PŘÍLOHA 2

STANDARDNÍ SMLUVNÍ DOLOŽKY SPOLEČNOSTI GLOOKO

ČÁST I

Doložka 1

Účel a rozsah

(a) Účelem těchto standardních smluvních doložek (dále jen „doložky“) je zajistit soulad s čl. 28 odst. 3 a 4 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

(b) Správci a zpracovatelé uvedení v příloze I souhlasili s těmito doložkami, aby zajistili soulad s čl. 28 odst. 3 a 4 nařízení (EU) 2016/679 a/nebo čl. 29 odst. 3 a 4 nařízení (EU) 2018/1725.

(c) Tyto doložky se vztahují na zpracování osobních údajů, jak je uvedeno v příloze II.

(d) Přílohy I až IV tvoří nedílnou součást doložek.

(e) Těmito doložkami nejsou dotčeny povinnosti, které se na správce vztahují na základě nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

(f) Tyto doložky samy o sobě nezajišťují splnění povinností týkajících se mezinárodního předávání v souladu s kapitolou V nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

Doložka 2

Neměnnost doložek

(a) Strany se zavazují, že nebudou tyto doložky měnit, s výjimkou doplnění informací do příloh nebo aktualizace informací v nich uvedených.

(b) To nebrání smluvním stranám zahrnout standardní smluvní doložky stanovené v těchto doložkách do širší smlouvy nebo přidat další doložky či dodatečné záruky za předpokladu, že nejsou v přímém či nepřímém rozporu s těmito doložkami nebo nenarušují základní práva či svobody subjektů údajů.

Doložka 3

Výklad

(a) Pokud se v těchto doložkách používají pojmy definované v nařízení (EU) 2016/679, případně v nařízení (EU) 2018/1725, mají tyto pojmy stejný význam jako v uvedeném nařízení.

(b) Tyto doložky se vykládají s ohledem na ustanovení nařízení (EU) 2016/679, případně nařízení (EU) 2018/1725.

(c) Tyto doložky nelze vykládat způsobem, který by byl v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679 / nařízení (EU) 2018/1725 nebo způsobem, který by poškozoval základní práva nebo svobody subjektů údajů.

Doložka 4

Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod mezi stranami, které existovaly v době sjednání těchto doložek nebo byly uzavřeny později, mají přednost tyto doložky.

Doložka 5 – volitelná

Dokovací doložka

(a) Každý subjekt, který není stranou těchto doložek, může se souhlasem všech stran k těmto doložkám kdykoli přistoupit jako správce nebo zpracovatel vyplněním příloh a podpisem přílohy I.

(b) Jakmile jsou přílohy uvedené v písmenu a) vyplněny a podepsány, přistupující subjekt se považuje za stranu těchto doložek a má práva a povinnosti správce nebo zpracovatele v souladu se svým označením v příloze I.

(c) Přistupující subjekt nemá žádná práva ani povinnosti vyplývající z těchto doložek za období předtím, než se stal smluvní stranou.

ČÁST II – POVINNOSTI STRAN

Doložka 6

Popis zpracování

Podrobnosti o operacích zpracování, zejména kategorie osobních údajů a účely zpracování, pro které jsou osobní údaje jménem správce zpracovávány, jsou uvedeny v příloze II.

Doložka 7

Povinnosti stran

7.1. Pokyny

(a) Zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů správce, pokud to po něm nevyžaduje právo Unie nebo členského státu, které se na zpracovatele vztahuje. V takovém případě musí zpracovatel před zpracováním informovat správce o tomto právním požadavku, pokud to zákon nezakazuje z důležitých důvodů veřejného zájmu. Po celou dobu zpracování osobních údajů může správce vydávat i následné pokyny. Tyto pokyny budou vždy doloženy.

(b) Zpracovatel neprodleně informuje správce, pokud podle jeho názoru pokyny správce porušují nařízení (EU) 2016/679 / nařízení (EU) 2018/1725 nebo příslušné předpisy Unie nebo členského státu o ochraně údajů.

7.2. Omezení účelu

Pokud zpracovatel od správce neobdrží další pokyny, zpracovává osobní údaje pouze pro konkrétní účel (účely) zpracování, jak je uvedeno v příloze II.

7.3. Doba zpracování osobních údajů

Zpracování ze strany zpracovatele probíhá pouze po dobu uvedenou v příloze II.

7.4. Bezpečnost zpracování

(a) Zpracovatel zavede alespoň technická a organizační opatření uvedená v příloze III, aby zajistil zabezpečení osobních údajů. To zahrnuje ochranu údajů před porušením zabezpečení, které vede k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zveřejnění nebo přístupu k údajům (porušení zabezpečení osobních údajů). Při posuzování vhodné úrovně zabezpečení strany náležitě zohlední stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování a související rizika pro subjekty údajů.

(b) Zpracovatel umožní přístup ke zpracovávaným osobním údajům svým zaměstnancům pouze v rozsahu nezbytně nutném pro provádění, správu a monitorování smlouvy. Zpracovatel zajistí, aby se osoby oprávněné zpracovávat obdržené osobní údaje zavázaly k mlčenlivosti nebo měly příslušnou zákonnou povinnost mlčenlivosti.

7.5. Citlivé údaje

Pokud zpracování zahrnuje osobní údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje týkající se zdraví nebo sexuálního života či sexuální orientace osoby nebo údaje týkající se rozsudků v trestních věcech a trestných činů („citlivé údaje“), použije zpracovatel zvláštní omezení a/nebo další ochranná opatření.

7.6. Dokumentace a soulad

(a) Strany musí být schopny prokázat soulad s těmito doložkami.

(b) Zpracovatel neprodleně a přiměřeně vyřídí dotazy správce týkající se zpracování údajů v souladu s těmito doložkami.

(c) Zpracovatel zpřístupní správci veškeré informace nezbytné k prokázání splnění povinností, které jsou stanoveny v těchto doložkách a vyplývají přímo z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725. Na žádost správce zpracovatel rovněž umožní audity činností zpracování, na které se vztahují tyto doložky, a podpoří je, a to v přiměřených intervalech nebo v případě, že se objeví náznaky nesouladu. Při rozhodování o přezkumu nebo auditu může správce zohlednit příslušná osvědčení, která zpracovatel vlastní.

(d) Správce se může rozhodnout, zda audit provede sám, nebo zda pověří nezávislého auditora. Audity mohou rovněž zahrnovat inspekce v prostorách nebo fyzických zařízeních zpracovatele a v případě potřeby se provádějí s přiměřeným oznámením.

(e) Strany na požádání zpřístupní informace uvedené v této doložce, včetně výsledků případných auditů, příslušnému dozorovému orgánu/orgánům.

7.7. Využití dílčích zpracovatelů

(a) Zpracovatel má obecné oprávnění správce k zapojení dílčích zpracovatelů z dohodnutého seznamu. Zpracovatel výslovně písemně informuje správce o všech zamýšlených změnách tohoto seznamu formou přidání nebo nahrazení dílčích zpracovatelů nejméně třicet (30) dnů předem, čímž poskytne správci dostatečný časový prostor k tomu, aby před zapojením dotčeného dílčího zpracovatele nebo zpracovatelů mohl vznést proti takovým změnám námitky. Zpracovatel poskytne správci informace nezbytné k tomu, aby správce mohl uplatnit právo vznést námitku.

(b) Pokud zpracovatel zapojí dílčího zpracovatele pro provádění konkrétních činností zpracování (jménem správce), učiní tak na základě smlouvy, která dílčímu zpracovateli ukládá v podstatě stejné povinnosti v oblasti ochrany údajů jako zpracovateli v souladu s těmito doložkami. Zpracovatel zajistí, aby dílčí zpracovatel plnil povinnosti, které se na něj vztahují podle těchto doložek a nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

(c) Na žádost správce poskytne zpracovatel správci kopii takové smlouvy s dílčím zpracovatelem a všech následných změn. Zpracovatel může text smlouvy před sdílením kopie upravit v rozsahu nezbytném pro ochranu obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů.

(d) Zpracovatel zůstává vůči správci plně odpovědný za plnění povinností dílčího zpracovatele v souladu s jeho smlouvou se zpracovatelem. Zpracovatel oznámí správci každé neplnění smluvních povinností ze strany dílčího zpracovatele.

(e) Je-li to možné, dohodne se zpracovatel s dílčím zpracovatelem na doložce o oprávněné třetí straně, podle níž má správce v případě, že zpracovatel fakticky zanikl, přestal právně existovat nebo se dostal do platební neschopnosti, právo ukončit smlouvu s dílčím zpracovatelem a dát dílčímu zpracovateli pokyn k vymazání nebo vrácení osobních údajů.

7.7. Mezinárodní předávání

(a) Předávání údajů do třetí země nebo mezinárodní organizaci zpracovatelem se provádí pouze na základě zdokumentovaných pokynů správce nebo za účelem splnění konkrétního

požadavku podle práva Unie nebo členského státu, kterému zpracovatel podléhá, a probíhá v souladu s kapitolou V nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.

(b) Správce souhlasí s tím, že pokud zpracovatel zapojí dílčího zpracovatele v souladu s bodem 7.7 pro provádění konkrétních činností zpracování (jménem správce) a tyto činnosti zpracování zahrnují předávání osobních údajů ve smyslu kapitoly V nařízení (EU) 2016/679, mohou zpracovatel a dílčí zpracovatel zajistit soulad s kapitolou V nařízení (EU) 2016/679 použitím standardních smluvních doložek přijatých Komisí v souladu s čl. 46 odst. 2 nařízení (EU) 2016/679, pokud jsou splněny podmínky pro použití těchto standardních smluvních doložek.

Doložka 8

Pomoc poskytovaná správci

(a) V případě, že zpracovatel obdrží žádost subjektu údajů, odkáže subjekty údajů na správce. Na žádost sám neodpovídá, pokud mu k tomu správce nedal oprávnění.

(b) Zpracovatel je správci nápomocen při plnění jeho povinnosti reagovat na žádosti subjektů údajů o uplatnění jejich práv, a to s přihlédnutím k povaze zpracování. Při plnění svých povinností podle písmen a) a b) se zpracovatel řídí pokyny správce.

(c) Kromě povinnosti zpracovatele být nápomocen správci podle bodu 8 písm. b) je zpracovatel dále nápomocen správci při zajišťování souladu s následujícími povinnostmi, a to s přihlédnutím k povaze zpracování údajů a informacím, které má zpracovatel k dispozici:

(1) povinnost provést posouzení dopadu plánovaných operací zpracování na ochranu osobních údajů („posouzení vlivu na ochranu osobních údajů“), pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob,

(2) povinnost konzultovat před zpracováním s příslušným dozorovým úřadem/úřady, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že pokud by správce nepřijal opatření ke zmírnění rizika, zpracování by vedlo k vysokému riziku,

(3) povinnost zajistit přesnost a aktuálnost osobních údajů tím, že neprodleně informuje správce, pokud zjistí, že osobní údaje, které zpracovává, jsou nepřesné nebo zastaralé,

(4) povinnosti uvedené v čl. 32 nařízení (EU) 2016/679.

(d) Strany stanoví v příloze III vhodná technická a organizační opatření, kterými je zpracovatel povinen pomáhat správci při uplatňování tohoto článku, jakož i rozsah a míru požadované pomoci.

Doložka 9

Oznámení o porušení zabezpečení osobních údajů

V případě porušení zabezpečení osobních údajů zpracovatel spolupracuje se správcem a je mu nápomocen při plnění jeho povinností podle čl. 33 a 34 nařízení (EU) 2016/679 nebo případně podle čl. 34 a 35 nařízení (EU) 2018/1725, přičemž přihlédne k povaze zpracování a informacím, které má zpracovatel k dispozici.

9.1 Porušení zabezpečení osobních údajů týkající se údajů zpracovávaných správcem

V případě porušení zabezpečení osobních údajů, které se týká údajů zpracovávaných správcem, je zpracovatel správci nápomocen:

(a) při ohlášení porušení zabezpečení osobních údajů příslušnému dozorovému úřadu, případně bez zbytečného odkladu poté, co se o něm správce dozvěděl (pokud není pravděpodobné, že by porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob),

(b) při získávání následujících informací, které musí být podle čl. 33 odst. 3 nařízení (EU) 2016/679 uvedeny v oznámení správce a musí obsahovat alespoň:

(1) povahu osobních údajů, pokud možno včetně kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného počtu dotčených záznamů osobních údajů,

(2) pravděpodobné důsledky porušení zabezpečení osobních údajů,

(3) opatření, která správce přijal nebo navrhuje přijmout k řešení porušení zabezpečení osobních údajů, případně včetně opatření ke zmírnění jeho možných nepříznivých účinků.

Pokud není možné poskytnout všechny tyto informace najednou, musí první oznámení obsahovat informace, které jsou v té době k dispozici, a další informace musí být poskytnuty bez zbytečného odkladu, jakmile budou k dispozici.

(c) při plnění povinnosti podle čl. 34 nařízení (EU) 2016/679 bez zbytečného odkladu oznámit porušení zabezpečení osobních údajů subjektu údajů, pokud je pravděpodobné, že toto porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

9.2 Porušení zabezpečení osobních údajů týkající se údajů zpracovávaných zpracovatelem

V případě porušení zabezpečení osobních údajů, které se týká údajů zpracovávaných zpracovatelem, oznámí zpracovatel toto porušení správci bez zbytečného odkladu poté, co se o něm dozvěděl. Toto oznámení musí obsahovat alespoň:

(a) popis povahy porušení zabezpečení osobních údajů, pokud možno včetně kategorií a přibližného počtu dotčených subjektů údajů a záznamů osobních údajů,

(b) údaje o kontaktním místě, kde lze získat další informace týkající se porušení zabezpečení osobních údajů,

(c) jeho pravděpodobné důsledky a opatření přijatá nebo navrhovaná k řešení tohoto porušení, včetně zmírnění jeho možných nepříznivých účinků.

Pokud není možné poskytnout všechny tyto informace najednou, musí první oznámení obsahovat informace, které jsou v té době k dispozici, a další informace musí být poskytnuty bez zbytečného odkladu, jakmile budou k dispozici.

Strany stanoví v příloze III všechny další prvky, které zpracovatel poskytne v rámci pomoci správci při plnění jeho povinností podle čl. 33 a 34 nařízení (EU) 2016/679.

ČÁST III – ZÁVĚREČNÁ USTANOVENÍ

Doložka 10

Nedodržení doložek a ukončení smlouvy

(a) Aniž by tím byla dotčena ustanovení nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725, může správce v případě, že zpracovatel porušuje své povinnosti podle těchto doložek, dát zpracovateli pokyn k pozastavení zpracování osobních údajů, dokud zpracovatel nesplní tyto doložky nebo dokud nebude ukončena rámcová smlouva. Zpracovatel v případě, že z jakéhokoli důvodu není schopen tyto doložky dodržet, neprodleně informuje správce.

(b) Správce je oprávněn vypovědět rámcovou smlouvu v rozsahu, v jakém se týká zpracování osobních údajů v souladu s těmito doložkami, pokud:

(1) zpracování osobních údajů zpracovatelem bylo pozastaveno správcem podle písmene a) a pokud nedojde k obnovení souladu s těmito doložkami v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení,

(2) zpracovatel podstatně nebo trvale porušuje tyto doložky nebo své povinnosti podle nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725,

(3) zpracovatel nedodržuje závazné rozhodnutí příslušného soudu nebo příslušného dozorového úřadu, pokud jde o jeho povinnosti podle těchto doložek nebo nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

(c) Zpracovatel je oprávněn ukončit rámcovou smlouvu v rozsahu, v jakém se týká zpracování osobních údajů podle těchto doložek, pokud správce poté, co jej zpracovatel informoval o tom, že jeho pokyny porušují platné právní požadavky v souladu s bodem 7.1 písm. b), trvá na dodržení těchto pokynů.

(d) Po ukončení rámcové smlouvy zpracovatel podle volby správce vymaže všechny osobní údaje zpracovávané jménem správce a potvrdí správci, že tak učinil, nebo vrátí všechny osobní údaje správci a vymaže existující kopie, pokud právo Unie nebo členského státu nevyžaduje uchovávání osobních údajů. Pokud správce nepožádá o vrácení všech osobních údajů zpracovávaných jménem správce do třiceti (30) dnů od ukončení rámcové smlouvy, je zpracovatel oprávněn podle vlastního uvážení osobní údaje vymazat. Dokud nejsou údaje vymazány nebo vráceny, musí zpracovatel i nadále zajišťovat dodržování těchto doložek.

PŘÍLOHA I SEZNAM STRAN

Správce (správci):

1. Klient (jak je uvedeno v rámcové smlouvě nebo objednávkovém formuláři)

Zpracovatel(é):

1. Glooko AB

PŘÍLOHA II: POPIS ZPRACOVÁNÍ

Kategorie subjektů údajů, jejichž osobní údaje jsou zpracovávány
- Autorizovaní uživatelé
- Pacienti

Kategorie zpracovávaných osobních údajů
U autorizovaných uživatelů
- Všeobecné informace (jméno)
- Kontaktní informace (e-mailová adresa, telefonní číslo)
- Informace o používání (uživatelské jméno, heslo, přístupová práva, protokoly auditu)

U pacientů
- Všeobecné informace (jméno, datum narození, pohlaví)
- Kontaktní informace (poštovní adresa, e-mailová adresa, telefonní číslo)
- Informace o používání (uživatelské jméno, heslo)
- Informace o zdravotním stavu (typ diabetu, rok diagnózy diabetu, odhadovaný porod, cílové rozmezí, hmotnost, výška, léčba)
- Informace o zařízení (sériové číslo inzulinové pumpy, glukometru a inzulinového pera, dávky, sacharidy, nastavení, alarmy)

Zpracovávané citlivé údaje (je-li to relevantní) a uplatňovaná omezení nebo ochranná opatření, která plně zohledňují povahu údajů a související rizika, jako je například přísné omezení účelu, omezení přístupu (včetně přístupu pouze pro zaměstnance, kteří absolvovali specializované školení), vedení záznamů o přístupu k údajům, omezení dalšího předávání nebo dodatečná bezpečnostní opatření.
- Údaje o zdravotním stavu

Informace o provedených zárukách viz příloha III

Povaha zpracování

Shromažďování, analýza, vizualizace a jiné zpracování osobních údajů v souladu s rámcovou smlouvou.

Účel(y), pro který(é) jsou osobní údaje jménem správce zpracovávány
Umožnění správci a jeho oprávněným uživatelům používat software a dodané produkty v souladu s rámcovou smlouvou.

Doba trvání zpracování

Po dobu poskytování softwaru a dodaných produktů podle rámcové smlouvy, mimo jiné včetně poskytování servisu a technické podpory.

U zpracování (dílčími) zpracovateli uveďte také předmět, povahu a dobu trvání zpracování
Viz příloha IV

Pokyny podle bodu 7.8 a) doložek týkající se mezinárodního předávání
Správce souhlasí s tím, že zpracovatel může předávat osobní údaje příjemcům nacházejícím se ve třetích zemích za předpokladu, že takové předání podléhá vhodným zárukám uznaným podle platných zákonů o ochraně údajů nebo je jinak v souladu s platnými zákony o ochraně údajů. Zpracovatel může předávat osobní údaje své přidružené společnosti a dílčímu zpracovateli, společnosti Glooko, Inc. ve Spojených státech amerických jako údaje nezbytné pro technickou podporu a splnění zákonných požadavků.

PŘÍLOHA III TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, VČETNĚ TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ PRO ZAJIŠTĚNÍ BEZPEČNOSTI ÚDAJŮ

1. Účel. Tato příloha popisuje bezpečnostní program společnosti Glooko, bezpečnostní certifikace a technická a organizační opatření na ochranu (a) osobních údajů zpracovávaných zpracovatelem jménem správce před neoprávněným použitím, přístupem, zveřejněním nebo krádeží a (b) softwaru. Vzhledem k tomu, že se bezpečnostní hrozby mění a vyvíjejí, společnost Glooko neustále aktualizuje svůj bezpečnostní program a strategii, aby pomohla chránit osobní údaje a software. Společnost Glooko si proto vyhrazuje právo tuto přílohu čas od času aktualizovat, avšak za podmínky, že jakákoli aktualizace podstatně nesníží celkovou ochranu stanovenou v této příloze.

2. Organizace a program zabezpečení. Společnost Glooko udržuje program zabezpečení založený na hodnocení rizik. Rámec programu zabezpečení společnosti Glooko zahrnuje administrativní, organizační, technická a fyzická ochranná opatření přiměřeně navržená k ochraně softwaru a důvěrnosti, integrity a dostupnosti osobních údajů. Program zabezpečení společnosti Glooko má za cíl být přiměřený povaze softwaru a velikosti a složitosti obchodních operací společnosti Glooko. Společnost Glooko má samostatný a specializovaný tým informační bezpečnosti, který řídí program zabezpečení společnosti Glooko. Tento tým usnadňuje a podporuje nezávislé audity a hodnocení prováděné třetími stranami. Rámec zabezpečení společnosti Glooko zahrnuje programy týkající se následujících oblastí: Zásady a postupy, správa aktiv, správa přístupu, kryptografie, fyzická bezpečnost, provozní bezpečnost, bezpečnost komunikace, bezpečnost kontinuity provozu, bezpečnost lidí, bezpečnost produktů, bezpečnost cloudové a síťové infrastruktury, dodržování bezpečnostních předpisů, bezpečnost třetích stran, správa chyb zabezpečení a monitorování bezpečnosti a reakce na incidenty. Zabezpečení je řízeno na nejvyšších úrovních společnosti a bezpečnostní ředitel společnosti Glooko se pravidelně setkává s výkonným vedením, aby diskutoval o problémech a koordinoval celopodnikové bezpečnostní iniciativy. Zásady a standardy informační bezpečnosti jsou nejméně jednou ročně přezkoumávány a schvalovány vedením a jsou k dispozici všem zaměstnancům společnosti Glooko.

3. Důvěrnost. Společnost Glooko má zavedeny kontrolní mechanismy k zachování důvěrnosti osobních údajů v souladu s rámcovou smlouvou. Všichni zaměstnanci a smluvní pracovníci společnosti Glooko jsou vázáni interními zásadami společnosti Glooko týkajícími se zachování důvěrnosti osobních údajů a jsou smluvně zavázáni tyto povinnosti dodržovat.

4. Bezpečnost osob

    a. Prověřování zaměstnanců. Společnost Glooko provádí prověrky všech nových zaměstnanců při jejich přijetí v souladu s platnými místními zákony. Společnost Glooko v současné době ověřuje vzdělání a předchozí zaměstnání nového zaměstnance a provádí kontrolu referencí. Tam, kde to povolují platné právní předpisy, může společnost Glooko provádět také trestní, kreditní, imigrační a bezpečnostní kontroly v závislosti na povaze a rozsahu funkce nového zaměstnance.

    b. Školení zaměstnanců. Alespoň jednou (1) ročně musí všichni zaměstnanci společnosti Glooko absolvovat školení o bezpečnosti a ochraně osobních údajů, které se týká bezpečnostních zásad společnosti Glooko, osvědčených bezpečnostních postupů a zásad ochrany osobních údajů. Zaměstnanci, kteří jsou na dovolené, mohou mít na absolvování tohoto ročního školení více času. Specializovaný bezpečnostní tým společnosti Glooko také realizuje kampaně na zvýšení povědomí o phishingu a informuje zaměstnance o nových hrozbách.

5. Řízení prodejců z řad třetích stran

    a. Hodnocení prodejců. Společnost Glooko může k poskytování softwaru využívat dodavatele z řad třetích stran. Společnost Glooko provádí hodnocení potenciálních dodavatelů na základě bezpečnostních rizik předtím, než s nimi začne spolupracovat, aby ověřila, zda splňují její bezpečnostní požadavky. Společnost Glooko pravidelně přezkoumává každého dodavatele s ohledem na bezpečnostní standardy a standardy kontinuity podnikání společnosti Glooko, včetně typu přístupu a klasifikace dat, ke kterým se přistupuje (pokud existují), kontrolních mechanismů nezbytných k ochraně údajů a právních/regulačních požadavků. Společnost Glooko zajišťuje, aby byly osobní údaje po ukončení vztahu s dodavatelem vráceny a/nebo vymazány.

    b. Smlouvy s prodejci. Společnost Glooko uzavírá se všemi svými prodejci písemné dohody, které obsahují závazky týkající se důvěrnosti, ochrany soukromí a bezpečnosti, které zajišťují odpovídající úroveň ochrany osobních údajů, které tito dodavatelé mohou zpracovávat.

6. Architektura, brány firewall a segregace dat. Veškerý síťový přístup mezi produkčními hostiteli je omezen pomocí firewallů, které umožňují interakci v produkční síti pouze autorizovaným službám. Firewally se používají ke správě síťové segregace mezi různými bezpečnostními zónami v produkčním a podnikovém prostředí. Společnost Glooko své databáze logicky odděluje. Rozhraní API společnosti Glooko je navrženo a vytvořeno tak, aby identifikovalo a umožňovalo přístup pouze příslušným odesílatelům a od nich. Tyto kontroly zabraňují zákazníkům v přístupu k údajům jiných zákazníků.

7. Fyzické zabezpečení. Datová centra, která jsou hostiteli softwaru, jsou přísně kontrolována po obvodu i na vstupech do budov profesionálními bezpečnostními pracovníky, kteří využívají kamerový systém, systémy detekce vniknutí a další elektronické prostředky. Pro případ výpadku elektrického proudu jsou k dispozici nepřerušitelné zdroje napájení a generátory na místě. Sídlo společnosti Glooko a kancelářské prostory jsou navíc vybaveny programem fyzického zabezpečení, který řídí návštěvníky, vstupy do budov a celkové zabezpečení kanceláří.

8. Zabezpečení již od návrhu. Společnost Glooko se při navrhování softwaru řídí zásadami zabezpečení již od návrhu. Společnost Glooko také používá standard Glooko Software Development Lifecycle (SDLC) k provádění mnoha činností souvisejících se zabezpečením softwaru v různých fázích životního cyklu tvorby produktu od shromažďování požadavků a návrhu produktu až po jeho nasazení.

9. Kontroly přístupu

    a. Poskytování přístupu. Aby se minimalizovalo riziko odhalení údajů, řídí se společnost Glooko při poskytování přístupu k systému zásadami nejmenších oprávnění prostřednictvím modelu řízení přístupu založeného na týmu. Zaměstnanci společnosti Glooko jsou oprávněni přistupovat k osobním údajům na základě své pracovní funkce, role a odpovědnosti a tento přístup vyžaduje souhlas nadřízeného zaměstnance. Přístup zaměstnance k osobním údajům je po ukončení pracovního poměru zrušen. Před udělením přístupu k produkčnímu prostředí musí být přístup schválen vedením a technik musí pro tento přístup absolvovat interní školení včetně školení o systémech příslušného týmu. Společnost Glooko zaznamenává vysoce rizikové akce a změny v produkčním prostředí. Společnost Glooko využívá automatizaci k identifikaci odchylek od interních technických standardů, které by mohly indikovat anomální/neautorizovanou aktivitu, aby bylo možné vyvolat upozornění během několika minut po změně konfigurace.

    b. Kontroly hesla. Když se autorizovaný uživatel přihlásí ke svému účtu, společnost Glooko jeho přihlašovací údaje před uložením zahashuje. Klienti mohou také

požadovat, aby jejich oprávnění uživatelé přidali ke svému účtu další úroveň zabezpečení pomocí dvoufaktorového ověřování (2FA).

10. Řízení změn. Společnost Glooko má formální proces řízení změn, kterým se řídí při správě změn produkčního prostředí softwaru, včetně změn základního softwaru, aplikací a systémů. Každá změna je před nasazením do produkčního prostředí softwaru pečlivě zkontrolována a vyhodnocena v testovacím prostředí. Všechny změny, včetně vyhodnocení změn v testovacím prostředí, jsou zdokumentovány pomocí formálního, auditovatelného systému záznamů. Nasazení rizikových změn musí schválit příslušné zainteresované strany organizace. Plány a postupy jsou zavedeny také pro případ, že je třeba nasazenou změnu vrátit zpět, aby byla zachována bezpečnost softwaru.

11. Šifrování. V případě softwaru jsou (a) databáze, v nichž jsou uloženy osobní údaje, šifrovány pomocí standardu Advanced Encryption Standard, a (b) osobní údaje jsou při přenosu mezi softwarovou aplikací klienta a softwarem šifrovány pomocí protokolu TLS v1.2.

12. Správa zranitelných míst. Společnost Glooko udržuje kontroly a zásady pro zmírnění rizika zranitelných míst, aby vyvážila riziko a obchodní/provozní požadavky. Společnost Glooko používá nástroj třetí strany, který pravidelně provádí kontrolu zranitelných míst cloudové infrastruktury a firemních systémů společnosti Glooko.

13. Penetrační testy. Společnost Glooko provádí penetrační testy a zapojuje nezávislé subjekty z řad třetích stran, které provádějí penetrační testy na úrovni aplikací. Zjištěné bezpečnostní hrozby a chyby zabezpečení jsou prioritizovány, tříděny a odstraňovány.

14. Řízení bezpečnostních incidentů. Společnost Glooko udržuje zásady řízení bezpečnostních incidentů. Tým společnosti Glooko pro reakci na bezpečnostní incidenty (T-SIRT) vyhodnocuje všechny relevantní bezpečnostní hrozby a chyby zabezpečení a stanovuje vhodná nápravná a zmírňující opatření. Společnost Glooko uchovává příslušné bezpečnostní protokoly.

15. Odolnost a kontinuita softwaru. Software využívá různé nástroje a mechanismy k dosažení vysoké dostupnosti a odolnosti. Pokud jde o software, infrastruktura společnosti Glooko zahrnuje několik zón dostupnosti nezávislých na poruchách v zeměpisných oblastech, které jsou od sebe fyzicky odděleny. Společnost Glooko také využívá specializované nástroje, které monitorují výkon serverů, data a kapacitu provozního zatížení v rámci každé zóny dostupnosti a kolokačního datového centra. Pokud je na serveru v zóně dostupnosti nebo v kolokačním datovém centru zjištěn neoptimální výkon serveru nebo přetížená kapacita, tyto specializované nástroje zvýší kapacitu nebo přesunou provoz, aby se snížil neoptimální výkon serveru nebo přetížení kapacity. Společnost Glooko je v případě neoptimálního výkonu serveru nebo přetížení kapacity také okamžitě informována.

16. Zálohy a obnova. Společnost Glooko provádí pravidelné zálohování osobních údajů. Zálohované osobní údaje jsou uchovávány redundantně ve více zónách dostupnosti a šifrovány při přenosu i v klidovém stavu pomocí pokročilých standardů šifrování.

PŘÍLOHA IV: SEZNAM DÍLČÍCH ZPRACOVATELŮ

Správce povolil používání těchto dílčích zpracovatelů:

1. Jméno: Amazon Web Services EMEA SARL
Adresa: 38 Avenue John F. Kennedy, L-1855, Lucembursko

Popis zpracování (včetně jasného vymezení odpovědností v případě, že je oprávněno několik dílčích zpracovatelů): Poskytovatel cloudových služeb

2. Jméno: Cegedim SA
Adresa: 137 rue d'Aguesseau, 92100 Boulogne-Billancourt, Francie

Popis zpracování (včetně jasného vymezení odpovědností v případě, že je oprávněno několik dílčích zpracovatelů): Poskytovatel cloudových služeb (lze použít pro klienty sídlící ve Francii)

3. Jméno: Pictime Groupe
Adresa: Campus du Digital 61, rue de l'Harmonie - 59262 Sainghin-en-Mélantois, Francie

Popis zpracování (včetně jasného vymezení odpovědností v případě, že je oprávněno několik dílčích zpracovatelů): Certifikovaný hostitel zdravotnických dat (lze použít pro klienty sídlící ve Francii a Německu)

4 Jméno: Glooko, Inc.
Adresa: 411 High Street, Palo Alto, Kalifornie, 94301

Popis zpracování (včetně jasného vymezení odpovědností v případě, že je povoleno několik dílčích zpracovatelů): technická podpora a regulační požadavky.