STANDARDOWE KLAUZULE UMOWNE GLOOKO

SEKCJA I

Klauzula 1
Cel i zakres

1. Niniejsze standardowe klauzule umowne (Klauzule) mają na celu zapewnienie zgodności z wymogami artykułu 28 ust. 3 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.
2. Administratorzy i podmioty przetwarzające wymienieni w Załączniku I wyrazili zgodę na niniejsze Klauzule w celu zachowania zgodności z wymogami artykułu 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 i/lub artykułu 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725.
3. Te Klauzule mają zastosowanie, jeśli wymogi określone w umowie ramowej zostały spełnione. Mają również zastosowanie do przetwarzania danych osobowych, jak określono w Załączniku II.
4. Załączniki od I do IV stanowią integralną część niniejszych Klauzul.
5. Niniejsze Klauzule nie naruszają obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679 i/lub rozporządzenia (UE) 2018/1725.
6. Niniejsze Klauzule same w sobie nie zapewniają zgodności z obowiązkami związanymi z międzynarodowym przekazywaniem zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 i/lub rozporządzenia (UE) 2018/1725.

Klauzula 2
Niezmienność klauzul

1. Strony zobowiązują się nie modyfikować Klauzul, za wyjątkiem dodawania informacji do Załączników lub aktualizowania informacji w nich zawartych.
2. Nie uniemożliwia to Stronom włączania standardowych klauzul umownych określonych w niniejszych Klauzulach do szerszej umowy lub dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem, że nie są one bezpośrednio ani pośrednio sprzeczne z niniejszymi Klauzulami ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą.

Klauzula 3
Interpretacja

1. W przypadku gdy w niniejszych Klauzulach stosuje się terminy zdefiniowane odpowiednio w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725, terminy te mają znaczenie nadane im w tym rozporządzeniu.

2. Niniejsze Klauzule należy odczytywać i interpretować w świetle przepisów rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.
3. Klauzul tych nie należy interpretować w sposób sprzeczny z prawami i obowiązkami określonymi w rozporządzeniu (UE) 2016/679 / rozporządzeniu (UE) 2018/1725 lub w jakikolwiek sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

Klauzula 4
Hierarchia

W przypadku sprzeczności między niniejszymi Klauzulami a postanowieniami powiązanych umów między Stronami, obowiązujących w chwili uzgodnienia niniejszych Klauzul lub zawartych w późniejszym terminie, niniejsze Klauzule mają charakter nadrzędny.

Klauzula 5 – Nieobowiązkowa
Klauzula przystąpienia

1. Każdy podmiot, który nie jest Stroną niniejszych Klauzul, może za zgodą Stron przystąpić do tych Klauzul w dowolnym momencie albo jako administrator danych, albo jako podmiot przetwarzający dane, wypełniając Załączniki i podpisując Załącznik I.
2. Po wypełnieniu i podpisaniu załączników w części (a) podmiot przystępujący staje się Stroną niniejszych Klauzul oraz nabywa prawa i obowiązki administratora danych lub podmiotu przetwarzającego dane, zgodnie z jego określeniem w Załączniku I.
3. Podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych Klauzul w odniesieniu do okresu, zanim został ich Stroną.

SEKCJA II – OBOWIĄZKI STRON

Klauzula 6
Opis przetwarzania

Szczegóły operacji przetwarzania, w szczególności kategorie danych osobowych oraz cele przetwarzania, w jakich dane osobowe są przetwarzane w imieniu administratora, określa Załącznik II.

Klauzula 7
Obowiązki Stron
7.1. Polecenia

1. Podmiot przetwarzający dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na

niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny. Dalsze polecenia mogą również być udzielane przez administratora przez cały okres przetwarzania danych osobowych. W każdym przypadku te polecenia muszą być udokumentowane.
2. Podmiot przetwarzające dane niezwłocznie poinformuje administratora, jeśli w jego opinii polecenia wydane przez administratora naruszają postanowienia rozporządzenia (UE) 2016/679 / rozporządzenia (UE) 2018/1725 lub obowiązujące przepisy Unii lub państwa członkowskiego dotyczące ochrony danych.

7.2. Ograniczenie celu

Podmiot przetwarzający dane przetwarza dane osobowe wyłącznie w określonym celu / określonych celach przekazywania, jak wskazano w Załączniku II, chyba że działa na podstawie dalszych poleceń wydanych przez administratora.

7.3. Czas trwania przetwarzania danych

Przetwarzanie danych przez podmiot przetwarzający dane odbywa się wyłącznie przez czas określony w Załączniku II.

7.4. Bezpieczeństwo przetwarzania

1. Podmiot przetwarzający dane wdraża odpowiednie środki techniczne i organizacyjne określone w Załączniku II w celu zapewnienia bezpieczeństwa danych osobowych. Obejmuje to ochronę przeciwko naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do tych danych (zwanego dalej „naruszeniem ochrony danych osobowych”). Przy ocenie odpowiedniego poziomu bezpieczeństwa Strony uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osób, których dane dotyczą.
2. Podmiot przetwarzający dane udziela dostępu do danych osobowych członkom swojego personelu wyłącznie w zakresie ściśle niezbędnym do wykonywania umowy, zarządzania umową oraz jej monitorowania. Podmiot przetwarzający dane zapewni, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

7.5. Dane wrażliwe

Gdy przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących i czynów zabronionych (zwane dalej „danymi wrażliwymi"), podmiot przetwarzający dane stosuje szczególne ograniczenia i/lub dodatkowe zabezpieczenia.

7.6 Dokumentacja i zgodność

1. Strony będą w stanie wykazać przestrzeganie niniejszych klauzul.
2. Podmiot przetwarzający dane niezwłocznie i w odpowiedni sposób rozpatruje zapytania administratora dotyczące przetwarzania danych na mocy niniejszych klauzul.
3. Podmiot przetwarzający dane udostępnia administratorowi wszelkie informacje niezbędne, aby wykazać przestrzeganie obowiązków określonych w niniejszych Klauzulach, wynikających z rozporządzenia (UE) 2016/679 i/lub rozporządzenia (UE) 2018/1725. Na wniosek administratora podmiot przetwarzający dane umożliwia również przeprowadzanie audytów czynności przetwarzania objętych niniejszymi klauzulami w rozsądnych odstępach czasu lub w przypadku wystąpienia oznak niespełnienia tych obowiązków, a także wnosi wkład w te audyty. Podejmując decyzję dotyczącą przeglądu lub przeprowadzenia audytu, administrator może uwzględnić odpowiednie certyfikacje posiadane przez podmiot przetwarzający dane.
4. Administrator może przeprowadzić audyt samodzielnie lub zlecić jego przeprowadzenie niezależnemu audytorowi. Audyty mogą obejmować kontrole w siedzibie lub obiektach podmiotu przetwarzającego dane i, w stosownych przypadkach, przeprowadzane są po powiadomieniu z rozsądnym wyprzedzeniem.
5. Strony udostępniają właściwemu organowi nadzorczemu / właściwym organom nadzorczym na żądanie informacje, o których mowa w niniejszych klauzulach, w tym wyniki wszelkich audytów.

7.7. Korzystanie z usług podwykonawców przetwarzania

1. Podmiot przetwarzający dane ma ogólną zgodę administratora na angażowanie podwykonawców przetwarzania widniejących w uzgodnionym wykazie. Podmiot przetwarzający dane wyraźnie informuje na piśmie administratora o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podwykonawców przetwarzania z wyprzedzeniem wynoszącym co najmniej trzydzieści (30) dni, dając w ten sposób administratorowi wystarczający czas na

wyrażenie sprzeciwu wobec takich zmian przed zaangażowaniem podwykonawcy lub podwykonawców przetwarzania. Podmiot przetwarzający dane dostarcza administratorowi informacje niezbędne do umożliwienia mu skorzystania z prawa do sprzeciwu.

2. Jeżeli podmiot przetwarzający dane angażuje podwykonawcę przetwarzania do celów wykonania określonych czynności przetwarzania (w imieniu administratora), czyni to na podstawie pisemnej umowy, która zasadniczo przewiduje takie same obowiązki dla podwykonawcy przetwarzania w odniesieniu do ochrony danych, jakie wiążą podmiot przetwarzający dane na mocy niniejszych klauzul. Podmiot przetwarzający dane zapewnia, że podwykonawca przetwarzania wywiązuje się z obowiązków ciążących na podmiocie przetwarzającym dane zgodnie z niniejszymi Klauzulami oraz rozporządzeniem (UE) 2016/679 i/lub rozporządzeniem (UE) 2018/1725.
3. Na żądanie administratora podmiot przetwarzający dane przekazuje administratorowi kopię umowy dotyczącej podwykonawstwa przetwarzania oraz wszelkich późniejszych zmian. W zakresie koniecznym do zapewnienia ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający dane może zredagować tekst umowy przed udostępnieniem jej kopii.
4. Podmiot przetwarzający dane pozostaje w pełni odpowiedzialny wobec administratora za wykonywanie obowiązków podwykonawcy przetwarzania wynikających z umowy zawartej przez niego z podmiotem przetwarzającym dane. Podmiot przetwarzający dane powiadamia administratora o każdym przypadku niewypełnienia przez podwykonawcę przetwarzania obowiązków wynikających z tej umowy.
5. Podmiot przetwarzający dane, w możliwym zakresie, uzgadnia z podwykonawcą przetwarzania klauzulę na rzecz osoby trzeciej, na rzecz której zawarto umowę, na mocy której to klauzuli – w przypadku gdy podmiot przetwarzający dane przestał istnieć faktycznie lub formalnie lub stał się niewypłacalny – administrator ma prawo rozwiązać umowę dotyczącą podwykonawstwa przetwarzania i polecić podwykonawcy przetwarzania usunięcie lub zwrot danych osobowych.

7.8. Międzynarodowe przekazywanie danych

1. Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający dane może nastąpić wyłącznie na podstawie udokumentowanych poleceń administratora lub w celu wypełnienia szczególnego wymogu wynikającego z prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający dane i powinno odbywać się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

2. Administrator zgadza się, że w przypadku gdy podmiot przetwarzający dane angażuje podwykonawcę przetwarzania zgodnie z Klauzulą 7.7 do celów wykonania określonych czynności przetwarzania (w imieniu administratora), a te czynności przetwarzania obejmują przekazywanie danych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, podmiot przetwarzający dane i podwykonawca przetwarzania mogą zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679, stosując standardowe klauzule umowne przyjęte przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679 pod warunkiem, że spełnione są warunki stosowania tych standardowych klauzul umownych.

Klauzula 8
Wsparcie dla administratora

1. W przypadku otrzymania przez podmiot przetwarzający dane żądania od osób, których dane dotyczą, odsyła on te osoby do kontaktu z administratorem. Nie odpowiada samodzielnie na żądania, chyba że administrator wyrazi na to zgodę.
2. Podmiot przetwarzający dane wspiera administratora w wywiązaniu się z jego obowiązków w zakresie reagowania na żądania osób, których dane dotyczą, w zakresie korzystania z ich praw, biorąc pod uwagę charakter przetwarzania. Wypełniając swoje obowiązki zgodnie z lit. (a) i (b), podmiot przetwarzający dane ma obowiązek stosować się do poleceń administratora.
3. Oprócz obowiązku podmiotu przetwarzającego dane dotyczącego udzielenia wsparcia administratorowi zgodnie z klauzulą 8 lit. b), podmiot przetwarzający dane ponadto pomaga administratorowi w zapewnieniu przestrzegania następujących obowiązków, biorąc pod uwagę charakter przetwarzania danych oraz informacje, którymi dysponuje podmiot przetwarzający dane:
    1. obowiązek przeprowadzania oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych (zwanej dalej „oceną skutków dla ochrony danych”), w przypadku których rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
    2. obowiązek konsultacji z właściwym organem nadzorczym / właściwymi organami nadzorczymi przed przystąpieniem do przetwarzania, jeżeli ocena skutków dla ochrony danych wskazuje, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka;
    3. obowiązek zapewnienia prawidłowości i aktualności danych osobowych, poprzez niezwłoczne poinformowanie administratora, jeżeli podmiot przetwarzający dowie się, że przetwarzane przez niego dane osobowe są nieprawidłowe lub zdezaktualizowane;

4. obowiązki określone w art. 32 rozporządzenia (UE) 2016/679.

4. Strony uzgodniły środki techniczne i organizacyjne określone w Załączniku III, za pomocą których podmiot przetwarzający dane ma obowiązek wspierać administratora w stosowaniu niniejszej klauzuli, a także zakres i stopień wymaganego wsparcia.

Klauzula 9

Zawiadamianie o naruszeniu ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający dane współpracuje z administratorem i pomaga mu w wywiązaniu się z jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679 lub art. 34 i 35 rozporządzenia (UE) 2018/1725, w stosownych przypadkach, uwzględniając charakter przetwarzania i informacje dostępne podmiotowi przetwarzającemu dane.

9.1. Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający dane wspiera administratora w następującym zakresie:

1. informowanie odpowiedniego organu nadzorczego / odpowiednich organów nadzorczych o naruszeniu ochrony danych osobowych bez zbędnej zwłoki po tym, jak administrator dowiedział się o naruszeniu, jeżeli ma to zastosowanie / (chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);
2. uzyskiwanie następujących informacji, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 powinny zostać podane w zgłoszeniu administratora i muszą opisywać co najmniej:
    1. charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    2. możliwe konsekwencje naruszenia ochrony danych osobowych;
    3. środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, początkowe zgłoszenie może zawierać dostępne wówczas informacje, a dalsze

informacje, gdy tylko staną się dostępne, będą udzielane sukcesywnie bez zbędnej zwłoki.

3. wywiązywanie się, zgodnie z art. 34 rozporządzenia (UE) 2016/679, z obowiązku poinformowania bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie ochrony danych osobowych z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

9.2. Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający dane

W przypadku naruszenia ochrony danych osobowych przetwarzanych przez podmiot przetwarzający dane, podmiot przetwarzający dane bez zbędnej zwłoki po stwierdzeniu naruszenia zgłasza je administratorowi. Takie zgłoszenie musi zawierać co najmniej:

1. opis charakteru naruszenia (w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą i wpisów danych osobowych, których dotyczy naruszenie);
2. dane osoby do kontaktu, od której można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
3. opis możliwych konsekwencji i środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, początkowe zgłoszenie może zawierać dostępne wówczas informacje, a dalsze informacje, gdy tylko staną się dostępne, będą udzielane sukcesywnie bez zbędnej zwłoki.

W Załączniku III Strony określają wszystkie pozostałe elementy, które podmiot przetwarzający dane ma zapewnić, pomagając administratorowi w wypełnianiu obowiązków administratora wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679.

SEKCJA III – POSTANOWIENIA KOŃCOWE

Klauzula 10

Brak zgodności z klauzulami i rozwiązanie umowy

1. W przypadku gdy podmiot przetwarzający dane narusza postanowienia niniejszych klauzul, administrator może poinstruować podmiot przetwarzający dane, aby zawiesił przetwarzanie danych osobowych do chwili ponownego zapewnienia przestrzegania klauzul lub rozwiązania umowy ramowej. Powyższe pozostaje bez uszczerbku dla postanowień rozporządzenia (UE) 2016/679 i/lub rozporządzenia (UE) 2018/1725. Podmiot przetwarzający dane niezwłocznie

informuje administratora, jeżeli z jakiegokolwiek powodu nie może zapewnić przestrzegania postanowień niniejszych klauzul.

2. Administrator jest uprawniony do rozwiązania umowy ramowej – o ile problem dotyczy przetwarzania danych osobowych na podstawie niniejszych klauzul – w przypadku, gdy:
    1. działanie polegające na przetwarzaniu danych przez podmiot przetwarzający dane zostało wstrzymane przez administratora na podstawie lit. (a), a zgodność z postanowieniami niniejszych klauzul nie została przywrócona w rozsądnym terminie, a w każdym razie w ciągu jednego miesiąca od wstrzymania;
    2. podmiot przetwarzający dane w poważnym stopniu lub uporczywie narusza swoje obowiązki wynikające z rozporządzenia (UE) 2016/679 i/lub rozporządzenia (UE) 2018/1725;
    3. podmiot przetwarzający dane nie zastosował się do wiążącej decyzji właściwego sądu lub organu nadzorczego dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679 i/lub rozporządzenia (UE) 2018/1725.
3. Podmiot przetwarzający dane ma prawo rozwiązać umowę ramową w zakresie dotyczącym przetwarzania danych osobowych na mocy niniejszych klauzul, jeżeli po poinformowaniu administratora, że jego polecenia naruszają obowiązujące wymagania prawne zgodnie z klauzulą 7.1 lit. b), administrator nalega na przestrzeganie poleceń.
4. Po rozwiązaniu umowy ramowej podmiot przetwarzający dane, zgodnie z wyborem administratora albo usuwa wszystkie dane osobowe przetworzone w imieniu administratora i potwierdza administratorowi ich usunięcie, albo zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, o ile prawo państwa członkowskiego nie wymaga przechowywania danych osobowych. Jeżeli administrator nie zażądał zwrotu wszystkich danych osobowych przetwarzanych w jego imieniu w ciągu trzydziestu (30) dni od rozwiązania umowy ramowej, podmiot przetwarzający ma prawo, według własnego uznania, usunąć dane osobowe. Do czasu usunięcia lub zwrotu danych podmiot przetwarzający dane nadal zapewnia zgodność z niniejszymi klauzulami.

ZAŁĄCZNIK I: WYKAZ STRON

Administrator(-rzy):

1. Klient (zgodnie z umową ramową lub formularzem zamówienia)

Podmiot(y) przetwarzający(-e) dane:

1. Glooko AB (zgodnie z umową ramową)

ZAŁĄCZNIK II: OPIS PRZETWARZANIA

Kategorie osób, których dane dotyczą i których dane są przetwarzane
– Upoważnieni użytkownicy
– Pacjenci
Kategorie przetwarzanych danych osobowych

W przypadku upoważnionych użytkowników
– Dane ogólne (imię i nazwisko)
– Dane kontaktowe (adres e-mail, numer telefonu)
– Dane dotyczące użytkowania (nazwa użytkownika, hasło, prawa dostępu, dzienniki kontroli)

W przypadku pacjentów
– Dane ogólne (imię i nazwisko, data urodzenia, płeć)
– Dane kontaktowe (adres korespondencyjny, adres e-mail, numer telefonu)
– Dane dotyczące użytkowania (nazwa użytkownika, hasło)
– Dane dotyczące zdrowia (typ cukrzycy, rok zdiagnozowania cukrzycy, szacowana data porodu, zakres docelowy, masa ciała, wzrost, leczenie)
– Informacje dotyczące urządzenia (numer[y] seryjny[-e] pompy insulinowej, glukometru i wstrzykiwacza insuliny, dawki, węglowodany, ustawienia, alarmy)

Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nim ryzyko, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla pracowników, który odbyli specjalistyczne szkolenie), przechowywanie zapisów przypadków uzyskiwania dostępu do danych, ograniczenia dalszego przekazywania lub dodatkowe środki bezpieczeństwa
– Dane dotyczące stanu zdrowia
Informacje dotyczące wdrożonych zabezpieczeń znajdują się w Załączniku III.

Charakter przetwarzania
Gromadzenie, analizowanie, wizualizacja i przetwarzanie w inny sposób danych osobowych zgodnie z umową ramową.

Cel(e), w którym(-ch) dane osobowe są przetwarzane w imieniu administratora
Umożliwienie administratorowi oraz upoważnionym użytkownikom korzystanie z oprogramowania i innych materiałów zgodnie z umową ramową.

Czas trwania przetwarzania
Na czas dostarczania oprogramowania i innych materiałów zgodnie z umową ramową.

W przypadku przetwarzania przez podmioty przetwarzające dane (lub podwykonawców przetwarzania) należy również wskazać przedmiot, charakter i czas trwania przetwarzania.
Patrz Załącznik IV.
Instrukcje zawarte w punkcie 7.8 a) niniejszych klauzul dotyczące międzynarodowego przekazywania danych
Standardowe klauzule umowne dotyczące międzynarodowego przekazywanie danych (zwane dalej „SCC") określone w Załączniku V będą miały zastosowanie w przypadku przekazywania danych osobowych przez podmiot przetwarzający poza obszar EOG, do kraju nieuznawanego przez Komisję Europejską za zapewniający odpowiedni stopień ochrony danych osobowych.

ZAŁĄCZNIK III: ŚRODKI TECHNICZNE I ORGANIZACYJNE, W TYM ŚRODKI TECHNICZNE I ORGANIZACYJNE MAJĄCE NA CELU ZAPEWNIENIE BEZPIECZEŃSTWA DANYCH

1. Cel. W niniejszym Załączniku opisano program bezpieczeństwa firmy Glooko, certyfikaty bezpieczeństwa oraz środki techniczne i organizacyjne mające na celu ochronę (a) danych osobowych przetwarzanych przez podmiot przetwarzający dane w imieniu administratora przed nieuprawnionym użyciem, dostępem, ujawnieniem lub kradzieżą oraz (b) oprogramowania. W miarę zmieniania się i ewoluowania zagrożeń dla bezpieczeństwa firma Glooko stale aktualizuje swój program i strategię bezpieczeństwa, aby pomóc chronić dane osobowe i oprogramowanie. Na przykład firma Glooko zastrzega sobie prawo do okresowej aktualizacji niniejszego załącznika, pod warunkiem, że żadna aktualizacja nie zmniejszy w istotny sposób ogólnych zabezpieczeń określonych w niniejszym Załączniku.
2. Organizacja i program bezpieczeństwa. Firma Glooko utrzymuje program bezpieczeństwa oparty na ocenie ryzyka. Schemat programu bezpieczeństwa firmy Glooko obejmuje zabezpieczenia administracyjne, organizacyjne, techniczne i fizyczne, zaprojektowane z myślą o ochronie oprogramowania oraz poufności, integralności i dostępności danych osobowych. Program bezpieczeństwa firmy Glooko ma odpowiadać charakterowi oprogramowania oraz skali i złożoności działalności biznesowej firmy Glooko. Firma Glooko posiada odrębny i dedykowany zespół ds. bezpieczeństwa danych, który zarządza programem bezpieczeństwa firmy. Ten zespół ułatwia i wspiera przeprowadzanie niezależnych audytów i ocen przez strony trzecie. Schemat bezpieczeństwa firmy Glooko obejmuje programy dotyczące następujących zagadnień: polityki i procedury, zarządzanie aktywami, zarządzanie dostępem, kryptografia, bezpieczeństwo fizyczne, bezpieczeństwo operacji, bezpieczeństwo komunikacji, bezpieczeństwo ciągłości działania, bezpieczeństwo dot. ludzi,

bezpieczeństwo produktów, bezpieczeństwo chmury i infrastruktury sieciowej, zgodność z zasadami bezpieczeństwa, bezpieczeństwo stron trzecich, zarządzanie lukami w zabezpieczeniach, monitorowanie bezpieczeństwa i reakcja na incydenty. Osoby odpowiedzialne za zarządzanie bezpieczeństwem zajmują najwyższe stanowiska w strukturach firmy. Specjalista ds. bezpieczeństwa firmy Glooko regularnie odbywa spotkania z kadrą kierowniczą w celu omówienia problemów i koordynowania działań dotyczących bezpieczeństwa w całej firmie. Polityki i normy dotyczące bezpieczeństwa danych są kontrolowane i zatwierdzane przez kadrę kierowniczą co najmniej raz w roku i są udostępniane pracownikom firmy Glooko do wglądu.

3. Poufność. Firma Glooko wdrożyła czynności kontrolne, aby zachować poufność danych osobowych zgodnie z umową ramową. Wszystkich pracowników i członków personelu kontraktowego firmy Glooko obowiązują wewnętrzne polityki firmy Glooko dotyczące zachowania poufności danych osobowych. Są oni zobowiązani umową do przestrzegania tych obowiązków.
4. Bezpieczeństwo dot. ludzi
    1. Weryfikacja życiorysu pracownika. Firma Glooko przeprowadza weryfikację życiorysów wszystkich nowych pracowników w chwili zatrudnienia zgodnie z obowiązującymi lokalnymi przepisami. Obecnie firma Glooko weryfikuje wykształcenie i dotychczasowe zatrudnienie nowego pracownika oraz sprawdza wskazane referencje. Jeśli jest to dopuszczalne na mocy obowiązującego prawa, firma Glooko może również przeprowadzać kontrole danych o karalności, historii kredytowej, imigracyjnej i dotyczącej bezpieczeństwa, w zależności od charakteru i zakresu stanowiska nowego pracownika.
    2. Szkolenie pracowników. Co najmniej raz (1) w roku wszyscy pracownicy firmy Glooko muszą przejść pełne szkolenie dotyczące bezpieczeństwa i ochrony prywatności, które obejmuje wszystkie polityki dotyczące bezpieczeństwa, najlepsze praktyki w zakresie bezpieczeństwa i zasady ochrony prywatności firmy Glooko. Pracownicy będący na urlopie otrzymają dodatkowy czas na ukończenie tego corocznego szkolenia. Dedykowany zespół ds. bezpieczeństwa firmy Glooko przeprowadza również kampanie szerzące świadomość phishingu oraz przekazuje pracownikom informacje na temat nowych zagrożeń.
5. Zarządzanie zewnętrznymi dostawcami
    1. Ocena dostawcy. Firma Glooko może korzystać z usług zewnętrznych dostawców w kwestii dostarczania oprogramowania. Firma Glooko przeprowadza ocenę bezpieczeństwa opartą na ryzyku w stosunku do potencjalnych dostawców przez rozpoczęciem współpracy w celu zweryfikowania, czy spełniają oni wymogi dotyczące bezpieczeństwa firmy

Glooko. Okresowo firma Glooko dokonuje przeglądu każdego dostawcy pod kątem standardów bezpieczeństwa i ciągłości działania firmy Glooko. Obejmuje to przegląd rodzaju dostępu i klasyfikacji danych, do których dostawca uzyskuje dostęp (w stosownych przypadkach), kontroli niezbędnych do ochrony danych oraz wymogów prawnych/regulacyjnych. Firma Glooko upewnia się, że dane osobowe zostają zwrócone i/lub usunięte pod koniec współpracy z dostawcą.

2. Umowy z dostawcami. Firma Glooko zawiera pisemne umowy ze wszystkimi dostawcami. Obejmują one obowiązek zachowania poufności, ochrony prywatności i zobowiązania dotyczące bezpieczeństwa, które zapewniają odpowiedni poziom ochrony danych osobowych, które mogą być przetwarzane przez tych dostawców.

6. Architektura, zapora sieciowa i segregacja danych. Każdy dostęp sieciowy pomiędzy hostami produkcyjnymi jest ograniczony przy użyciu zapór sieciowych, aby umożliwić interakcję w sieci produkcyjnej tylko autoryzowanym usługom. Zapora sieciowa jest stosowana w celu zarządzania segregacją sieci między różnymi strefami bezpieczeństwa w środowisku produkcyjnym i korporacyjnym. Firma Glooko w sposób logiczny oddziela swoje bazy danych. Interfejsy oprogramowania aplikacji (API) Glooko zostały zaprojektowane w taki sposób, aby identyfikowały i zezwalały na dostęp wyłącznie do i od odpowiednich nadawców. Te środki kontrolne uniemożliwiają klientom uzyskanie dostępu do danych innych klientów.
7. Bezpieczeństwo fizyczne. Centra danych, które są hostami oprogramowania, są ściśle kontrolowane zarówno w okolicy, jak i w punktach wejścia do budynków przez profesjonalnych pracowników ochrony korzystających z monitoringu wideo, systemów wykrywania włamań i innych środków elektronicznych. W obiektach dostępne są zasilacze bezprzerwowe i generatory, które zapewniają zasilanie awaryjne w przypadku awarii prądu. Ponadto siedziba główna oraz przestrzenie biurowe firmy Glooko posiadają program zapewnienia bezpieczeństwa fizycznego, który ma na celu zarządzanie gośćmi, wejściami do budynków i ogólnym bezpieczeństwem biura.
8. Bezpieczeństwo w fazie projektowania. Projektując oprogramowanie, firma Glooko kieruje się zasadami bezpieczeństwa już w fazie projektowania. Firma Glooko stosuje normę dotyczącą cyklu życia rozwoju oprogramowania (SDLC) w celu przeprowadzenia licznych czynności związanych z bezpieczeństwem w kontekście oprogramowania w różnych fazach cyklu tworzenia produktu, począwszy od gromadzenia wymogów oraz projektowania produktu, aż po prace rozwojowe produktu.

9. Kontrola dostępu
    1. Udzielanie dostępu. Aby zminimalizować ryzyko ujawnienia danych, udzielając dostępu do systemu, firma Glooko przestrzega zasady nadawania najmniejszych uprawnień w myśl modelu kontroli dostępu opartego na zespołach. Pracownicy firmy Glooko są upoważnieni do uzyskiwania dostępu do danych osobowych w zależności od pełnionej przez nich funkcji, ich roli i obowiązków, a dostęp taki wymaga zgody przełożonego danego pracownika. Dostęp pracownika do danych osobowych jest usuwany w chwili zakończenia stosunku pracy. Zanim inżynier uzyska dostęp do środowiska produkcyjnego, dostęp musi zostać zatwierdzony przez kadrę kierowniczą, a inżynier musi ukończyć wewnętrzne szkolenia wymagane do uzyskania takiego dostępu, w tym szkolenia z systemów odpowiedniego zespołu. Firma Glooko rejestruje czynności wysokiego ryzyka i zmiany w środowisku produkcyjnym. Firma Glooko wykorzystuje automatyzację do identyfikowania wszelkich odstępstw od wewnętrznych norm technicznych, które mogą wskazywać na nietypowe/nieautoryzowane czynności, w celu zgłoszenia ostrzeżenia w ciągu kilku minut od zmiany konfiguracji.
    2. Kontrole dotyczące haseł. Kiedy upoważniony użytkownik loguje się na swoje konto, firma Glooko haszuje dane uwierzytelniające użytkownika zanim zostaną one zachowane. Klienci mogą również wymagać od upoważnionych użytkowników dodania kolejnej warstwy zabezpieczeń do swojego konta w postaci uwierzytelniania dwuskładnikowego (2FA).
10. Zarządzanie zmianą. Firma Glooko postępuje zgodnie z wdrożonym formalnym procesem zarządzania zmianą, który ma na celu kierowanie zmianami w środowisku produkcyjnym oprogramowania, w tym wszelkimi zmianami w podstawowym oprogramowaniu, aplikacjach i systemach. Każda zmiana jest uważnie weryfikowana i oceniana w środowisku testowym przed jej wdrożeniem w środowisku produkcyjnym oprogramowania. Wszystkie zmiany, łącznie z oceną zmian w środowisku testowym, są rejestrowane w formalnym systemie zapisów, który można poddawać audytom. Wymagane jest zatwierdzenie wdrożenia zmian wiążących się z wysokim ryzykiem przez odpowiednich interesariuszy w organizacji. Wdrażane są także plany i procedury na wypadek konieczności wycofania wdrożonej zmiany w celu zachowania bezpieczeństwa oprogramowania.
11. Szyfrowanie. W przypadku oprogramowania (a) bazy danych, w których przechowywane są dane osobowe są szyfrowane za pomocą szyfru Advanced Encryption Standard oraz (b) dane osobowe są szyfrowane podczas przesyłania między aplikacją klienta a oprogramowaniem przy użyciu protokołu TLS v1.2.

12. Zarządzanie lukami w zabezpieczeniach. Firma Glooko utrzymuje czynności kontrolne i polityki mające na celu ograniczenie ryzyka luk w zabezpieczeniach, aby wprowadzić równowagę między ryzykiem a wymaganiami biznesowymi/operacyjnymi. Firma Glooko korzysta z narzędzia podmiotu zewnętrznego do regularnego przeprowadzania skanów luk w zabezpieczeniach, aby ocenić luki w infrastrukturze chmury i systemach korporacyjnych Glooko.
13. Testy penetracyjne. Firma Glooko przeprowadza testy penetracyjne i zatrudnia niezależne podmioty zewnętrzne do przeprowadzania testów penetracyjnych na poziomie aplikacji. Zagrożeniom bezpieczeństwa i lukom w zabezpieczeniach, które są wykrywane, nadawany jest priorytet, a następnie są one kategoryzowane i naprawiane.
14. Zarządzanie incydentami dotyczącymi bezpieczeństwa. Firma Glooko posiada polityki zarządzania incydentami dotyczącymi bezpieczeństwa. Zespół ds. reakcji na incydenty dotyczące bezpieczeństwa (T-SIRT) firmy Glooko ocenia wszystkie istotne zagrożenia i luki w zabezpieczeniach oraz ustala odpowiednie działania zaradcze i łagodzące. Firma Glooko przechowuje odpowiednie rejestry bezpieczeństwa.
15. Odporność i ciągłość oprogramowania. Oprogramowanie wykorzystuje różne narzędzia i mechanizmy w celu osiągnięcia wysokiej dostępności i odporności. W kwestii oprogramowania infrastruktura firmy Glooko obejmuje wiele niezależnych od usterek stref dostępności w regionach geograficznych znajdujących się w pewnej odległości od siebie. Firma Glooko wykorzystuje również specjalistyczne narzędzia monitorujące wydajność serwerów, dane i obciążenie ruchem w każdej strefie dostępności i kolokacji centrum danych. W przypadku wykrycia nieoptymalnej wydajności serwera lub przeciążenia serwera w strefie dostępności lub kolokacji, te specjalistyczne narzędzia zwiększają pojemność lub przekierowują ruch, aby skorygować nieoptymalną wydajność serwera lub przeciążenie. Firma Glooko jest niezwłocznie informowana o stwierdzeniu nieoptymalnej wydajności serwera lub przeciążenia serwera.
16. Kopie zapasowe i odzyskiwanie. Firma Glooko regularnie tworzy kopie zapasowe danych osobowych. Dane osobowe, których kopie zapasowe są tworzone, są przechowywane w wielu strefach dostępności i są szyfrowane podczas przesyłania i przechowywania przy użyciu szyfrów Advanced Encryption Standards.

ZAŁĄCZNIK IV: WYKAZ PODWYKONAWCÓW PRZETWARZANIA

Administrator zezwolił na korzystanie z usług następujących podwykonawców przetwarzania:

1. Nazwa: Amazon Web Services EMEA SARL
   Adres: 38 Avenue John F. Kennedy, L-1855, Luxembourg

Opis przetwarzania (w tym wyraźnie rozgraniczenie obowiązków, jeżeli upoważnionych jest kilku podwykonawców przetwarzania): Dostawca usług w chmurze

2. Nazwa: Glooko, Inc.
   Adres: 579 University Avenue, Palo Alto CA 94301

Opis przetwarzania (w tym wyraźnie rozgraniczenie obowiązków, jeżeli upoważnionych jest kilku podwykonawców przetwarzania): Zapewnienie wsparcia technicznego i wykonywanie swoich obowiązków prawnych zgodnie z obowiązującymi wymogami regulacyjnymi.