou à la pseudonymisation, notamment pendant la transmission, lorsque la finalité du traitement peut être atteinte de cette manière.

- (b) L'exportateur de données aide l'importateur de données à garantir une sécurité appropriée des données conformément au paragraphe a). En cas de violation de données à caractère personnel concernant les données à caractère personnel traitées par l'exportateur de données au titre des présentes clauses, ce dernier en informe l'importateur de données dans les meilleurs délais après avoir eu connaissance de la violation et l'aide à y remédier.
- (c) L'exportateur de données veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

8.3 Documentation et conformité

- (a) Les parties sont en mesure de démontrer le respect des présentes clauses.
- (b) L'exportateur de données met à la disposition de l'importateur de données toutes les informations nécessaires pour démontrer le respect des obligations qui lui incombent au titre des présentes clauses et pour permettre la réalisation d'audits et y contribuer.

Clause 9

Recours à des sous-traitants ultérieurs

Non applicable

Clause 10

Droits des personnes concernées

Les parties se prêtent mutuellement assistance pour répondre aux demandes de renseignements et aux autres demandes formulées par les personnes concernées en vertu de la législation locale applicable à l'importateur de données ou, en cas de traitement par l'exportateur de données dans l'UE, en vertu du règlement (UE) 2016/679.

Clause 11

Voies de recours

- (a) L'importateur de données informe les personnes concernées, sous une forme transparente et aisément accessible, au moyen d'une notification individuelle ou sur son site web, d'un point de contact autorisé à traiter les réclamations. Il traite sans délai toute réclamation reçue d'une personne concernée.

Clause 12

Responsabilité



- (a) Chaque partie est responsable envers la ou les autres parties de tout dommage qu'elle cause à l'autre ou aux autres parties du fait d'un manquement aux présentes clauses.
- (b) Chaque partie est responsable à l'égard de la personne concernée, et la personne concernée a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par une partie du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses. Ceci est sans préjudice de la responsabilité de l'exportateur de données en vertu du règlement (UE) 2016/679.
- (c) Lorsque plusieurs parties sont responsables d'un dommage causé à la personne concernée du fait d'une violation des présentes clauses, toutes les parties responsables le sont conjointement et solidairement et la personne concernée a le droit d'intenter une action en justice contre n'importe laquelle de ces parties.
- (d) Les parties conviennent que, si la responsabilité d'une d'entre elles est reconnue en vertu du paragraphe c), celle-ci est en droit de réclamer auprès de l'autre ou des autres parties la part de la réparation correspondant à sa/leur part de responsabilité dans le dommage.
- (e) L'importateur de données ne peut invoquer le comportement d'un sous-traitant ou d'un sous-traitant ultérieur pour échapper à sa propre responsabilité.

Clause 13

Contrôle

Non applicable

**SECTION III – LÉGISLATIONS LOCALES ET OBLIGATIONS EN CAS D'ACCÈS
DES AUTORITÉS PUBLIQUES**

Clause 14

Législations et pratiques locales ayant une incidence sur le respect des clauses

Non applicable

Clause 15

Obligations de l'importateur de données en cas d'accès des autorités publiques

Non applicable



SECTION IV — DISPOSITIONS FINALES

Clause 16

Non-respect des clauses et résiliation

- (a) L'importateur de données informe sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses, quelle qu'en soit la raison.
- (b) Dans le cas où l'importateur de données enfreint les présentes clauses ou n'est pas en mesure de les respecter, l'exportateur de données suspend le transfert de données à caractère personnel à l'importateur de données jusqu'à ce que le respect des présentes clauses soit à nouveau garanti ou que le contrat soit résilié. Ceci est sans préjudice de la clause 14, paragraphe f).
- (c) L'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses, lorsque:
 - (i) l'exportateur de données a suspendu le transfert de données à caractère personnel à l'importateur de données en vertu du paragraphe b) et que le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;
 - (ii) l'importateur de données enfreint gravement ou de manière persistante les présentes clauses; ou
 - (iii) l'importateur de données ne se conforme pas à une décision contraignante d'une juridiction ou d'une autorité de contrôle compétente concernant les obligations qui lui incombent au titre des présentes clauses.

Dans ces cas, il informe l'autorité de contrôle compétente de ce non-respect. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement.

- (d) Les données à caractère personnel collectées par l'exportateur de données dans l'UE qui ont été transférées avant la résiliation du contrat au titre du paragraphe (c), ainsi que toute copie de celles-ci, sont immédiatement effacées dans leur intégralité. L'importateur de données apporte la preuve de l'effacement des données à l'exportateur de données. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel transférées, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données que dans la mesure où et aussi longtemps que cette législation locale l'exige.
- (e) Chaque partie peut révoquer son consentement à être liée par les présentes clauses i) si la Commission européenne adopte une décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 qui couvre le transfert de données à caractère personnel auquel les présentes clauses s'appliquent; ou ii) si le règlement (UE) 2016/679 est intégré dans le cadre juridique du pays vers lequel les données à caractère personnel sont transférées. Ceci est sans préjudice des autres obligations qui s'appliquent au traitement en question en vertu du règlement (UE) 2016/679.

Clause 17

Droit applicable



Les présentes clauses sont régies par le droit d'un pays qui reconnaît des droits au tiers bénéficiaire. Les parties conviennent qu'il s'agit du droit du pays tel que spécifié dans le Contrat-cadre.

Clause 18

Élection de for et juridiction

Tout litige survenant du fait des présentes clauses est tranché par les juridictions du pays spécifié dans le Contrat-cadre.



APPENDICE

ANNEXE I

A. LISTE DES PARTIES

1. Exportateur(s) de données: [*Identité et coordonnées du ou des exportateurs de données et, le cas échéant, de leur délégué à la protection des données et/ou de leur représentant dans l'Union européenne*]

1. Nom: L'entité Glooko telle que spécifiée dans le Contrat-cadre

Adresse: Telle que spécifiée dans le Contrat-cadre

Nom, fonction et coordonnées de la personne de contact: Jesper Forster, Data Protection Officer. Glooko AB, Nellickevägen 20B412 63 Gothenburg, Sweden. Email: dpo@glooko.com

Activités en rapport avec les données transférées au titre des présentes clauses: Fourniture des Produits livrables tels que spécifiés dans le Bon de commande applicable

Signature et date : Telles que spécifiées dans le Bon de commande applicable, conformément au Contrat-cadre

Rôle (responsable du traitement/sous-traitant) : Sous-traitant

2. Importateur(s) de données: [*Identité et coordonnées du ou des importateurs de données, y compris de toute personne de contact chargée de la protection des données*]

1. Nom: Client (tel que spécifié dans le Bon de commande applicable)

Adresse: Adresse du Client (telle que spécifiée dans le Bon de commande applicable)

Nom, fonction et coordonnées de la personne de contact: Adresse du Client (telle que spécifiée dans le Bon de commande applicable)

Activités en rapport avec les données transférées au titre des présentes clauses: Recevoir les Produits livrables tels que spécifiés dans le Bon de commande applicable

Signature et date: Telles que spécifiées dans le Bon de commande applicable, conformément au Contrat-cadre

Rôle (responsable du traitement/sous-traitant): Responsable du traitement

B. DESCRIPTION DU TRANSFERT

Catégories de personnes concernées dont les données à caractère personnel sont transférées

- Utilisateurs autorisés du Client
- Patients

Catégories de données à caractère personnel transférées

Pour les Utilisateurs autorisés du Client

- Informations générales (nom)
- Informations de contact (adresse email, numéro de téléphone)
- Informations sur l'utilisation (nom d'utilisateur, mot de passe, droits d'accès, logs)



d'audits)

Pour les Patients

- Informations générales (nom, date de naissance, sexe)
- Informations de contact (adresse postale, adresse email, numéro de téléphone)
- Informations sur l'utilisation (nom d'utilisateur, mot de passe)
- Données de santé (type de diabète, année de diagnostic du diabète, partus estimé, fourchette cible, poids, taille, traitements)
- Informations sur les appareils (numéro(s) de série de la pompe à insuline, du glucomètre et du stylo à insuline, doses, glucides, paramètres, alarmes)

Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que la limitation stricte des finalités, les restrictions d'accès (notamment l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

- Données de santé (type de diabète, année de diagnostic du diabète, partus estimé, fourchette cible, poids, taille, traitements)

Restrictions d'accès au personnel qui a uniquement besoin de connaître les informations (tant pour le sous-traitant que pour le responsable du traitement).

L'accès aux données est consigné dans un journal.

Les données en transit et au repos sont cryptées.

Fréquence du transfert (indiquez, par exemple, si les données sont transférées sur une base ponctuelle ou continue).

Les données à caractère personnel sont stockées par le sous-traitant, mais le responsable du traitement peut y accéder à tout moment (si, par exemple, les Produits livrables consistent en un logiciel en SaaS). Les données à caractère personnel pourraient dans ce cas être considérées comme transférées de l'EEE vers un pays tiers.

Nature du traitement

Télécharger, calculer, analyser, visualiser, transférer et traiter de toute autre manière les données personnelles pour permettre aux Utilisateurs autorisés d'utiliser les Produits livrables.

Finalité(s) du transfert et du traitement ultérieur des données

La finalité du transfert est de permettre au Client d'utiliser les Produits livrables.

Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères utilisés pour déterminer cette durée

Le Traitement n'est pas limité dans le temps et est réalisé tant que les Produits livrables sont fournis



ou jusqu'à ce que l'accord de traitement des données personnelles applicable soit résilié.

Pour les transferts à des sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature et la durée du traitement

Non applicable

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

Indiquez la ou les autorités de contrôle compétentes conformément à la clause 13

Non applicable



**ANNEXE II - MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS
LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR
LA SÉCURITÉ DES DONNÉES**

Non applicable

ANNEXE III – Liste des sous-traitants ultérieurs

Non applicable