اتفاقية معالجة البيانات

القسم الأول

البند 1

الغرض والنطاق

1. الغرض من هذه البنود التعاقدية القياسية (البنود) هو ضمان الامتثال للمادة 28 البندين (3) و(4) من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) الصادرة عن البرلمان الأوروبي والمجلس، بتاريخ 27 أبريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات.
2. وقد وافق المراقبون والمعالجون المدرجون في الملحق الأول على هذه البنود من أجل ضمان الامتثال للمادة 28 البندين (3) و(4) من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو المادة 29 البندين (3) و(4) من اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي).
3. تنطبق هذه البنود إذا تم استيفاء المتطلبات المنصوص عليها في الاتفاقية الرئيسية، وعلى معالجة البيانات الشخصية على النحو المحدد في الملحق الثاني.
4. وتشكل الملحقات من الأول إلى الرابع جزءًا لا يتجزأ من البنود.
5. لا تخل هذه البنود بالالتزامات التي يخضع لها المراقب بموجب اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي).
6. لا تضمن هذه البنود في حد ذاتها الامتثال للالتزامات المتعلقة بعمليات النقل الدولية وفقًا للفصل الخامس من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي).

البند 2

ثبات البنود

1. تتعهد الأطراف بعدم تعديل البنود، باستثناء إضافة معلومات إلى الملحقات أو تحديث المعلومات فيها.
2. وهذا لا يمنع الأطراف من إدراج البنود التعاقدية القياسية المنصوص عليها في هذه البنود في عقد أوسع نطاقًا أو إضافة بنود أخرى أو ضمانات إضافية شريطة ألا تتعارض بشكلٍ مباشر أو غير مباشر مع البنود أو تنتقص من الحقوق أو الحريات الأساسية لأصحاب البيانات.

البند 3

التفسير

1. في حال استخدام هذه البنود المصطلحات المحددة في اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي) على التوالي، يجب أن يكون لتلك المصطلحات نفس المعنى كما في تلك اللائحة.
2. تجب قراءة هذه البنود وتفسيرها في ضوء أحكام اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي) على التوالي.
3. لا يجوز تفسير هذه البنود بطريقة تتعارض مع الحقوق والالتزامات المنصوص عليها في اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي) أو بطريقة تخل بالحقوق أو الحريات الأساسية لأصحاب البيانات.

البند 4

التسلسل الهرمي

في حال وجود تناقض بين هذه البنود وأحكام الاتفاقات ذات الصلة المُبرمة بين الأطراف والتي كانت سارية في وقت الاتفاق على هذه البنود أو إبرامها لاحقًا، تسود هذه البنود.

المادة 5 - اختياري

بند الاندماج

1. يجوز لأي كيان ليس طرفًا في هذه البنود، بموافقة جميع الأطراف، أن ينضم إلى هذه البنود في أي وقت كمراقب أو معالج عن طريق استكمال الملحقات والتوقيع على الملحق الأول.
2. بمجرد الانتهاء من الملحقات الواردة في (أ) والتوقيع عليها، يُعامل الكيان المنضم كطرف في هذه البنود ويكون له حقوق والتزامات المراقب أو المعالج، وفقًا لتعيينه في الملحق الأول.
3. لا يكون للكيان المنضم أي حقوق أو التزامات ناتجة عن هذه البنود من الفترة السابقة ليصبح طرفًا.

القسم الثاني: التزامات الأطراف

البند 6

وصف عملية (عمليات) المعالجة

ترد تفاصيل عمليات المعالجة، ولا سيما فئات البيانات الشخصية وأغراض المعالجة التي تتم معالجة البيانات الشخصية من أجلها نيابةً عن المراقب، في الملحق الثاني.

البند 7
التزامات الأطراف

7.1. التعليمات

1. تجب على المعالج معالجة البيانات الشخصية فقط بناءً على تعليمات موثقة من المراقب، ما لم يكن ذلك مطلوبًا بموجب قانون الاتحاد أو الدول الأعضاء الذي يخضع له المعالج. وفي هذه الحالة، يجب على المعالج إبلاغ المراقب عن هذا المطلب القانوني قبل المعالجة، ما لم يحظر القانون ذلك لأسباب مهمة تتعلق بالمصلحة العامة. يمكن أيضًا إعطاء تعليمات لاحقة من قبل المراقب طوال مدة معالجة البيانات الشخصية. ويجب دائمًا توثيق هذه التعليمات.
2. يجب على المعالج إبلاغ المراقب على الفور إذا رأى المعالج أن التعليمات المقدمة من قبل وحدة التحكم تنتهك اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي) أو أحكام حماية البيانات المعمول بها في الاتحاد أو الدول الأعضاء.

7.2. تحديد الغرض

تجب على المعالج معالجة البيانات الشخصية فقط لغرض (أغراض) محددة من المعالجة، على النحو المبين في الملحق الثاني، ما لم يتلق المزيد من التعليمات من المراقب.

7.3. مدة معالجة البيانات الشخصية

لا تجوز للمعالج معالجة البيانات الشخصية إلا خلال المدة المحددة في الملحق الثاني.

7.4. أمان المعالجة

1. يجب على المعالج على الأقل تنفيذ التدابير الفنية والتنظيمية المحددة في الملحق الثالث لضمان أمان البيانات الشخصية. ويشمل ذلك حماية البيانات من الاختراق الأمني الذي يؤدي إلى تدمير أو فقدان أو تغيير أو كشف غير مصرح به أو وصول غير مصرح به إلى البيانات (انتهاك البيانات الشخصية) بشكل عرضي أو غير قانوني. وعند تقييم المستوى المناسب من الأمان، تُراعي الأطراف على النحو الواجب أحدث ما توصلت إليه البيانات وتكاليف التنفيذ وطبيعة المعالجة ونطاقها وسياقها وأغراضها والمخاطر التي يتعرض لها أصحاب البيانات.
2. يجب على المعالج منح الوصول إلى البيانات الشخصية التي تخضع للمعالجة لأعضاء موظفيه فقط بالقدر الضروري للغاية لتنفيذ العقد وإدارته ومراقبته. أيضًا يجب على المعالج التأكد من أن الأشخاص المخول لهم معالجة البيانات الشخصية المستلمة قد تعهدوا بالسرية أو أنهم يخضعون لالتزام قانوني مناسب بالسرية.

7.5. البيانات الحساسة

إذا كانت المعالجة تتضمن بيانات شخصية تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية في النقابات أو البيانات الوراثية أو البيانات البيومترية لغرض تحديد هوية الشخص الطبيعي بشكل فريد أو البيانات المتعلقة بالصحة أو الحياة الجنسية للشخص أو ميوله الجنسية أو البيانات المتعلقة بالإدانات الجنائية والجرائم (يُشار إليها باسم "البيانات الحساسة")، فيجب على المعالج تطبيق قيود محددة و/أو ضمانات إضافية.

7.6 التوثيق والامتثال

1. يجب أن يكون الأطراف قادرين على إثبات الامتثال لهذه البنود.
2. يجب على المعالج التعامل بسرعة وبشكلٍ كافٍ مع الاستفسارات من المراقب حول معالجة البيانات وفقًا لهذه البنود.
3. يجب على المعالج أن يقدم للمراقب كل المعلومات اللازمة لإثبات الامتثال للالتزامات المنصوص عليها في هذه البنود والمُستمدة بشكلٍ مباشرٍ من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي). وبناءً على طلب المراقب، يجب على المعالج أيضًا السماح والمساهمة في عمليات تدقيق أنشطة المعالجة التي تغطيها هذه البنود، وذلك على فترات زمنية معقولة أو في حال وجود مؤشرات على عدم الامتثال. عند اتخاذ قرار بشأن المراجعة أو التدقيق، قد يأخذ المراقب في الاعتبار الشهادات ذات الصلة التي يمتلكها المعالج.
4. يجوز للمراقب أن يختار إجراء عملية التدقيق بنفسه أو تكليف مُدقق حسابات مستقل. ويمكن أن تشمل عمليات التدقيق أيضًا عمليات تفتيش في أماكن العمل أو المنشآت المادية للمعالج، ويجب، عند الاقتضاء، أن تتم في غضون مهلة معقولة.
5. يجب على الأطراف تقديم المعلومات المُشار إليها في هذا البند، بما في ذلك نتائج أي عمليات تدقيق، إلى السلطة/السلطات الإشرافية المختصة بناءً على طلبها.

7.7. الاستعانة بمعالجين فرعيين

1. يملك المعالج إذنًا عامًا من المراقب لإشراك معالجين فرعيين من قائمة متفق عليها. ويجب على المعالج إبلاغ المراقب خطيًا بأي تغييرات مقترحة لتلك القائمة من خلال إضافة أو استبدال المعالجين الفرعيين قبل ثلاثين (30) يومًا على الأقل، وبالتالي منح المراقب وقتًا كافيًا للاعتراض على مثل هذه التغييرات قبل إشراك المعالج الفرعي المعني (المعالجين الفرعيين المعنيين). يجب على المعالج تزويد المراقب بالمعلومات اللازمة لتمكينه من ممارسة الحق في الاعتراض.
2. عندما يستعين المعالج بمعالج فرعي لتنفيذ أنشطة معالجة محددة (نيابة عن المراقب)، يجب عليه القيام بذلك عن طريق عقد يفرض على المعالج الفرعي، في جوهره، نفس التزامات حماية البيانات مثل تلك المفروضة على معالج البيانات وفقًا لهذه البنود. ويجب على المعالج التأكد من أن المعالج الفرعي يمتثل للالتزامات التي يخضع لها المعالج وفقًا لهذه البنود واللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي).
3. بناءً على طلب المراقب، يجب على المعالج تقديم نسخة من اتفاقية المعالج الفرعي وأي تعديلات لاحقة عليها للمراقب. يحق للمعالج، بالقدر الضروري لحماية سرية العمل أو أية معلومات سرية أخرى، بما في ذلك البيانات الشخصية، أن يحجب نص الاتفاقية قبل مشاركة النسخة.

4. يظل المعالج مسؤولاً بشكلٍ كاملٍ تجاه المراقب عن أداء التزامات المعالج الفرعي وفقًا للعقد المبرم مع المعالج. ويجب على المعالج إخطار المراقب بأي تقصير من قبل المعالج الفرعي في الوفاء بالتزاماته التعاقدية.
5. يجب على المعالج، حيثما أمكن ذلك، أن يوافق على بند الطرف الثالث المستفيد مع المعالج الفرعي وبموجبه - إذا اختفى المعالج فعليًا أو لم يعد موجودًا في القانون أو أصبح معسرًا - يحق للمراقب إنهاء عقد المعالج الفرعي وتوجيه المعالج الفرعي لمحو البيانات الشخصية أو إرجاعها.

7.8. عمليات النقل الدولية

1. لا يجوز نقل أي بيانات إلى دولة ثالثة أو منظمة دولية من قبل المعالج إلا بناءً على تعليمات موثقة من المراقب أو من أجل الوفاء بمتطلبات محددة بموجب قانون الاتحاد أو الدول الأعضاء الذي يخضع له المعالج ويجب أن يتم ذلك وفقًا للفصل الخامس من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي).
2. يوافق المراقب على أنه في حال قيام المعالج بإشراك معالج فرعي وفقًا للبند 7.7. لتنفيذ أنشطة معالجة محددة (نيابةً عن المراقب) وكانت أنشطة المعالجة هذه تنطوي على نقل البيانات الشخصية بالمعنى المقصود في الفصل الخامس من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي)، فيمكن للمعالج والمعالج الفرعي ضمان الامتثال للفصل الخامس من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) باستخدام البنود التعاقدية القياسية التي اعتمدتها المفوضية وفقًا للمادة 46 البند (2) من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي)، شريطة استيفاء بنود استخدام تلك البنود التعاقدية القياسية.

البند 8

مساعدة المراقب

1. تجب على المعالج إحالة أصحاب البيانات للاتصال بالمراقب، في حال تلقي المعالج طلبًا من أحد أصحاب البيانات. ولا يجوز له الاستجابة للطلب نفسه، ما لم يأذن له المراقب بذلك.
2. تجب على المعالج مساعدة المراقب في الوفاء بالتزاماته للرد على طلبات أصحاب البيانات لممارسة حقوقهم، مع مراعاة طبيعة المعالجة. وعند الوفاء بالتزاماته وفقًا للفقرتين (أ) و(ب)، يجب على المعالج الامتثال لتعليمات المراقب
3. بالإضافة إلى التزام المعالج بمساعدة المراقب وفقًا للبند 8 (ب)، تجب على المعالج أيضًا مساعدة المراقب في ضمان الامتثال للالتزامات الآتية، مع مراعاة طبيعة معالجة البيانات والمعلومات المتاحة للمعالج:
   أ. الالتزام بإجراء تقييم لتأثير عمليات المعالجة المتوخاة على حماية البيانات الشخصية (يُشار إليه باسم "تقييم تأثير حماية البيانات") عندما يكون من المحتمل أن يؤدي نوع من المعالجة إلى خطر كبير على حقوق الأشخاص الطبيعيين وحرياتهم؛
   ب. الالتزام باستشارة السلطة/السلطات الرقابية المختصة قبل المعالجة عندما يشير تقييم تأثير حماية البيانات إلى أن المعالجة ستؤدي إلى مخاطر عالية في غياب التدابير التي يتخذها المراقب للتخفيف من المخاطر؛
   ج. الالتزام بضمان دقة البيانات الشخصية وتحديثها، من خلال إبلاغ المراقب من دون تأخير إذا أصبح المعالج على علم بأن البيانات الشخصية التي يقوم بمعالجتها غير دقيقة أو أصبحت قديمة؛
   د. الالتزامات الواردة في المادة 32 للائحة رقم 679/عام 2016 (الاتحاد الأوروبي).

وتحدد الأطراف في الملحق الثالث التدابير التقنية والتنظيمية المناسبة التي يطلب من المعالج بواسطتها مساعدة المراقب في تطبيق هذا البند، وكذلك نطاق المساعدة المطلوبة ومداها.

البند 9

الإخطار بانتهاك البيانات الشخصية

في حال حدوث انتهاك للبيانات الشخصية، يجب على المعالج التعاون مع المراقب ومساعدته في الامتثال لالتزاماته بموجب المادتين 33 و34 من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) أو بموجب المادتين 34 و35 من اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي)، حيثما ينطبق ذلك، مع مراعاة طبيعة المعالجة والمعلومات المتاحة للمعالج.

9.1. انتهاك البيانات المتعلق بالبيانات التي تتم معالجتها من قِبَل المراقب

في حال حدوث انتهاك للبيانات الشخصية يتعلق بالبيانات التي تتم معالجتها من قِبَل المراقب، تجب على المعالج مساعدة المراقب في ما يأتي:

1. إخطار السلطة/السلطات الرقابية المختصة بانتهاك البيانات الشخصية من دون تأخير لا مبرر له بعد أن أصبح المراقب على علم بذلك، حيثما كان ذلك مناسبًا (ما لم يكن من غير المحتمل أن يؤدي انتهاك البيانات الشخصية إلى مخاطر على حقوق الأشخاص الطبيعيين وحرياتهم)؛
2. الحصول على المعلومات الآتية التي يجب ذكرها في إخطار المراقب، وفقًا للمادة 33 البند (3) من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي)، ويجب أن تتضمن على الأقل:
   أ. طبيعة البيانات الشخصية بما في ذلك فئات البيانات المعنية وعددها التقريبي وفئات سجلات البيانات الشخصية المعنية وعددها التقريبي، حيثما أمكن ذلك؛
   ب. العواقب المحتملة لانتهاك البيانات الشخصية؛
   ج. التدابير المتخذة أو المقترح اتخاذها من قبل المراقب لمعالجة انتهاك البيانات الشخصية، بما في ذلك، عند الاقتضاء، تدابير التخفيف من آثارها السلبية المحتملة.
   د. وإذا تعذر تقديم كل هذه المعلومات في الوقت نفسه وبقدر ما يتعذر ذلك، فيجب أن يتضمن الإخطار الأوّلي المعلومات المتاحة حينئذ، وتقدم المعلومات الإضافية لاحقًا، متى توفرت، من دون تأخير لا مبرر له.
3. الامتثال، وفقًا للمادة 34 من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي)، للالتزام بالإبلاغ من دون تأخير لا مبرر له عن انتهاك البيانات الشخصية لموضوع البيانات، عندما يكون من المحتمل أن يؤدي انتهاك البيانات الشخصية إلى مخاطر كبيرة على حقوق الأشخاص الطبيعيين وحرياتهم.

9.2. انتهاك البيانات المتعلق بالبيانات التي تتم معالجتها من قِبَل المعالج

في حال حدوث انتهاك للبيانات الشخصية يتعلق بالبيانات التي تتم معالجتها من قِبَل المعالج، يجب على المعالج إخطار المراقب من دون تأخير لا مبرر له بعد أن يصبح المعالج على علم بهذا الانتهاك. ويجب أن يتضمن هذا الإخطار، على الأقل، ما يأتي:

1. وصف لطبيعة الانتهاك (بما في ذلك، حيثما أمكن، فئات البيانات المعنية وعددها التقريبي)؛
2. تفاصيل نقطة الاتصال حيث يمكن الحصول على مزيد من المعلومات المتعلقة بانتهاك البيانات الشخصية؛
3. عواقبه المحتملة والتدابير المتخذة أو المقترح اتخاذها لمعالجة الانتهاك، بما في ذلك التخفيف من آثاره السلبية المحتملة.

وإذا تعذر تقديم كل هذه المعلومات في الوقت نفسه وبقدر ما يتعذر ذلك، فيجب أن يتضمن الإخطار الأوّلي المعلومات المتاحة حينئذ، وتقدم المعلومات الإضافية لاحقًا، متى توفرت، من دون تأخير لا مبرر له.

تحدد الأطراف في الملحق الثالث كل العناصر الأخرى التي يجب أن يقدمها المعالج عند مساعدة المراقب في الامتثال لالتزامات المراقب بموجب المادتين 33 و34 من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي).

القسم الثالث: الأحكام النهائية

البند 10

عدم الامتثال للبنود والإنهاء

1. من دون الإخلال بأي أحكام من اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي)، في حال انتهاك المعالج لالتزاماته بموجب هذه البنود، فيجوز للمراقب توجيه المعالج إلى تعليق معالجة البيانات الشخصية حتى يتوافق الأخير مع هذه البنود أو يتم إنهاء الاتفاقية الرئيسية. ويجب على المعالج إبلاغ المراقب على الفور في حال عدم قدرته على الامتثال لهذه البنود، لأي سببٍ من الأسباب.
2. يحق للمراقب إنهاء الاتفاقية الرئيسية بقدر ما يتعلق الأمر بمعالجة البيانات الشخصية وفقًا لهذه البنود إذا:

أ) علّق المراقب معالجة البيانات الشخصية من قِبَل المعالج وفقًا للنقطة (أ) وإذا لم تتم استعادة الامتثال لهذه البنود في غضون فترة زمنية معقولة وعلى أي حال في غضون شهر واحد بعد التعليق؛

ب) انتهك المعالج البنود أو التزاماته بشكلٍ كبير أو مستمر بموجب اللائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو اللائحة رقم 1725/عام 2018 (الاتحاد الأوروبي)؛

ج) تعذر على المعالج الالتزام بقرار ملزم صادر عن محكمة مختصة أو السلطة/السلطات الرقابية المختصة فيما يتعلق بالتزاماته وفقًا لهذه البنود أو للائحة رقم 679/عام 2016 (الاتحاد الأوروبي) و/أو للائحة رقم 1725/عام 2018 (الاتحاد الأوروبي).

3. يحق للمعالج إنهاء الاتفاقية الرئيسية بقدر ما يتعلق الأمر بمعالجة البيانات الشخصية بموجب هذه البنود، حيث يصر المراقب على الامتثال للتعليمات بعد إبلاغ المراقب بأن تعليماته تنتهك المتطلبات القانونية المعمول بها وفقًا للبند 7.1 (ب).
4. بعد إنهاء الاتفاقية الرئيسية، يجب على المعالج، بناءً على اختيار المراقب، حذف كل البيانات الشخصية التي تمت معالجتها نيابةً عن المراقب وإصدار شهادة للمراقب تؤكد على أنه فعل ذلك، أو إرجاع كل البيانات الشخصية إلى المراقب وحذف النُسخ الموجودة ما لم يتطلب قانون الاتحاد أو الدول الأعضاء تخزين البيانات الشخصية. وإذا لم يطلب المراقب معالجة كل البيانات الشخصية نيابةً عن المراقب في غضون ثلاثين (30) يومًا من إنهاء الاتفاقية الرئيسية، فيحق للمعالج، وفقًا لتقديره الخاص، حذف البيانات الشخصية. وحتى يتم حذف البيانات أو إعادتها، يستمر المعالج في ضمان الامتثال لهذه البنود.

الملحق الأول: قائمة الأطراف

المراقب (المراقبون): العميل (كما هو محدد في الاتفاقية الرئيسية أو نموذج الطلب)

المعالج (المعالجون): Glooko AB (كما هو محدد في الاتفاقية الرئيسية)

الملحق الثاني: وصف المعالجة

فئات الأشخاص الذين تتم معالجة بياناتهم الشخصية

- المستخدمون المصرح لهم
- المرضى

فئات البيانات الشخصية التي تتم معالجتها

<u>للمستخدمين المصرح لهم</u>

- معلومات عامة (الاسم)
- معلومات التواصل (عنوان البريد الإلكتروني ورقم الهاتف)
- معلومات الاستخدام (اسم المستخدم وكلمة المرور وحقوق الوصول وسجلات التدقيق)

<u>للمرضى</u>

- معلومات عامة (الاسم وتاريخ الميلاد والجنس)
- معلومات التواصل (العنوان البريدي وعنوان البريد الإلكتروني ورقم الهاتف)
- معلومات الاستخدام (اسم المستخدم وكلمة المرور)

- المعلومات الصحية (نوع مرض السكري وسنة تشخيص مرض السكري وتاريخ الولادة المقدر والنطاق المستهدف والوزن والطول والعلاجات)
- معلومات الجهاز (مضخة الإنسولين وجهاز قياس الجلوكوز والرقم (الأرقام) التسلسلي لقلم الإنسولين والجرعات والكربوهيدرات والإعدادات والتنبيهات)

معالجة البيانات الحساسة (إن وجدت) وفرض قيود أو ضمانات تأخذ في الاعتبار تمامًا طبيعة البيانات والمخاطر التي تنطوي عليها، مثل القيود الصارمة على الغرض والقيود المفروضة على الوصول (بما في ذلك الوصول فقط للموظفين الذين تلقوا تدريبًا متخصصًا) والاحتفاظ بسجل للوصول إلى البيانات والقيود المفروضة على التحويلات اللاحقة أو التدابير الأمنية الإضافية.

- البيانات المتعلقة بالصحة
للاطلاع على المعلومات المتعلقة بالضمانات المنفذة، راجع الملحق الثالث

طبيعة المعالجة
جمع البيانات الشخصية وتحليلها وتصورها ومعالجتها بطريقة أخرى وفقًا للاتفاقية الرئيسية.
الغرض (الأغراض) التي تتم معالجة البيانات الشخصية من أجلها نيابةً عن المراقب
لتمكين المراقب والمستخدمين المصرح لهم من استخدام البرنامج والتسليمات الأخرى وفقًا للاتفاقية الرئيسية.

مدة المعالجة
طوال مدة توفير البرنامج وغيره من التسليمات وفقًا للاتفاقية الرسمية، بما في ذلك على سبيل المثال لا الحصر توفير الخدمة والدعم الفني.

للمعالجة بواسطة المعالجين (المعالجين الفرعيين)، حدد أيضًا موضوع المعالجة وطبيعتها ومدتها
راجع الملحق الرابع

التعليمات الواردة في القسم 7.8 أ) بالنسبة إلى البنود المتعلقة بعمليات النقل الدولية
يوافق المراقب على أنه يجوز للمعالج نقل البيانات الشخصية إلى مستلمين موجودين في بلدان ثالثة شريطة أن يخضع هذا النقل للضمانات المناسبة المعترف بها بموجب قوانين حماية البيانات المعمول بها أو يتوافق مع قوانين حماية البيانات المعمول بها. يجوز للمعالج نقل البيانات الشخصية إلى الشركة التابعة لها والمعالج الفرعي، Glooko, Inc. في الولايات المتحدة حسب الضرورة للدعم الفني والمتطلبات التنظيمية.

الملحق الثالث: التدابير التقنية والتنظيمية التي تشمل التدابير التقنية والتنظيمية لضمان أمان البيانات

1. الغرض. يصف هذا الملحق برنامج الأمان الخاص بشركة Glooko والشهادات الأمنية والتدابير التقنية والتنظيمية لحماية (أ) البيانات الشخصية التي يعالجها المعالج نيابةً عن المراقب من الاستخدام غير المصرح به أو الوصول أو الكشف أو السرقة و(ب) البرامج. مع تحول التهديدات الأمنية وتطورها، تواصل Glooko تحديث برنامجها واستراتيجيتها الأمنية للمساعدة في حماية البيانات الشخصية والبرامج. وعلى هذا النحو، تحتفظ Glooko بالحق في تحديث هذا الملحق من وقت لآخر؛ ولكن شريطة أن أي تحديث لن يقلل ماديًا من الحماية الشاملة المنصوص عليها في هذا الملحق.
2. تنظيم وبرنامج الأمان. تحتفظ Glooko ببرنامج أمان لتقييم المخاطر. يتضمن إطار عمل برنامج الأمان الخاص بشركة Glooko ضمانات إدارية وتنظيمية وتقنية ومادية مصممة بشكلٍ معقول لحماية البرامج وسرية البيانات الشخصية وسلامتها وتوفرها. يهدف برنامج الأمان الخاص بشركة Glooko إلى أن يكون مناسبًا لطبيعة البرنامج وحجم العمليات التجارية لشركة Glooko وتعقيدها. كما تمتلك شركة Glooko فريق أمان معلومات منفصلاً ومخصصًا يدير برنامج أمان Glooko. ويقوم هذا الفريق بتسهيل ودعم عمليات التدقيق والتقييم المستقلة التي تقوم بها جهات خارجية. يتضمن إطار العمل الأمني الخاص بشركة Glooko برامج تغطي ما يأتي: السياسات والإجراءات وإدارة الأصول وإدارة الوصول والتشفير والأمان المادي وأمان العمليات وأمان الاتصالات وأمان استمرارية الأعمال وأمان الأشخاص وأمان المنتجات وأمان البنية الأساسية للسحابة والشبكة والامتثال الأمني وأمان الجهات الخارجية وإدارة الثغرات الأمنية ومراقبة الأمان والاستجابة للحوادث. تتم إدارة الأمان على أعلى المستويات في الشركة، حيث يجتمع مسؤول الأمان لشركة Glooko مع الإدارة التنفيذية بانتظام لمناقشة القضايا وتنسيق المبادرات الأمنية على مستوى الشركة. كما تتم مراجعة سياسات ومعايير أمان المعلومات والموافقة عليها من قبل الإدارة سنويًا على الأقل ويتم توفيرها لجميع موظفي Glooko للرجوع إليها.
3. السرية. لدى Glooko ضوابط مطبقة للحفاظ على سرية البيانات الشخصية وفقًا للاتفاقية الرئيسية. يلتزم جميع موظفي Glooko وموظفي العقود بالسياسات الداخلية لشركة Glooko فيما يتعلق بالحفاظ على سرية البيانات الشخصية وهم ملزمون تعاقديًا بالامتثال لهذه الالتزامات.
4. أمان الأشخاص

أ) التحقق من هوية الموظف. تقوم Glooko بإجراء عمليات تحقق من هوية جميع الموظفين الجدد في وقت التوظيف وفقًا للقوانين المحلية المعمول بها. تقوم Glooko حاليًا بالتحقق من تعليم الموظف الجديد ووظائفه السابقة وإجراء فحوصات مرجعية. وحين يسمح القانون المعمول به، يجوز لشركة Glooko أيضًا إجراء تحقيقات جنائية وائتمانية ومرتبطة بالهجرة وأمنية بناءً على طبيعة ونطاق دور الموظف الجديد.

ب) تدريب الموظفين. على الأقل مرة واحدة (1) في السنة، يجب على جميع موظفي Glooko إكمال تدريب على الأمان والخصوصية يغطي سياسات الأمان وأفضل الممارسات الأمنية ومبادئ الخصوصية من Glooko. ويمكن أن يتاح للموظفين الذين هم في إجازة وقت إضافي لإكمال هذا التدريب السنوي. كما يقوم فريق الأمان المخصص في شركة Glooko بحملات توعية للتصيد الاحتيالي وإرسال التهديدات الناشئة إلى الموظفين.

5. إدارة البائعين من الجهات الخارجية

أ) تقييم البائعين. قد تستخدم شركة Glooko بائعين من جهات خارجية لتوفير البرنامج. وتقوم Glooko بإجراء تقييم قائم على المخاطر الأمنية للبائعين المحتملين قبل العمل معهم للتحقق من أنهم يستوفون المتطلبات الأمنية لشركة Glooko. كما تقوم Glooko بمراجعة كل بائع بشكل دوري في ضوء معايير الأمان واستمرارية الأعمال الخاصة بشركة Glooko، بما في ذلك نوع الوصول إلى البيانات وتصنيفها (إن وجدت) والضوابط اللازمة لحماية البيانات والمتطلبات القانونية/التنظيمية. تضمن Glooko إرجاع البيانات الشخصية و/أو حذفها في نهاية علاقة البائع.

ب) اتفاقيات البائعين. تبرم شركة Glooko اتفاقيات مكتوبة مع جميع بائعيها والتي تشمل السرية والخصوصية والتزامات الأمان التي توفر مستوى مناسبًا من الحماية للبيانات الشخصية التي قد يقوم هؤلاء البائعون بمعالجتها.

6. البنية وجدران الحماية وفصل البيانات. يتم تقييد كل عمليات الوصول إلى الشبكة بين مضيفي الإنتاج، باستخدام جدران الحماية للسماح فقط للخدمات المصرح بها بالتفاعل في شبكة الإنتاج. وتُستخدم جدران الحماية لإدارة فصل الشبكة بين مناطق الأمان المختلفة في بيئات الإنتاج والشركات. كما تفصل Glooko قواعد بياناتها بشكل منطقي. تم تصميم وبناء واجهات برمجة تطبيقات Glooko لتحديد والسماح بالوصول فقط من وإلى المرسلين المعنيين. تمنع عناصر التحكم هذه العملاء من الوصول إلى بيانات العملاء الآخرين.

7. الأمان المادي. يتم التحكم في مراكز البيانات التي تستضيف البرنامج بشكلٍ صارم في كل من المحيط الخارجي وعند نقاط الدخول من قبل موظفي الأمان المحترفين الذين يستخدمون المراقبة بالفيديو وأنظمة كشف التسلل وغيرها من الوسائل الإلكترونية. وتتوفر مصادر الطاقة غير المنقطعة والمولدات في الموقع لتوفير طاقة احتياطية في حال حدوث عطل كهربائي. وبالإضافة إلى ذلك، يمتلك مقر Glooko ومساحاتها المكتبية برنامجًا للأمان المادي يتحكم في الزوار ومداخل المباني وأمان المكاتب بشكلٍ عام.

8. الأمان من خلال التصميم. تتبع Glooko مبادئ الأمان من خلال التصميم عند تصميم البرنامج. تطبق Glooko أيضًا معيار دورة حياة تطوير البرمجيات (SDLC) من Glooko لإجراء العديد من الأنشطة المتعلقة بالأمان للبرنامج عبر مراحل مختلفة من دورة حياة إنشاء المنتج بدءًا من جمع المتطلبات وتصميم المنتج ووصولاً إلى نشر المنتج.

9. عناصر التحكم في الوصول

أ) توفير الوصول. لتقليل مخاطر التعرض للبيانات، تتبع Glooko مبادئ الحد الأدنى من الامتيازات من خلال نموذج تحكم في الوصول بناءً على فريق العمل عند توفير الوصول إلى النظام. يحق لموظفي Glooko الوصول إلى البيانات الشخصية بناءً على وظائفهم ودورهم ومسؤولياتهم، ويتطلب هذا الوصول موافقة مدير الموظفين. وتتم إزالة وصول الموظف إلى البيانات الشخصية عند إنهاء وظيفته. لكن قبل منح المهندس إمكانية الوصول إلى بيئة الإنتاج، يجب أن تتم الموافقة على الوصول من قبل الإدارة ويُطلب من المهندس إكمال التدريبات الداخلية لهذا الوصول بما في ذلك التدريب على أنظمة الفريق ذات الصلة. وتُسجل Glooko الإجراءات العالية المخاطر والتغيرات في بيئة الإنتاج. كما تستفيد Glooko من الأتمتة لتحديد أي انحراف عن المعايير التقنية الداخلية التي يمكن أن تشير إلى نشاط غير طبيعي/غير مصرح به لإصدار تنبيه في غضون دقائق من تغيير التكوين.

ب) عناصر التحكم في كلمة المرور. عندما يقوم مستخدم مُصرح له بتسجيل الدخول إلى حسابه، تقوم Glooko بتجزئة بيانات اعتماد المستخدم قبل تخزينها. قد يطلب العملاء أيضًا من المستخدمين المصرح لهم إضافة طبقة أخرى من الأمان إلى حساباتهم باستخدام المصادقة الثنائية (2FA).

10. إدارة التغييرات. تطبق Glooko عملية رسمية لإدارة التغييرات تقوم بها لإدارة التغييرات في بيئة الإنتاج للبرنامج، بما في ذلك أي تغييرات على البرامج والتطبيقات والأنظمة الأساسية الخاصة بها. وتتم مراجعة كل تغيير بعناية وتقييمه في بيئة اختبار قبل نشره في بيئة إنتاج البرنامج. كما يتم توثيق كل التغييرات، بما في ذلك تقييم التغييرات في بيئة الاختبار، باستخدام نظام تسجيل رسمي قابل للمراجعة. ويلزم الحصول على موافقة الأطراف المعنية التنظيمية الصحيحة على نشر التغييرات التي تنطوي على مخاطر عالية. ويتم تنفيذ الخطط والإجراءات أيضًا في حال الحاجة إلى التراجع عن التغيير المنشور للحفاظ على أمان البرنامج.

11. التشفير. بالنسبة إلى البرنامج، (أ) يتم تشفير قواعد البيانات التي تخزن البيانات الشخصية باستخدام معيار التشفير المتقدم و(ب) يتم تشفير البيانات الشخصية عند نقلها بين تطبيق برنامج العميل والبرنامج باستخدام بروتوكول TLS الإصدار 1.2

12. إدارة الثغرات الأمنية. تحتفظ Glooko بضوابط وسياسات للتخفيف من مخاطر الثغرات الأمنية لتحقيق التوازن بين المخاطر ومتطلبات العمل/التشغيل. تستخدم Glooko أداة تابعة لجهة خارجية لإجراء عمليات مسح الثغرات الأمنية ضوئيًا بانتظام لتقييم الثغرات الأمنية في البنية التحتية السحابية وأنظمة الشركات في Glooko.

13. اختبار الاختراق. تُجري Glooko اختبارات الاختراق وتشرك كيانات خارجية مستقلة لإجراء اختبارات الاختراق على مستوى التطبيق. ويتم تحديد أولويات التهديدات والثغرات الأمنية التي يتم اكتشافها وتصنيفها ومعالجتها.

14. إدارة الحوادث الأمنية. تحافظ Glooko على سياسات إدارة الحوادث الأمنية. إذ يقوم فريق الاستجابة للحوادث الأمنية (T-SIRT) التابع لشركة Glooko بتقييم كل التهديدات والثغرات الأمنية ذات الصلة ووضع إجراءات الإصلاح والتخفيف المناسبة. وتحتفظ شركة Glooko بسجلات الأمان ذات الصلة.

15. المرونة واستمرارية البرمجيات. يستخدم البرنامج مجموعة متنوعة من الأدوات والآليات لتحقيق المرونة والتوفر العالي. بالنسبة إلى البرنامج، تمتد البنية التحتية لشركة Glooko لتشمل مناطق توفر متعددة خالية من الأعطال في مناطق جغرافية منفصلة ماديًا بعضها عن بعض. وتستفيد Glooko أيضًا من الأدوات المتخصصة التي تراقب أداء الخادم والبيانات وسعة تحميل حركة البيانات داخل كل منطقة توفر ومركز بيانات مشترك. وإذا تم الكشف عن أداء خادم دون المستوى الأمثل أو سعة تحميل زائدة على خادم ضمن منطقة التوفر أو مركز البيانات المشترك، فإن هذه الأدوات المتخصصة تزيد من السعة أو تنقل حركة البيانات لتخفيف أي أداء خادم دون المستوى الأمثل أو زيادة سعة التحميل. كما يتم إخطار شركة Glooko على الفور في حال وجود أي أداء خادم دون المستوى الأمثل أو سعة تحميل زائدة.

16. النُسخ الاحتياطية والاسترداد. تنشئ Glooko نُسخًا احتياطية منتظمة من البيانات الشخصية. يتم الاحتفاظ بالبيانات الشخصية التي يتم نسخها احتياطيًا بشكلٍ متكرر عبر مناطق توفر متعددة وتشفيرها في أثناء النقل وعند الراحة باستخدام معايير التشفير المتقدمة.

الملحق الرابع: قائمة المعالجين الفرعيين

صرّح المراقب بالاستعانة بالمعالجين الفرعيين الآتين:

1. الاسم: Amazon Web Services EMEA SARL
العنوان: 38 Avenue John F. Kennedy, L-1855, Luxembourg
وصف المعالجة (بما في ذلك تحديد واضح للمسؤوليات في حال التصريح بالعديد من المعالجين الفرعيين): مزود الخدمات السحابية

2. الاسم: Glooko, Inc.
العنوان: 579 University Avenue, Palo Alto, California, 94301

وصف المعالجة (بما في ذلك تحديد واضح للمسؤوليات في حال التصريح بالعديد من المعالجين الفرعيين): لتقديم الدعم الفني وأداء الواجبات القانونية بموجب المتطلبات التنظيمية المعمول بها.