ANEXO 2

CLÁUSULAS CONTRATUAIS-TIPO DA GLOOKO

SECÇÃO I

Cláusula 1.ª

Finalidade e âmbito

(a) A finalidade das presentes Cláusulas Contratuais-Tipo (as Cláusulas) é assegurar o cumprimento do artigo 28.º, n.os 3 e 4 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

(b) Os responsáveis pelo tratamento e os subcontratantes indicados no Anexo I concordaram com as presentes Cláusulas para garantir a conformidade com o artigo 28.º, n.os 3 e 4 do Regulamento (UE) 2016/679 e/ou com o artigo 29.º, n.os 3 e 4 do Regulamento (UE) 2018/1725.

(c) As presentes Cláusulas aplicam-se ao tratamento de dados pessoais, conforme especificado no Anexo II.

(d) Os Anexos I a IV são parte integrante das Cláusulas.

(e) As presentes Cláusulas não prejudicam as obrigações a que o responsável pelo tratamento está sujeito ao abrigo do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725.

(f) As presentes Cláusulas não garantem, por si só, o cumprimento das obrigações relacionadas com transferências internacionais, em conformidade com o Capítulo V do Regulamento (UE) 2016/679 e/ou o Regulamento (UE) 2018/1725.

Cláusula 2.ª

Invariabilidade das Cláusulas

(a) As Partes comprometem-se a não alterar as Cláusulas, exceto no que se refere à adição de informações aos Anexos ou à atualização das informações contidas nos mesmos.

(b) Tal não impede as Partes de incluir as cláusulas contratuais-tipo previstas nas presentes Cláusulas num contrato mais amplo ou de acrescentar outras cláusulas ou salvaguardas adicionais, desde que não contradigam direta ou indiretamente as Cláusulas ou prejudiquem os direitos ou liberdades fundamentais dos titulares dos dados.

Cláusula 3.ª

Interpretação

(a) Quando as presentes Cláusulas utilizarem os termos definidos no Regulamento (UE) 2016/679 ou no Regulamento (UE) 2018/1725, respetivamente, esses termos terão o mesmo significado que no referido Regulamento.

(b) As presentes Cláusulas devem ser lidas e interpretadas à luz das disposições do Regulamento (UE) 2016/679 ou do Regulamento (UE) 2018/1725, respetivamente.

(c) As presentes Cláusulas não devem ser interpretadas de forma contrária aos direitos e obrigações previstos no Regulamento (UE) 2016/679 ou no Regulamento (UE) 2018/1725, ou de forma a prejudicar os direitos ou liberdades fundamentais dos titulares dos dados.

Cláusula 4.ª

Hierarquia

Em caso de contradição entre as presentes Cláusulas e as disposições de acordos conexos entre as Partes existentes no momento em que as presentes Cláusulas forem acordadas ou posteriormente celebrados, as presentes Cláusulas prevalecerão.

Cláusula 5.ª – Opcional

Cláusula de acoplagem

(a) Qualquer entidade que não seja Parte nas presentes Cláusulas pode, com o acordo de todas as Partes, aderir às presentes Cláusulas em qualquer momento enquanto responsável pelo tratamento ou subcontratante, preenchendo os Anexos e assinando o Anexo I.

(b) Uma vez preenchidos e assinados os Anexos indicados na alínea a), a entidade aderente será tratada como Parte nas presentes Cláusulas e terá os direitos e obrigações de um responsável pelo tratamento ou subcontratante, em conformidade com a sua designação no Anexo I.

(c) A entidade aderente não terá quaisquer direitos ou obrigações decorrentes das presentes Cláusulas referentes ao período anterior à sua adesão enquanto Parte.

SECÇÃO II – OBRIGAÇÕES DAS PARTES

Cláusula 6.ª

Descrição do(s) tratamento(s)

Os pormenores das operações de tratamento, nomeadamente as categorias de dados pessoais e as finalidades de tratamento para as quais os dados pessoais são tratados em nome do responsável pelo tratamento, são especificados no Anexo II.

Cláusula 7.ª

Obrigações das Partes

7.1. Instruções

(a) O subcontratante deve tratar os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, a menos que lhe seja exigido que o faça de acordo com a legislação da União ou dos Estados-Membros a que o subcontratante está sujeito. Neste caso, o subcontratante deve informar o responsável pelo tratamento desse requisito legal antes do tratamento, a menos que a lei o proíba por motivos importantes de interesse público. O responsável pelo tratamento pode também fornecer instruções subsequentes durante todo o tratamento dos dados pessoais. Estas instruções devem ser sempre documentadas.

(b) O subcontratante deverá informar imediatamente o responsável pelo tratamento se, na opinião do subcontratante, as instruções dadas pelo responsável pelo tratamento infringirem o Regulamento (UE) 2016/679 ou o Regulamento (UE) 2018/1725, ou as disposições aplicáveis de proteção de dados da União ou dos Estados-Membros.

7.2. Limitação da finalidade

O subcontratante apenas tratará os dados pessoais para a(s) finalidade(s) específica(s) do tratamento, conforme estabelecido no Anexo II, a menos que receba instruções adicionais do responsável pelo tratamento.

7.3. Duração do tratamento de dados pessoais

O tratamento por parte do subcontratante só será efetuado durante o período especificado no Anexo II.

7.4. Segurança de tratamento

(a) O subcontratante deverá aplicar, pelo menos, as medidas técnicas e organizativas especificadas no Anexo III para garantir a segurança dos dados pessoais. Tal inclui a proteção dos dados contra uma violação de segurança que resulte em destruição, perda, alteração, divulgação não autorizada ou acesso aos dados acidental ou ilegal (violação de dados pessoais). Ao avaliarem o nível de segurança adequado, as Partes terão em devida consideração o estado da arte, os custos de implementação, a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos inerentes para os titulares dos dados.

(b) O subcontratante só deverá conceder aos membros do seu pessoal o acesso aos dados pessoais que estão a ser tratados na medida do estritamente necessário para a implementação, gestão e monitorização do contrato. O subcontratante deverá garantir que as pessoas autorizadas a tratar os dados pessoais recebidos se comprometeram com a confidencialidade ou estão sob uma obrigação legal de confidencialidade adequada.

7.5. Dados sensíveis

Se o tratamento envolver dados pessoais reveladores de origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, dados genéticos ou dados biométricos para efeitos de identificação exclusiva de uma pessoa singular, dados relativos à saúde ou à vida sexual ou orientação sexual de uma pessoa, ou dados relativos a condenações penais e infrações ("dados sensíveis"), o subcontratante deverá aplicar restrições específicas e/ou salvaguardas adicionais.

7.6 Documentação e conformidade

(a) As Partes deverão demonstrar a conformidade com as presentes Cláusulas.

(b) O subcontratante deverá responder de forma oportuna e adequada a questões do responsável pelo tratamento sobre o tratamento de dados, em conformidade com as presentes Cláusulas.

(c) O subcontratante deverá disponibilizar ao responsável pelo tratamento todas as informações necessárias para demonstrar a conformidade com as obrigações estabelecidas nas presentes Cláusulas e que decorrem diretamente do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725. A pedido do responsável pelo tratamento, o subcontratante deverá também permitir e contribuir para auditorias das atividades de tratamento abrangidas pelas presentes Cláusulas, em intervalos razoáveis ou se existirem indícios de não conformidade. Ao decidir sobre uma revisão ou auditoria, o responsável pelo tratamento pode ter em consideração as certificações relevantes detidas pelo subcontratante.

(d) O responsável pelo tratamento pode optar por realizar a auditoria sozinho ou mandatar um auditor independente. As auditorias podem igualmente incluir inspeções no local ou nas instalações físicas do subcontratante e, se for caso disso, serão efetuadas com um aviso prévio razoável.

(e) As Partes porão à disposição da(s) autoridade(s) de controlo competente(s), a pedido, as informações referidas na presente Cláusula, incluindo os resultados de quaisquer auditorias.

7.7. Utilização de subcontratantes ulteriores

(a) O subcontratante tem a autorização geral do responsável pelo tratamento para a contratação de subcontratantes ulteriores a partir de uma lista acordada. O subcontratante deverá informar por escrito o responsável pelo tratamento de quaisquer alterações previstas à lista em questão, através da adição ou substituição de subcontratantes ulteriores, com pelo menos trinta (30) dias de antecedência, dando assim tempo suficiente ao responsável pelo tratamento para poder opor-se a tais alterações antes da contratação do(s) subcontratante(s) ulterior(es) em causa. O subcontratante deverá fornecer ao responsável pelo tratamento as informações necessárias para permitir que o responsável pelo tratamento exerça o direito de oposição.

(b) Quando o subcontratante contratar um subcontratante ulterior para a realização de atividades de tratamento específicas (em nome do responsável pelo tratamento), fá-lo-á através de um contrato que impõe, em substância, ao subcontratante ulterior as mesmas obrigações de proteção de dados que as impostas ao subcontratante em conformidade com as presentes Cláusulas. O subcontratante deverá garantir que o subcontratante ulterior cumpre as obrigações a que o subcontratante está sujeito nos termos das presentes Cláusulas e do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725.

(c) A pedido do responsável pelo tratamento, o subcontratante deverá fornecer uma cópia do acordo do subcontratante ulterior em questão e quaisquer alterações subsequentes ao responsável pelo tratamento. Na medida do necessário para proteger o segredo comercial ou outras informações confidenciais, incluindo dados pessoais, o subcontratante pode redigir o texto do acordo antes de partilhar a cópia.

(d) O subcontratante continuará a ser plenamente responsável perante o responsável pelo tratamento pelo cumprimento das obrigações do subcontratante ulterior, em conformidade com o contrato celebrado com o subcontratante ulterior. O subcontratante deverá notificar o responsável pelo tratamento de qualquer incumprimento por parte do subcontratante ulterior das suas obrigações contratuais.

(e) O subcontratante deverá acordar, sempre que possível, uma cláusula de terceiro beneficiário com o subcontratante ulterior, mediante a qual, no caso de o subcontratante ter desaparecido factualmente, ter deixado de existir por lei ou se ter tornado insolvente, o responsável pelo tratamento terá o direito de cessar o contrato do subcontratante ulterior e de o instruir a apagar ou devolver os dados pessoais.

7.8. Transferências internacionais

(a) Qualquer transferência de dados para um país terceiro ou uma organização internacional pelo subcontratante só será efetuada com base nas instruções documentadas do responsável pelo tratamento ou para cumprir um requisito específico ao abrigo da legislação da União ou dos Estados-Membros a que o subcontratante está sujeito e terá lugar em conformidade com o Capítulo V do Regulamento (UE) 2016/679 ou do Regulamento (UE) 2018/1725.

(b) O responsável pelo tratamento concorda que, quando o subcontratante contrata um subcontratante ulterior, em conformidade com a Cláusula 7.7. para a realização de atividades de tratamento específicas (em nome do responsável pelo tratamento) e essas atividades de tratamento implicam uma transferência de dados pessoais na aceção do Capítulo V do Regulamento (UE) 2016/679, o subcontratante e o subcontratante ulterior podem garantir a conformidade com o Capítulo V do Regulamento (UE) 2016/679 utilizando cláusulas contratuais-tipo adotadas pela Comissão em conformidade com o artigo 46.º, n.º 2 do Regulamento (UE) 2016/679, desde que sejam cumpridas as condições para a utilização das cláusulas contratuais-tipo em questão.

Cláusula 8.ª

Assistência ao responsável pelo tratamento

(a) O subcontratante deverá encaminhar os titulares dos dados para contactarem o responsável pelo tratamento, caso o subcontratante receba um pedido de um titular dos dados. Não deve responder ao pedido propriamente dito, salvo com autorização para o fazer por parte do responsável pelo tratamento.

(b) O subcontratante deverá ajudar o responsável pelo tratamento no cumprimento das suas obrigações de resposta aos pedidos dos titulares dos dados para o exercício dos respetivos direitos, tendo em conta a natureza do tratamento. No cumprimento das suas obrigações nos termos das alíneas a) e b), o subcontratante deverá respeitar as instruções do responsável pelo tratamento.

(c) Além da obrigação do subcontratante de prestar assistência ao responsável pelo tratamento, nos termos da alínea b) da Cláusula 8.ª, o subcontratante deverá prestar ainda assistência ao responsável pelo tratamento a fim de garantir o cumprimento das seguintes obrigações, tendo em conta a natureza do tratamento de dados e as informações de que dispõe o subcontratante:

(1) a obrigação de proceder a uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais (uma "avaliação do impacto da proteção de dados") sempre que um tipo de tratamento possa conduzir a um risco elevado para os direitos e liberdades das pessoas singulares;

(2) a obrigação de consultar a(s) autoridade(s) de controlo competente(s) antes do tratamento, sempre que uma avaliação de impacto da proteção de dados indicar que o tratamento resultaria num risco elevado na ausência de medidas tomadas pelo responsável pelo tratamento para atenuar o risco;

(3) a obrigação de garantir que os dados pessoais são precisos e atualizados, informando imediatamente o responsável pelo tratamento se o subcontratante tomar conhecimento de que os dados pessoais que está a tratar estão incorretos ou se tornaram desatualizados;

(4) as obrigações previstas no artigo 32.º do Regulamento (UE) 2016/679.

(d) As Partes definirão no Anexo III as medidas técnicas e organizativas adequadas através das quais o subcontratante é obrigado a prestar assistência ao responsável pelo tratamento na aplicação da presente Cláusula, bem como o âmbito e a extensão da assistência necessária.

Cláusula 9.ª

Notificação de violação de dados pessoais

Em caso de violação de dados pessoais, o subcontratante deverá cooperar com o responsável pelo tratamento e prestar-lhe assistência para que este cumpra as suas obrigações nos termos dos artigos 33.º e 34.º do Regulamento (UE) 2016/679 ou dos artigos 34.º e 35.º do Regulamento (UE) 2018/1725, quando aplicável, tendo em conta a natureza do tratamento e as informações disponíveis para o subcontratante.

9.1 Violação de dados relativa a dados tratados pelo responsável pelo tratamento

Em caso de violação de dados pessoais relativamente a dados tratados pelo responsável pelo tratamento, o subcontratante deverá auxiliar o responsável pelo tratamento:

(a) a notificar a violação de dados pessoais à(s) autoridade(s) de controlo competente(s), sem demora injustificada após o responsável pelo tratamento ter conhecimento da mesma, quando relevante/(a menos que a violação de dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares);

(b) a obter as seguintes informações que, nos termos do artigo 33.º, n.º 3 do Regulamento (UE) 2016/679, devem ser indicadas na notificação do responsável pelo tratamento e devem incluir, pelo menos:

(1) a natureza dos dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de titulares dos dados em causa, bem como as categorias e o número aproximado de registos de dados pessoais em causa;

(2) as consequências prováveis da violação de dados pessoais;

(3) as medidas tomadas ou propostas a tomar pelo responsável pelo tratamento para resolver a violação de dados pessoais, incluindo, se for caso disso, medidas destinadas a atenuar os seus possíveis efeitos adversos.

Sempre que, e na medida em que, não seja possível fornecer todas estas informações simultaneamente, a notificação inicial deve conter as informações então disponíveis e, à medida que estas se tornem disponíveis, as informações adicionais devem ser fornecidas sem demora injustificada.

(c) a cumprir, nos termos do artigo 34.º do Regulamento (UE) 2016/679, a obrigação de comunicar sem demora injustificada a violação de dados pessoais ao titular dos dados, quando a violação de dados pessoais for suscetível de resultar num risco elevado para os direitos e liberdades das pessoas singulares.

9.2 Violação de dados relativa a dados tratados pelo subcontratante

Em caso de violação de dados pessoais relativamente a dados tratados pelo subcontratante, este deverá notificar o responsável pelo tratamento sem demora injustificada depois de ter conhecimento da violação. Tal notificação deve conter, pelo menos:

(a) uma descrição da natureza da violação (incluindo, se possível, as categorias e o número aproximado de titulares dos dados e registos de dados em causa);

(b) os detalhes de um ponto de contacto onde podem ser obtidas mais informações relativas à violação de dados pessoais;

(c) as suas consequências prováveis e as medidas tomadas ou propostas a tomar para resolver a violação, incluindo para mitigar os seus possíveis efeitos adversos.

Sempre que, e na medida em que, não seja possível fornecer todas estas informações simultaneamente, a notificação inicial deve conter as informações então disponíveis e, à medida que estas se tornem disponíveis, as informações adicionais devem ser fornecidas sem demora injustificada. As Partes definirão no Anexo III todos os outros elementos a fornecer pelo subcontratante aquando da assistência ao responsável pelo tratamento no cumprimento das suas obrigações nos termos dos artigos 33.º e 34.º do Regulamento (UE) 2016/679.

SECÇÃO III – DISPOSIÇÕES FINAIS

Cláusula 10.ª

Não conformidade com as Cláusulas e cessação

(a) Sem prejuízo de quaisquer disposições do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725, caso o subcontratante viole as suas obrigações ao abrigo das presentes Cláusulas, o responsável pelo tratamento pode instruir o subcontratante a suspender o tratamento de dados pessoais até que este cumpra as presentes Cláusulas ou o Acordo Principal seja cessado. O subcontratante deve informar imediatamente o responsável pelo tratamento caso não seja capaz de cumprir as presentes Cláusulas por qualquer motivo.

(b) O responsável pelo tratamento tem o direito de cessar o Acordo Principal, na medida em que diga respeito ao tratamento de dados pessoais, em conformidade com as presentes Cláusulas, se:

(1) o tratamento de dados pessoais pelo subcontratante foi suspenso pelo responsável pelo tratamento nos termos da alínea a) e se a conformidade com as presentes Cláusulas não for restabelecida num prazo razoável e, em qualquer caso, no prazo de um mês após a suspensão;

(2) o subcontratante estiver em violação substancial ou persistente das presentes Cláusulas ou das suas obrigações ao abrigo do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725;

(3) o subcontratante não cumprir uma decisão vinculativa de um tribunal competente ou das autoridades de controlo competentes relativamente às suas obrigações nos termos das presentes Cláusulas ou do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725.

(c) O subcontratante tem o direito de cessar o Acordo Principal, na medida em que diga respeito ao tratamento de dados pessoais ao abrigo das presentes Cláusulas, se, após ter informado o responsável pelo tratamento de que as suas instruções infringem os requisitos legais aplicáveis, em conformidade com a Cláusula 7.1 (b), o responsável pelo tratamento insistir no cumprimento das instruções.

(d) Após a cessação do Acordo Principal, o subcontratante deverá, a critério do responsável pelo tratamento, eliminar todos os dados pessoais tratados em nome do responsável pelo tratamento e certificar a este que o fez, ou, em alternativa, devolver todos os dados pessoais ao responsável pelo tratamento e eliminar as cópias existentes, a menos que a legislação da União ou dos Estados-Membros exija o armazenamento dos dados pessoais. Se o responsável pelo tratamento não tiver solicitado o tratamento de todos os dados pessoais em nome do responsável pelo tratamento no prazo de trinta (30) dias a contar da data de cessação do Acordo Principal, o subcontratante terá o direito de, a seu exclusivo critério, eliminar os dados pessoais. Até que os dados sejam eliminados ou devolvidos, o subcontratante continuará a garantir a conformidade com as presentes Cláusulas.

ANEXO I: LISTA DAS PARTES

Responsável(eis) pelo tratamento:

1. O Cliente (conforme identificado no Acordo Principal ou no Formulário de Encomenda)

Subcontratante(s):

1. Glooko AB

ANEXO II: DESCRIÇÃO DO TRATAMENTO

Categorias de titulares dos dados cujos dados pessoais são tratados
- Utilizadores Autorizados
- Pacientes

Categorias de dados pessoais tratados
Para Utilizadores Autorizados
- Informações gerais (nome)
- Informações de contacto (endereço de e-mail, número de telefone)
- Informações de utilização (nome de utilizador, palavra-passe, direitos de acesso, registos de auditoria)

Para Pacientes
- Informações gerais (nome, data de nascimento, género)
- Informações de contacto (endereço postal, endereço de e-mail, número de telefone)
- Informações de utilização (nome de utilizador, palavra-passe)
- Informações de saúde (tipo de diabetes, ano do diagnóstico da diabetes, parto estimado, intervalo alvo, peso, altura, tratamentos)
- Informações sobre o dispositivo (número[s] de série da bomba de insulina, do medidor de glicose e da caneta de insulina, doses, hidratos de carbono, definições, alarmes)

Dados sensíveis tratados (se aplicável) e restrições ou salvaguardas aplicadas que tenham plenamente em conta a natureza dos dados e riscos envolvidos, como, por exemplo, uma limitação rigorosa da finalidade, restrições de acesso (incluindo o acesso apenas aos colaboradores que tenham seguido a formação especializada), retenção de um registo do acesso aos dados, restrições para transferências posteriores ou medidas de segurança adicionais.
- Dados relativos à saúde

Para informações sobre as salvaguardas implementadas, consultar o Anexo III

Natureza do tratamento

Recolha, análise, visualização e tratamento de dados pessoais em conformidade com o Acordo Principal.

Finalidade(s) para a(s) qual(is) os dados pessoais são tratados em nome do responsável pelo tratamento
Permitir que o responsável pelo tratamento e os seus Utilizadores Autorizados utilizem o Software e outros Produtos em conformidade com o Acordo Principal.

Duração do tratamento

Durante o fornecimento do Software e de outros Produtos em conformidade com o Acordo Principal, incluindo, sem limitação, o fornecimento de serviços e a assistência técnica.

Para o tratamento por parte de subcontratantes (ulteriores), especificar igualmente o objeto, a natureza e a duração do tratamento
Consultar o Anexo IV

Instruções na secção 7.8, alínea a) das Cláusulas relativas às transferências internacionais
O responsável pelo tratamento concorda que o subcontratante pode transferir dados pessoais para destinatários localizados num país terceiro, desde que essa transferência esteja sujeita a salvaguardas adequadas reconhecidas ao abrigo das leis de proteção de dados aplicáveis ou que, de outra forma, esteja em conformidade com as leis de proteção de dados aplicáveis. O subcontratante pode transferir dados pessoais para a sua afiliada e subcontratante ulterior, a Glooko, Inc., nos Estados Unidos, conforme necessário para assistência técnica e requisitos regulamentares.

ANEXO III: MEDIDAS TÉCNICAS E ORGANIZATIVAS, INCLUINDO MEDIDAS TÉCNICAS E ORGANIZATIVAS PARA GARANTIR A SEGURANÇA DOS DADOS

1. Finalidade. O presente Anexo descreve o programa de segurança da Glooko, as certificações de segurança e as medidas técnicas e organizativas para proteger (a) os dados pessoais tratados pelo subcontratante em nome do responsável pelo tratamento contra a utilização, acesso, divulgação ou roubo não autorizados e (b) o Software. À medida que as ameaças de segurança mudam e evoluem, a Glooko continua a atualizar o seu programa e estratégia de segurança para ajudar a proteger os dados pessoais e o Software. Como tal, a Glooko reserva-se o direito de atualizar periodicamente o presente Anexo, desde que, no entanto, qualquer atualização não reduza materialmente as proteções globais estabelecidas no presente Anexo.

2. Organização e Programa de Segurança. A Glooko mantém um programa de segurança de avaliação baseado no risco. A estrutura do programa de segurança da Glooko inclui salvaguardas administrativas, organizativas, técnicas e físicas razoavelmente concebidas para proteger o Software e a confidencialidade, integridade e disponibilidade de dados pessoais. O programa de segurança da Glooko destina-se a ser adequado à natureza do Software e à dimensão e complexidade das operações comerciais da Glooko. A Glooko tem uma equipa de segurança de informações separada e dedicada que gere o programa de segurança da Glooko. Esta equipa facilita e apoia auditorias e avaliações independentes realizadas por terceiros. A estrutura de segurança da Glooko inclui programas que abrangem: Políticas e Procedimentos, Gestão de Ativos, Gestão de Acesso, Criptografia, Segurança Física, Segurança das Operações, Segurança das Comunicações, Segurança da Continuidade do Negócio, Segurança das Pessoas, Segurança dos Produtos, Segurança da Infraestrutura de Rede e Nuvem, Conformidade com a Segurança, Segurança de Terceiros, Gestão de Vulnerabilidades e Monitorização de Segurança e Resposta a Incidentes. A segurança é gerida nos níveis mais elevados da empresa, através da reunião regular do Responsável pela Segurança da Glooko com a direção executiva para discutir questões e coordenar iniciativas de segurança em toda a empresa. As políticas e normas de segurança de informações são revistas e aprovadas pela direção pelo menos uma vez por ano e são disponibilizadas a todos os funcionários da Glooko para consulta.

3. Confidencialidade. A Glooko dispõe de controlos para manter a confidencialidade dos dados pessoais em conformidade com o Acordo Principal. Todos os funcionários e pessoal contratado da Glooko estão vinculados pelas políticas internas da Glooko relativas à manutenção da confidencialidade dos dados pessoais e estão contratualmente obrigados a cumprir estas obrigações.

4. Segurança das Pessoas

    a. Verificação de Antecedentes dos Funcionários. A Glooko realiza verificações de antecedentes de todos os novos funcionários no momento da contratação, em conformidade com as leis locais aplicáveis. Atualmente, a Glooko verifica o grau académico e o emprego anterior de um novo funcionário e realiza verificações de referência. Quando permitido pela lei aplicável, a Glooko pode também realizar verificações de registo criminal, crédito, imigração e segurança, dependendo da natureza e do âmbito da função de um novo funcionário.

    b. Formação de Funcionários. Pelo menos uma (1) vez por ano, todos os funcionários da Glooko devem concluir uma formação de segurança e privacidade que abrange as políticas de segurança, as práticas recomendadas de segurança e os princípios de privacidade da Glooko. Os funcionários a usufruir de licenças podem ter tempo adicional para concluir esta formação anual. A equipa de segurança dedicada da Glooko também realiza campanhas de sensibilização sobre phishing e comunica ameaças emergentes aos funcionários.

5. Gestão de Fornecedores Terceiros

    a. Avaliação de Fornecedores. A Glooko pode recorrer a fornecedores terceiros para fornecer o Software. A Glooko realiza uma avaliação baseada no risco de segurança dos potenciais fornecedores antes de trabalhar com os mesmos para validar que cumprem os requisitos de segurança da Glooko. A Glooko revê periodicamente cada fornecedor à luz dos padrões de segurança e continuidade do negócio da Glooko, incluindo o tipo de acesso e classificação dos dados a serem acedidos (se existentes), os controlos necessários para proteger os dados e os requisitos legais/regulamentares. A Glooko garante que os dados pessoais são devolvidos e/ou eliminados no final de uma relação com um fornecedor.

    b. Acordos com Fornecedores. A Glooko celebra acordos escritos com todos os seus fornecedores que incluem obrigações de confidencialidade, privacidade e segurança que fornecem um nível adequado de proteção para dados pessoais que estes fornecedores possam tratar.

6. Arquitetura, Firewalls e Separação de Dados. Todo o acesso à rede entre anfitriões de produção é restrito, utilizando firewalls para permitir que apenas serviços autorizados interagem na rede de produção. São utilizadas firewalls para gerir a separação da rede entre diferentes zonas de segurança nos ambientes de produção e corporativos. A Glooko separa logicamente as suas bases de dados. As API da Glooko foram concebidas e desenvolvidas para identificar e permitir o acesso apenas a e dos respetivos remetentes. Estes controlos impedem que os clientes tenham acesso a dados de outros clientes.

7. Segurança Física. Os centros de dados que alojam o Software são estritamente controlados tanto no perímetro como nos pontos de entrada do edifício por funcionários de segurança profissionais que utilizam vigilância por vídeo, sistemas de deteção de intrusão e outros meios eletrónicos. Estão disponíveis fontes de alimentação ininterruptas e geradores no local para fornecer energia de reserva em caso de falha elétrica. Além disso, as sedes e os espaços de escritório da Glooko têm um programa de segurança física que gere visitantes, entradas de edifícios e a segurança geral do escritório.

8. Segurança desde a Conceção. A Glooko segue os princípios de segurança desde a conceção quando concebe o Software. A Glooko também aplica o padrão de Ciclo de Vida de Desenvolvimento do Software (SDLC) da Glooko para executar diversas atividades relacionadas com a segurança para o Software em diferentes fases do ciclo de vida da criação do produto, desde a recolha de requisitos e conceção do produto à implementação do produto.

9. Controlos de Acesso

    a. Fornecimento de Acesso. Para minimizar o risco de exposição dos dados, a Glooko segue os princípios de menor privilégio através de um modelo de controlo de acesso baseado em equipa ao fornecer o acesso ao sistema. O pessoal da Glooko está autorizado a aceder a dados pessoais com base na sua função, cargo e responsabilidades, e este acesso requer a aprovação do diretor do funcionário. O acesso de um funcionário a dados pessoais é removido após a cessação do seu emprego. Antes de um engenheiro ter acesso ao ambiente de produção, o acesso deve ser aprovado pela direção e o engenheiro deve concluir formações internas para este acesso, incluindo formações sobre os sistemas da equipa relevante. A Glooko regista ações de alto risco e alterações no ambiente de produção. A Glooko tira partido da automatização para identificar qualquer desvio às normas técnicas internas que possa indicar atividade anómala/não autorizada e alertar dentro de minutos para uma alteração de configuração.

b. Controlos de Palavras-passe. Quando um Utilizador Autorizado inicia sessão na sua conta, a Glooko gera hashes das credenciais do utilizador antes de serem armazenadas. Os clientes também podem exigir que os seus Utilizadores Autorizados adicionem outra camada de segurança à sua conta, utilizando a autenticação de dois fatores (2FA).

10. Gestão de Alterações. A Glooko tem um processo formal de gestão de alterações que segue para administrar alterações no ambiente de produção do Software, incluindo quaisquer alterações no seu software, aplicações e sistemas subjacentes. Cada alteração é cuidadosamente analisada e avaliada num ambiente de teste antes de ser implementada no ambiente de produção do Software. Todas as alterações, incluindo a avaliação das alterações num ambiente de teste, são documentadas utilizando um sistema de registo formal e auditável. É necessária a aprovação de implementação para alterações de alto risco por parte das partes interessadas organizacionais corretas. Também são implementados planos e procedimentos caso uma alteração implementada necessite de ser revertida para preservar a segurança do Software.

11. Encriptação. Para o Software, (a) as bases de dados que armazenam dados pessoais são encriptadas utilizando o Advanced Encryption Standard e (b) os dados pessoais são encriptados quando estão em trânsito entre a aplicação de software do Cliente e o Software utilizando o TLS v1.2.

12. Gestão de Vulnerabilidades. A Glooko mantém controlos e políticas para atenuar o risco de vulnerabilidades de segurança para equilibrar o risco e os requisitos comerciais/ operacionais. A Glooko utiliza uma ferramenta de terceiros para realizar análises de vulnerabilidades regularmente, de forma a avaliar vulnerabilidades na infraestrutura na nuvem e nos sistemas corporativos da Glooko.

13. Testes de Penetração. A Glooko realiza testes de penetração e envolve entidades independentes terceiras para realizar testes de penetração ao nível da aplicação. As ameaças e vulnerabilidades de segurança detetadas são priorizadas, triadas e solucionadas.

14. Gestão de Incidentes de Segurança. A Glooko mantém políticas de gestão de incidentes de segurança. A Equipa de Resposta a Incidentes de Segurança (T-SIRT) da Glooko avalia todas as ameaças e vulnerabilidades de segurança relevantes e estabelece medidas adequadas de correção e atenuação. A Glooko retém os seus registos de segurança pertinentes.

15. Resiliência e Continuidade do Software. O Software utiliza uma variedade de ferramentas e mecanismos para alcançar uma elevada disponibilidade e resiliência. Para o Software, a infraestrutura da Glooko abrange várias zonas de disponibilidade independentes de falhas em regiões geográficas fisicamente separadas umas das outras. A Glooko também tira partido de ferramentas especializadas que monitorizam o desempenho do servidor, os dados e a capacidade de carga de tráfego dentro de cada zona de disponibilidade e centro de dados de colocalização. Se for detetado um desempenho de servidor sub-ideal ou uma sobrecarga de capacidade num servidor dentro de uma zona de disponibilidade ou centro de dados de colocalização, estas ferramentas especializadas aumentam a capacidade ou alteram o tráfego para aliviar qualquer sobrecarga de capacidade ou desempenho de servidor sub-ideal. A Glooko também é imediatamente notificada em caso de desempenho sub-ideal do servidor ou de uma sobrecarga de capacidade.

16. Cópias de Segurança e Recuperação. A Glooko realiza cópias de segurança regulares de dados pessoais. Os dados pessoais com cópia de segurança são retidos de forma redundante em várias zonas de disponibilidade e encriptados quando estão em trânsito e em repouso utilizando os Advanced Encryption Standards.

ANEXO IV: LISTA DE SUBCONTRATANTES ULTERIORES

O responsável pelo tratamento autorizou a utilização dos seguintes subcontratantes ulteriores:

1. Nome: Amazon Web Services EMEA SARL
Morada: 38 Avenue John F. Kennedy, L-1855, Luxemburgo

Descrição do tratamento (incluindo uma delimitação clara das responsabilidades no caso de vários subcontratantes ulteriores serem autorizados): fornecedor de serviços na nuvem

2. Nome: Cegedim SA
Morada: 137 rue d'Aguesseau, 92100 Boulogne-Billancourt, França

Descrição do tratamento (incluindo uma delimitação clara das responsabilidades no caso de vários subcontratantes ulteriores serem autorizados): fornecedor de serviços na nuvem (pode ser utilizado para clientes localizados em França)

3. Nome: Pictime Groupe
Morada: Campus du Digital 61, rue de l'Harmonie - 59262 Sainghin-en-Mélantois, França

Descrição do tratamento (incluindo uma delimitação clara das responsabilidades no caso de vários subcontratantes ulteriores serem autorizados): Anfitrião de Dados de Saúde Certificado (pode ser utilizado para clientes localizados em França e na Alemanha)

4. Nome: Glooko, Inc.
Morada: 411 High Street, Palo Alto, California, 94301

Descrição do tratamento (incluindo uma delimitação clara das responsabilidades no caso de vários subcontratantes ulteriores serem autorizados): assistência técnica e requisitos regulamentares.