BILAG 2

GLOOKOS STANDARDKONTRAKTSKLAUSULER

AVSNITT I

Klausul 1

Formål og omfang

(a) Formålet med disse standardkontraktsklausulene (klausulene) er å sikre samsvar med artikkel 28(3) og (4) i Europaparlamentets og Europarådets forordning (EU) 2016/679 av 27. april 2016 om beskyttelse av fysiske personer med hensyn til behandling av personopplysninger og om fri flyt av slike opplysninger.

(b) De behandlingsansvarlige og databehandlerne oppført i Vedlegg I har godtatt disse klausulene for å sikre samsvar med artikkel 28(3) og (4) i forordning (EU) 2016/679 og/eller artikkel 29(3) og (4) i forordning (EU) 2018/1725.

(c) Disse klausulene gjelder for behandling av personopplysninger som spesifisert i Vedlegg II.

(d) Vedlegg I til IV er en integrert del av klausulene.

(e) Disse klausulene berører ikke forpliktelser som behandlingsansvarlig er underlagt i henhold til forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725.

(f) Disse klausulene sikrer ikke i seg selv overholdelse av forpliktelser knyttet til internasjonale overføringer i samsvar med kapittel V i forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725.

Klausul 2

Klausulenes ufravikelighet

(a) Partene forplikter seg til ikke å endre klausulene, bortsett fra tilføying av informasjon til vedleggene eller oppdatering av informasjon i dem.

(b) Dette hindrer ikke partene i å inkludere standardkontraktsklausulene fastsatt i disse klausulene i en bredere kontrakt, eller i å legge til andre klausuler eller tilleggsgarantier, forutsatt at de ikke direkte eller indirekte er i strid med klausulene eller forringer de grunnleggende rettighetene eller frihetene til registrerte.

Klausul 3

Tolkning

(a) Der det disse klausulene anvendes termer definert i henholdsvis forordning (EU) 2016/679 eller forordning (EU) 2018/1725, skal disse termene ha samme betydning som i den gitte forordningen.

(b) Disse klausulene skal leses og tolkes i lys av bestemmelsene i henholdsvis forordning (EU) 2016/679 eller forordning (EU) 2018/1725.

(c) Disse klausulene skal ikke tolkes på en måte som strider mot rettighetene og forpliktelsene fastsatt i forordning (EU) 2016/679 / forordning (EU) 2018/1725 eller på en måte som svekker de grunnleggende rettighetene eller frihetene til de registrerte.

Klausul 4

Hierarki

Ved en motsigelse mellom disse klausulene og bestemmelsene i relaterte avtaler mellom partene som eksisterer på tidspunktet disse klausulene godtas, eller inngås senere, skal disse klausulene ha forrang.

Klausul 5 – Valgfritt

Inntredelsesklausul

(a) Ved samtykke fra alle partene kan enhver enhet som ikke er en part i disse klausulene, når som helst slutte seg til disse klausulene som behandlingsansvarlig eller databehandler ved å fylle ut vedleggene og signere Vedlegg I.

(b) Når vedleggene i (a) er fylt ut og signert, skal den tilsluttende enheten behandles som en part i disse klausulene og ha rettighetene og forpliktelsene til en behandlingsansvarlig eller en databehandler, i samsvar med betegnelsen i Vedlegg I.

(c) Den tilsluttende enheten skal ikke ha noen rettigheter eller forpliktelser som følge av disse klausulene fra perioden før enheten ble en part.

AVSNITT II – PARTENES FORPLIKTELSER

Klausul 6

Beskrivelse av behandling

Detaljene i behandlingsoperasjonene, særlig kategoriene av personopplysninger og formålene med behandlingen som personopplysningene behandles for på vegne av den behandlingsansvarlige, er spesifisert i Vedlegg II.

Klausul 7

Partenes forpliktelser

7.1. Instruksjoner

(a) Databehandleren skal kun behandle personopplysninger etter dokumenterte instruksjoner fra den behandlingsansvarlige, med mindre det er påkrevd i henhold til lovgivningen i unions- eller medlemslandet som databehandleren er underlagt. I slike tilfeller skal databehandleren informere den behandlingsansvarlige om det rettslige kravet før behandlingen, med mindre loven forbyr dette på grunn av viktige allmenne interesser. Påfølgende instruksjoner kan også gis av den behandlingsansvarlige så lenge behandlingen av personopplysninger varer. Disse instruksjonene skal alltid dokumenteres.

(b) Databehandleren skal umiddelbart informere den behandlingsansvarlige dersom instruksjoner gitt av den behandlingsansvarlige bryter, etter databehandlerens mening, med forordning (EU) 2016/679 / forordning (EU) 2018/1725 eller gjeldende databeskyttelses-bestemmelser i unions- eller medlemslandet.

7.2. Formålsbegrensning

Databehandleren skal behandle personopplysningene kun for det spesifikke formålet /de spesifikke formålene med behandlingen, som angitt i Vedlegg II, med mindre den mottar ytterligere instruksjoner fra den behandlingsansvarlige.

7.3. Varighet av behandlingen av personopplysninger

Behandlingen utført av databehandleren skal bare finne sted så lenge det er angitt i Vedlegg II.

7.4. Behandlingssikkerhet

(a) Databehandleren skal minst iverksette de tekniske og organisatoriske tiltakene angitt i Vedlegg III for å ivareta sikkerheten til personopplysningene. Dette inkluderer beskyttelse av opplysningene mot brudd på sikkerheten som fører til utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert avsløring eller tilgang til dataene (personopplysningsbrudd). Ved vurderingen av det hensiktsmessige sikkerhetsnivået skal partene ta behørig hensyn til

dagens løsninger, kostnadene ved implementering, arten, omfanget, konteksten og formålene med behandlingen samt de involverte risikoene for de registrerte.

(b) Databehandleren skal gi tilgang til personopplysningene som behandles, til medlemmer av dets personell kun i den grad det er strengt nødvendig for å implementere, administrere og overvåke kontrakten. Databehandleren skal sikre at personer som er autorisert til å behandle de mottatte personopplysningene, har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt.

7.5. Sensitive opplysninger

Dersom behandlingen involverer personopplysninger som avslører rase eller etnisk opprinnelse, politiske syn, religiøse eller filosofiske overbevisninger, eller fagforeningsmedlemskap, genetiske opplysninger eller biometriske opplysninger der formålet er unik identifisering av en fysisk person, opplysninger om helse eller en persons sexliv eller seksuelle orientering, eller opplysninger knyttet til straffedommer og lovbrudd («sensitive opplysninger»), skal databehandleren implementere spesifikke restriksjoner og/eller ytterligere sikkerhetstiltak.

7.6 Dokumentasjon og overholdelse

(a) Partene skal kunne demonstrere overholdelse av disse klausulene.

(b) Databehandleren skal raskt og adekvat håndtere henvendelser fra den behandlingsansvarlige om behandling av opplysninger i samsvar med disse klausulene.

(c) Databehandleren skal gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å demonstrere overholdelse av forpliktelsene som er fastsatt i disse klausulene og stammer direkte fra forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725. På den behandlingsansvarliges anmodning skal databehandleren også tillate og bidra til revisjoner av behandlingsaktivitetene som omfattes av disse klausulene, med rimelige intervaller eller dersom det er indikasjoner på manglende samsvar. Ved avgjørelse om gjennomgang eller revisjon kan den behandlingsansvarlige ta hensyn til relevante sertifiseringer som behandles av databehandleren.

(d) Den behandlingsansvarlige kan velge å utføre revisjonen alene eller gi en uavhengig revisor fullmakt. Revisjoner kan også omfatte inspeksjoner i databehandlerens lokaler eller fysiske fasiliteter og skal utføres der det er hensiktsmessig, med rimelig varsel.

(e) Partene skal gjøre informasjonen nevnt i denne klausulen, inkludert resultatene av eventuelle revisjoner, tilgjengelig for de(n) kompetente tilsynsmyndigheten(e) på forespørsel.

7.7. Bruk av underdatabehandlere

(a) Databehandleren har generell fullmakt fra den behandlingsansvarlige for engasjement av underdatabehandlere fra en avtalt liste. Databehandleren skal spesifikt informere den behandlingsansvarlige skriftlig om eventuelle tiltenkte endringer av denne listen gjennom tillegg eller utskifting av underdatabehandlere minst tretti (30) dager i forveien, og dermed gi den behandlingsansvarlige tilstrekkelig tid til å kunne motsette seg slike endringer før engasjement av den eller de aktuelle underdatabehandlerne. Databehandleren skal gi den behandlingsansvarlige informasjonen som er nødvendig for at den behandlingsansvarlige skal kunne utøve innsigelsesretten.

(b) Når databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter (på vegne av den behandlingsansvarlige), skal den gjøre det i form av en kontrakt som i hovedsak pålegger underdatabehandleren de samme databeskyttelsesforpliktelsene som de som er pålagt databehandleren i henhold til disse klausulene. Databehandleren skal sikre at underdatabehandleren overholder forpliktelsene som databehandleren er underlagt i henhold til disse klausulene samt forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725.

(c) På anmodning fra behandlingsansvarlig skal databehandleren gi behandlingsansvarlig en kopi av en slik underdatabehandleravtale og eventuelle senere endringer. I den grad det er nødvendig for å beskytte forretningshemmeligheter eller annen konfidensiell informasjon, inkludert personopplysninger, kan databehandleren redigere avtaleteksten før kopien deles.

(d) Databehandleren skal forbli fullt ansvarlig overfor behandlingsansvarlig for oppfyllelsen av underdatabehandlerens forpliktelser i henhold til kontrakten med databehandleren. Databehandleren skal varsle behandlingsansvarlig om underdatabehandlerens manglende oppfyllelse av kontraktsforpliktelsene.

(e) Der det er mulig, skal databehandleren avtale en tredjepartsbegunstigelsesklausul med underdatabehandleren hvor behandlingsansvarlig – i tilfeller der databehandleren faktisk har forsvunnet, opphørt å eksistere ifølge loven eller har blitt insolvent – skal ha rett til å si opp underdatabehandlerkontrakten og til å instruere underdatabehandleren om å slette eller returnere personopplysningene.

7.8. Internasjonal overføring

(a) Enhver overføring av opplysninger til et tredjeland eller en internasjonal organisasjon utført av databehandleren skal kun gjøres på grunnlag av dokumenterte instruksjoner fra behandlingsansvarlig eller for å oppfylle et spesifikt krav i henhold til lovgivningen i unions- eller medlemslandet som databehandleren er underlagt, og skal skje i samsvar med kapittel V i forordning (EU) 2016/679 eller forordning (EU) 2018/1725.

(b) Behandlingsansvarlig samtykker i følgende: I tilfeller der databehandleren engasjerer en underdatabehandler i samsvar med klausul 7.7. for å utføre spesifikke behandlingsaktiviteter (på vegne av den behandlingsansvarlige), og disse behandlingsaktivitetene innebærer en overføring av personopplysninger i henhold til kapittel V i forordning (EU) 2016/679, kan databehandleren og underdatabehandleren sikre samsvar med kapittel V i forordning (EU) 2016/679 ved å bruke standardkontraktsklausuler vedtatt av kommisjonen i samsvar med artikkel 46(2) i forordning (EU) 2016/679, forutsatt at betingelser for bruk av disse standardkontraktsklausulene er oppfylt.

Klausul 8

Assistanse til behandlingsansvarlig

(a) I tilfeller der databehandleren mottar en forespørsel fra registrerte, skal databehandleren henvise registrerte til å kontakte behandlingsansvarlig. Den skal ikke svare på selve forespørselen, med mindre behandlingsansvarlig har gitt tillatelse til det.

(b) Databehandleren skal bistå behandlingsansvarlig med å oppfylle dens forpliktelser til å svare på de registrertes forespørsler om å utøve deres rettigheter, under hensyntagen til behandlingens art. Ved oppfyllelse av sine forpliktelser i henhold til (a) og (b) skal databehandleren følge instruksjoner fra behandlingsansvarlig.

(c) I tillegg til databehandlerens plikt til å bistå behandlingsansvarlig i henhold til punkt 8(b), skal databehandleren videre bistå behandlingsansvarlig med å sikre overholdelse av følgende forpliktelser, under hensyntagen til databehandlingens art og informasjonen som er tilgjengelig for databehandleren:

(1) forpliktelsen til å foreta en vurdering av virkningen av de planlagte behandlingsoperasjonene på beskyttelsen av personopplysninger (en «konsekvensvurdering av databeskyttelse»), der en type databehandling sannsynligvis vil resultere i høy risiko for rettighetene og frihetene til naturlige personer;

(2) forpliktelsen til å konsultere de(n) kompetente tilsynsmyndigheten(e) før databehandling der en konsekvensvurdering av databeskyttelse indikerer at behandlingen vil resultere i høy risiko hvis behandlingsansvarlig ikke implementerer tiltak for å redusere risikoen;

(3) forpliktelsen til å sikre at personopplysninger er nøyaktige og oppdatert, ved å informere behandlingsansvarlig uten forsinkelser dersom databehandleren blir klar over at personopplysningene den behandler, er unøyaktige eller har blitt utdatert;

(4) forpliktelsene i artikkel 32, forordning (EU) 2016/679.

(d) Partene skal i Vedlegg III angi passende tekniske og organisatoriske tiltak som databehandleren må assistere behandlingsansvarlig med ved håndhevelse av denne klausulen, samt omfanget og graden av assistansen som kreves.

Klausul 9

Varsling om personopplysningsbrudd

Ved et personopplysningsbrudd skal databehandleren samarbeide med og bistå behandlingsansvarlig for at behandlingsansvarlig skal overholde sine forpliktelser i henhold til artikkel 33 og 34 i forordning (EU) 2016/679 eller under artikkel 34 og 35 i forordning (EU) 2018/1725, der det er aktuelt, under hensyntagen til databehandlingens art og informasjonen som er tilgjengelig for databehandleren.

9.1 Opplysningsbrudd relatert til opplysninger behandlet av behandlingsansvarlig

Ved personopplysningsbrudd relatert til opplysninger behandlet av behandlingsansvarlig skal databehandleren bistå behandlingsansvarlig:

(a) ved å varsle om personopplysningsbruddet til de(n) vedkommende tilsynsmyndigheten(e) uten unødig forsinkelse etter at behandlingsansvarlig har fått kjennskap til det, der det er relevant (med mindre det er usannsynlig at personopplysningsbruddet vil resultere i en risiko for rettighetene og frihetene til fysiske personer);

(b) ved å innhente følgende opplysninger som, i henhold til artikkel 33(3) i forordning (EU) 2016/679, skal oppgis i den behandlingsansvarliges varsling, og som minst skal omfatte:

(1) arten av personopplysningene, inkludert om mulig kategoriene av, og omtrentlig antall berørte registrerte samt kategoriene av, og omtrentlig antall berørte personopplysningsoppføringer;

(2) de sannsynlige konsekvensene av personopplysningsbruddet;

(3) tiltakene som er implementert eller foreslått implementert av den behandlingsansvarlige for å håndtere personopplysningsbruddet, inkludert – der det er hensiktsmessig – tiltak for å redusere de mulige skadevirkningene.

Der, og i den grad det ikke er mulig å oppgi all denne informasjonen samtidig, skal det innledende varselet inneholde informasjonen som er tilgjengelig på det gitte tidspunktet. Ytterligere informasjon skal oppgis etter som den blir tilgjengelig, uten unødig forsinkelse.

(c) ved å overholde, i henhold til artikkel 34 i forordning (EU) 2016/679, forpliktelsen til uten unødig forsinkelse å formidle personopplysningsbruddet til den registrerte, når personopplysningsbruddet sannsynligvis vil resultere i høy risiko for rettighetene og frihetene til fysiske personer.

9.2 Opplysningsbrudd relatert til opplysninger behandlet av databehandleren

Ved personopplysningsbrudd relatert til opplysninger behandlet av databehandleren, skal databehandleren uten unødig forsinkelse varsle den behandlingsansvarlige etter at databehandleren har fått kjennskap til bruddet. Et slikt varsel skal minst inneholde:

(a) en beskrivelse av arten av bruddet (inkludert om mulig kategoriene av, samt omtrentlig antall berørte registrerte og dataoppføringer);

(b) detaljert informasjon om et kontaktpunkt der mer informasjon om personopplysningsbruddet kan fås;

(c) dets sannsynlige konsekvenser og tiltakene som er implementert eller foreslått implementert for å håndtere bruddet, inkludert for å redusere de mulige negative effektene.

Der, og i den grad det ikke er mulig å oppgi all denne informasjonen samtidig, skal det innledende varselet inneholde informasjonen som er tilgjengelig på det gitte tidspunktet. Ytterligere informasjon skal oppgis etter som den blir tilgjengelig, uten unødig forsinkelse.
Partene skal i Vedlegg III angi alle andre elementer som skal oppgis av databehandleren når den bistår den behandlingsansvarlige med å overholde den behandlingsansvarliges forpliktelser i henhold til artikkel 33 og 34 i forordning (EU) 2016/679.

AVSNITT III – SLUTTBESTEMMELSER

Klausul 10

Manglende overholdelse av klausulene og oppsigelse

(a) Følgende gjelder uten at det berører eventuelle bestemmelser i forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725: I tilfeller der databehandleren bryter sine forpliktelser i henhold til disse klausulene, kan den behandlingsansvarlige instruere databehandleren om å suspendere behandlingen av personopplysninger inntil sistnevnte overholder disse klausulene eller hovedavtalen sies opp. Databehandleren skal umiddelbart informere den behandlingsansvarlige i tilfeller der den ikke er i stand til å overholde disse klausulene, uavhengig av årsak.

(b) Den behandlingsansvarlige skal ha rett til å si opp hovedavtalen i den grad den gjelder behandling av personopplysninger i samsvar med disse klausulene, dersom:

(1) databehandlerens behandling av personopplysninger har blitt utsatt av behandlingsansvarlig i henhold til punkt (a), og dersom samsvar med disse klausulene ikke gjenopprettes innen rimelig tid og i alle fall innen én måned etter suspendering;

(2) databehandleren begår et vesentlig eller vedvarende brudd på disse klausulene eller sine forpliktelser i henhold til forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725;

(3) databehandleren unnlater å overholde en bindende avgjørelse fra en kompetent domstol eller de(n) kompetente tilsynsmyndigheten(e) angående dens forpliktelser i henhold til disse klausulene eller forordning (EU) 2016/679 og/eller forordning (EU) 2018/1725.

(c) Databehandleren har rett til å si opp hovedavtalen i den grad den gjelder behandling av personopplysninger i henhold til disse klausulene, i tilfeller der den behandlingsansvarlige insisterer på å overholde instruksjonene etter å ha blitt informert om at dens instruksjoner overtrer gjeldende lovkrav i henhold til punkt 7.1 (b).

(d) Etter oppsigelse av hovedavtalen skal databehandleren, etter den behandlingsansvarliges valg, slette alle personopplysninger behandlet på vegne av behandlingsansvarlig og bekrefte overfor behandlingsansvarlig at den har gjort det, eller returnere alle personopplysninger til behandlingsansvarlig og slette eksisterende kopier, med mindre lovgivningen i unions- eller medlemslandet krever lagring av personopplysningene. Dersom den behandlingsansvarlige ikke har bedt om å få alle personopplysninger behandlet på vegne av behandlingsansvarlig returnert innen tretti (30) dager etter oppsigelse av hovedavtalen, skal databehandleren ha rett til å slette personopplysningene etter eget skjønn. Inntil dataene slettes eller returneres, skal databehandleren fortsette å sikre overholdelse av disse klausulene.

VEDLEGG I LISTE OVER PARTER

Behandlingsansvarlig(e):

1. Kunden (som identifisert i hovedavtalen eller ordreskjemaet)

Databehandler(e):

1. Glooko AB

VEDLEGG II: BESKRIVELSE AV DATABEHANDLINGEN

Kategorier av registrerte hvis personopplysninger behandles
– Autoriserte brukere
– Pasienter

Kategorier av personopplysninger som behandles
For autoriserte brukere
– Generell informasjon (navn)
– Kontaktinformasjon (e-postadresse, telefonnummer)
– Bruksinformasjon (brukernavn, passord, tilgangsrettigheter, revisjonslogger)

For pasienter
– Generell informasjon (navn, fødselsdato, kjønn)
– Kontaktinformasjon (postadresse, e-postadresse, telefonnummer)
– Bruksinformasjon (brukernavn, passord)
– Helseopplysninger (diabetestype, år for diabetesdiagnoser, estimert fødsel, målområde, vekt, høyde, behandlinger)
– Enhetsinformasjon (insulinpumpe, glukosemåler og insulinpennen(e)s serienummer/serienumre, doser, karbohydrater, innstillinger, alarmer)

De behandlede sensitive opplysningene (hvis aktuelt) og anvendte begrensninger eller sikkerhetstiltak som fullt ut tar hensyn til dataenes art og de involverte risikoene, for eksempel strenge formålsbegrensninger, tilgangsbegrensninger (inkludert tilgang kun for personell som har gjennomgått spesialistopplæring), føring av et register over tilgang til dataene, restriksjoner for videre overføringer eller ytterligere sikkerhetstiltak.
– Opplysninger om helse

Informasjon om implementerte sikkerhetstiltak finner du i Vedlegg III

Databehandlingens art

Innsamling, analyse, visualisering og annen behandling av personopplysningene i henhold til hovedavtalen.

Formål som personopplysningene behandles for på vegne av behandlingsansvarlig
Å gjøre det mulig for den behandlingsansvarlige og dens autoriserte brukere å bruke programvaren og andre leveranser i samsvar med hovedavtalen

Databehandlingens varighet

Så lenge programvaren og andre leveranser leveres i henhold til hovedavtalen, inkludert, men ikke begrenset til tjenestelevering og teknisk støtte.

For behandling utført av (under)databehandlere: spesifiser også emne, art og varighet av databehandlingen
Se Vedlegg IV

Instruksjoner under punkt 7.8 a) i klausulene om internasjonale overføringer
Den behandlingsansvarlige godtar at databehandleren kan overføre personopplysninger til mottakere som befinner seg i et tredjeland, forutsatt at slik overføring er underlagt passende sikkerhetstiltak anerkjent under gjeldende databeskyttelseslover eller på annen måte overholder gjeldende databeskyttelseslover. Databehandleren kan overføre personopplysninger til sitt tilknyttede selskap og sin underdatabehandler, Glooko, Inc. i USA, etter behov for teknisk støtte og i henhold til regulatoriske krav.

VEDLEGG III TEKNISKE OG ORGANISATORISKE TILTAK, INKLUDERT TEKNISKE OG ORGANISATORISKE TILTAK FOR Å SIKRE SIKKERHETEN TIL OPPLYSNINGENE

1. Formål. Dette vedlegget beskriver Glookos sikkerhetsprogram, sikkerhetssertifiseringer samt tekniske og organisatoriske tiltak for å beskytte (a) personopplysninger som behandles av databehandleren på vegne av behandlingsansvarlig, fra uautorisert bruk, tilgang, avsløring eller tyveri og (b) programvaren. Etter som sikkerhetstrusler endrer og utvikler seg, driver Glooko et kontinuerlig arbeid for å oppdatere sitt sikkerhetsprogram og sin strategi for å beskytte personopplysninger og programvaren. På bakgrunn av dette forbeholder Glooko seg retten til å oppdatere dette vedlegget fra tid til annen; dog under forutsetning av at ingen oppdatering vil redusere de generelle beskyttelsene som omhandles i dette vedlegget, i vesentlig grad.

2. Sikkerhetsorganisering og program. Glooko vedlikeholder sikkerhetsprogram basert på risikovurdering. Rammeverket for Glookos sikkerhetsprogram inkluderer administrative, organisatoriske, tekniske og fysiske sikkerhetsforanstaltninger som er designet for å beskytte programvaren og konfidensialiteten, integriteten og tilgjengeligheten av personopplysninger. Glookos sikkerhetsprogram er ment å stå i forhold til programvarens beskaffenhet og Glookos forretningsdrifts størrelse og kompleksitet. Glooko har et separat og dedikert informasjonssikkerhetsteam som forvalter Glookos sikkerhetsprogram. Dette teamet tilrettelegger og støtter uavhengige revisjoner og vurderinger utført av tredjeparter. Glookos sikkerhetsrammeverk inkluderer programmer som dekker: Retningslinjer og prosedyrer, kapitalforvaltning, tilgangsforvaltning, kryptografi, fysisk sikkerhet, operasjonssikkerhet, kommunikasjonssikkerhet, Business Continuity-sikkerhet, personsikkerhet, produktsikkerhet, infrastruktursikkerhet for sky og nettverk, sikkerhetssamsvar, tredjepartssikkerhet, sårbarhetshåndtering, og sikkerhetsovervåkning og hendelsesrespons. Sikkerhet håndteres på øverste nivå i firmaet, hvor Glookos sikkerhetsoffiser møter utøvende ledelse jevnlig for å diskutere saker og koordinere sikkerhetsinitiativer i hele organisasjonen. Retningslinjer og standarder for informasjonssikkerhet revideres og godkjennes av ledelsen minst en gang årlig og gjøres tilgjengelige for referanse til alle Glooko-ansatte.

3. Konfidensialitet. Glooko har kontrollmekanismer for å opprettholde konfidensialiteten til personopplysninger i samsvar med hovedavtalen. Alle ansatte og alt kontraktspersonell hos Glooko er bundet av Glookos interne retningslinjer angående opprettholdelse av konfidensialiteten til personopplysninger og er kontraktsmessig bundet til å overholde disse forpliktelsene.

4. Personsikkerhet

    a. Bakgrunnssjekk av ansatte. Glooko utfører bakgrunnssjekker av alle nyansatte ved ansettelsen i tråd med gjeldende lokalt lovverk. Glooko verifiserer for tiden nyansattes utdanning og tidligere arbeidsforhold samt utfører referansesjekker. Når det er tillatt i tråd med gjeldende lovverk, kan Glooko også innhente vandelsattest, kredittopplysninger, migrasjonsopplysninger og foreta andre sikkerhetssjekker avhengig av arten og omfanget av en nyansatts rolle.

    b. Opplæring av ansatte. Minst én (1) gang årlig må alle ansatte i Glooko gjennomføre sikkerhets- og personvernopplæring, som omfatter Glookos sikkerhetsretningslinjer, beste praksis for sikkerhet, samt prinsipper for personvern. Medarbeidere i permisjon kan få innvilget lengre tid til å gjennomføre denne årlige opplæringen. Glookos dedikerte sikkerhetsteam gjennomfører også bevissthetsbyggende kampanjer om phishing og informerer om kommende trusler til ansatte.

5. Administrasjon av tredjepartsleverandører

    a. Leverandørvurdering. Glooko kan ta i bruk tredjepartsleverandører til å levere programvaren. Glooko utfører en sikkerhets- og risikovurdering av potensielle leverandører før samarbeid innledes, for å validere at de oppfyller Glookos sikkerhetskrav. Glooko reviderer med jevne mellomrom hver leverandør i lys av Glookos standarder for sikkerhet og forretningskontinuitet, inkludert tilgangstype og klassifisering av eventuelle opplysninger som åpnes (hvis aktuelt), nødvendige kontroller for å beskytte data, og juridiske/regulatoriske krav. Glooko sørger for at personopplysninger returneres og/eller slettes ved slutten av et leverandørsamarbeid.

    b. Leverandøravtaler. Glooko inngår skriftlige avtaler med alle sine leverandører, som inkluderer konfidensialitet, personvern og sikkerhetsforpliktelser som gir et passende nivå av beskyttelse for de personopplysninger som disse leverandørene kan behandle.

6. Arkitektur, brannmurer og datasegregering. All nettverkstilgang mellom produksjonsverter er begrenset ved hjelp av brannmurer som kun tillater autoriserte tjenester å interagere i produksjonsnettverket. Brannmurer brukes for å håndtere nettverkssegregering mellom ulike sikkerhetssoner i produksjonen og forretningsmiljøene. Glooko holder sine databaser logisk atskilt. Glooko-API-ene er designet og bygget for å identifisere og tillate tilgang kun til og fra de respektive senderne. Disse kontrollmekanismene forhindrer at kunder får tilgang til andre kunders opplysninger.

7. Fysisk sikkerhet. Datasentrene som er verter for programvaren, er strengt kontrollert av profesjonelt sikkerhetspersonale både på området og ved bygningenes inngangspunkter gjennom videoovervåking, inntrengerdeteksjonssystemer og andre elektroniske midler. Avbruddsfri strømforsyning og generatorer på stedet er tilgjengelige for å gi reservestrømkraft i tilfelle bortfall av elektrisitet fra strømnettet. I tillegg har Glookos hovedkvarter og kontorområder et fysisk sikkerhetsprogram som håndterer besøkende, bygningsinnganger og generell kontorsikkerhet.

8. Sikkerhet gjennom utforming. Glooko følger Sikkerhet gjennom utforming-prinsippene under design av programvaren. Glooko anvender også Glooko Software Development Lifecycle-standarden (SDLC) for å utføre en rekke sikkerhetsrelaterte aktiviteter for programvaren på tvers av de ulike fasene i produktutviklingssyklusen, fra kravspek og produktdesign og helt til produktdistribusjon.

9. Tilgangskontroller

    a. Tildeling av tilgang. For å minimere risikoen for dataeksponering følger Glooko prinsippene for minste privilegium gjennom en teambasert tilgangskontrollmodell ved klargjøring av systemtilgang. Glooko-personell er autorisert til å få tilgang til personopplysninger basert på jobbfunksjonen, rollen og ansvarsområdene. Slik tilgang krever godkjenning fra den ansattes leder. En ansatt sin tilgang til personopplysninger fjernes ved opphør av ansettelsesforholdet. Før en tekniker innvilges tilgang til produksjonsmiljøet, må tilgangen godkjennes av ledelsen, og teknikeren må gjennomføre intern opplæring for slik tilgang, inkludert opplæring på de relevante teamenes systemer. Glooko loggfører høyrisikohandlinger og endringer i produksjonsmiljøet. Glooko benytter automasjon til å identifisere ethvert avvik fra interne tekniske standarder som kan indikere unormal/uautorisert aktivitet, til å avgi et varsel innen noen minutter etter en konfigurasjonsendring.

    b. Passordkontroller. Når en autorisert bruker logger inn på sin konto, vil Glooko endre brukerens påloggingsinformasjon til firkanter før den lagres. Kunder kan også kreve at deres autoriserte brukere legger til ytterligere et lag med sikkerhet til kontoen sin gjennom bruk av tofaktorautentisering (2FA).

10. Endringsledelse. Glooko har en formell endringshåndteringsprosess for å administrere endringer i produksjonsmiljøet til programvaren. Dette inkluderer enhver endring i underliggende programvare, apper og systemer. Alle endringer blir underlagt en nøye gjennomgang og evalueres i et testmiljø før de blir utplassert i programvarens produksjonsmiljø. Alle endringer, inkludert evaluering av endringene i et testmiljø, dokumenteres ved hjelp av et formelt og reviderbart sakssystem. Ibruktakingsgodkjenning for høyrisikoendringer skal skje fra de riktige organisatoriske interessenter. Planer og prosedyrer implementeres også i tilfeller hvor en endring som ble tatt i bruk, må rulles tilbake for å ivareta programvarens sikkerhet.

11. Kryptering. For programvaren gjelder følgende: (a) databasene som lagrer personopplysninger krypteres i samsvar med avanserte krypteringsstandarder og (b) personopplysninger krypteres i transitt mellom kundens programvareapp og programvaren som bruker TLS v1.2

12. Håndtering av systemsårbarheter. Glooko opprettholder kontroller og retningslinjer for å redusere risikoen for sikkerhetssårbarheter, for å balansere risiko og forretnings-/ driftskravene. Glooko bruker et tredjepartsverktøy for å gjennomføre jevnlige sårbarhetsskanninger for å vurdere sårbarheter i Glookos skyinfrastruktur og forretningssystemer.

13. Gjennomtrengningstesting. Glooko utfører gjennomtrengningstester og engasjerer uavhengige tredjepartsenheter for å gjennomføre gjennomtrengningstester på appnivå. Sikkerhetstrusler og sårbarheter som oppdages, prioriteres, triageres og utbedres.

14. Håndtering av sikkerhetshendelser. Glooko opprettholder retningslinjer for håndtering av sikkerhetshendelser. Glookos responsteam for sikkerhetshendelser (T-SIRT) vurderer alle relevante sikkerhetstrusler og sårbarheter og etablerer hensiktsmessige utbedrings- og avbøtende tiltak. Glooko oppbevarer de relevante sikkerhetsloggene.

15. Robusthet og programvarekontinuitet. Programvaren bruker en rekke verktøy og mekanismer for å oppnå høy tilgjengelighet og robusthet. Når det gjelder programvaren, spenner Glookos infrastruktur over flere feiluavhengige tilgjengelighetssoner i geografiske områder som er fysisk atskilt fra hverandre. Glooko utnytter også spesialiserte verktøy som overvåker serverytelse, data og trafikkbelastningskapasitet innenfor hver tilgjengelighetssone og hvert samlokaliserte datasenter. Dersom suboptimal serverytelse eller kapasitetsoverlast oppdages på en server innenfor en tilgjengelighetssone eller et samlokalisert datasenter, vil disse spesialiserte verktøyene øke kapasiteten eller flytte trafikk for å avlaste enhver suboptimal serverytelse eller overbelastet kapasitet. Glooko blir umiddelbart varslet dersom suboptimal serverytelse eller kapasitetsoverlast oppdages.

16. Sikkerhetskopier og gjenoppretting. Glooko utfører regelmessig sikkerhetskopiering av personopplysninger. Personopplysninger som er sikkerhetskopiert, beholdes redundant på tvers av flere tilgjengelighetssoner og krypteres under transitt og lagring ved hjelp av avanserte krypteringsstandarder.

VEDLEGG IV: LISTE OVER UNDERDATABEHANDLERE

Den behandlingsansvarlige har autorisert bruk av følgende underdatabehandlere:

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

Beskrivelse av databehandlingen (inkludert en klar avgrensning av ansvarsområder i tilfeller der flere underdatabehandlere er autorisert): Skytjenesteleverandør

2. Navn: Cegedim SA
Adresse: 137 rue d'Aguesseau, 92100 Boulogne-Billancourt, Frankrike

Beskrivelse av databehandlingen (inkludert en klar avgrensning av ansvarsområder i tilfeller der flere underdatabehandlere er autorisert): Skytjenesteleverandør (kan brukes for kunder i Frankrike)

3. Navn: Pictime Groupe
Adresse: Campus du Digital 61, rue de l'Harmonie - 59262 Sainghin-en-Mélantois, Frankrike

Beskrivelse av databehandlingen (inkludert en klar avgrensning av ansvarsområder i tilfeller der flere underdatabehandlere er autorisert): Sertifisert helseopplysningsvert (kan brukes for kunder i Frankrike og Tyskland)

4. Navn: Glooko, Inc.
Adresse: 411 High Street, Palo Alto, California, 94301

Beskrivelse av databehandlingen (inkludert en klar avgrensning av ansvarsområder i tilfeller der flere underdatabehandlere er autorisert): teknisk støtte og forskriftskrav.