Sveriges Kommuner och Regioner

PROMEMORIA

2022-06-09

Laglighetsprövning av molntjänsten Glooko med avseende på dataskydd och annat integritetsskydd

Sammanfattande bedömning av regelefterlevnad och risker

I det följande redovisas enbart identifierade brister och risker i regelefterlevnad vid granskningen av tjänsterna.

OBS! Tjänsteleverantören har valt att lämna ett eget yttrande som framgår av bilaga 1.

Glooko har efter genomförd granskning av dess digitala tjänster presenterat ett utkast till ny reviderad integritetspolicy (sekretessmeddelande) som ska ersätta föreliggande från den 26 mars 2021 och korrigera däri påtalade brister samt i övrigt föreslagit vissa tekniska åtgärder. Vad dessa korrigeringar och åtgärder består av framgår av denna promemoria. Glooko har också presenterat ändringar i sitt personuppgiftsbiträdesavtal som tecknas med svenska vårdgivare. Eftersom Glooko lämnat en försäkran om att redovisade korrigeringar och åtgärder ska genomföras, upptas inte berörda brister och andra iakttagelser i denna sammanfattning.

1 Glookos molntjänst Glooko används av enskilda användare och vårdgivare för att ladda upp och dela glukosdata från mer än 190 olika glukosmätare, insulinpumpar, CGM-system och aktivitetsmätare. Tjänsten inklusive app kan användas för flera ändamål, såsom hälso- och sjukvård enligt hälso- och sjukvårdslagen, egenvård och för rent konsumentbruk (självhjälp). Glookos tjänst Diasend omfattas inte av denna laglighetsprövning eftersom Glooko påbörjat en migrering av enskilda användare och vårdgivare från Diasend-molnet till Glooko-molnet.

2 Glooko, Inc. är ett amerikanskt bolag. Bolaget har ett fast verksamhetsställe i Sverige genom Glooko AB. Avtalspart för Glookos tjänster i Sverige och inom EU/EES är emellertid Glooko AB i Sverige. Drift av Glookos data sker på Irland. I Glookos fall överförs svenska användares personuppgifter till USA och andra tredjeländer i både identifierbar och anonymiserad form för bl.a. ändamålen teknisk support, kvalitets- och säkerhetsövervakning av medicintekniska produkter (myndigheter) och framtida forskning (Glooko, Inc.). Överföringen är reglerad i Glooko AB:s villkor för molntjänsten Glooko, både i villkoren för enskilda privata användare respektive vårdgivare.

3 Glooko AB anlitar underleverantören Amazon Web Services (AWS) för applikationsförvaltning och lagring av hälsorelaterade personuppgifter i Glooko-appen och Glooko-molnet. Lagring av data sker på Irland. Glooko AB anlitar dessutom, såvitt är känt,

andra underleverantörer, bl.a. Twilio, Inc. i USA. Lagring av den analysdata som Twilio samlar in sker i USA.

4 Glooko, AWS och Twilio är emellertid amerikanska företag som, såvitt kan bedömas, enligt avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Glookos, AWS och Twilios avtal innehåller bl.a. ansvarsfriskrivningar för det fallet att de skulle tvingas av amerikansk myndighet eller domstol att lämna ut uppgifter enligt bl.a. FISA 702 eller Cloud Act. Det finns således en risk, trots organisatoriska och tekniska åtgärder från Glookos sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av Glookos kunduppgifter genom Glooko eller Twilio får dock betraktas som mycket låg med hänsyn till Glookos kärnverksamhet (diabetesmonitorering). Det finns andra risker, t.ex. cyberattacker mot molntjänster, som får betraktas som högre och mer allvarliga.

5 Glookos lösning för datadelning mellan invånare och vårdgivare är närmast att betrakta som egenvård enligt Socialstyrelsens egenvårdsföreskrifter, och inte distanssjukvård, och där vårdgivaren är personuppgiftsansvarig enbart för den uppföljning som sker av data inom ramen för egenvårdsbeslutet som den enskilde personen har godkänt får automatiskt lämnas ut till vårdgivarens lagringsyta i Glooko när denne efterfrågar uppgifterna. Glooko är personuppgiftsansvarig för den enskilda individens användarkonto och lämnar ut uppgifterna till vårdgivare enligt samtycke från användaren. För att en vårdgivare ska kunna bedriva hälso- och sjukvård per definition enligt hälso- och sjukvårdslagen, alltså distanssjukvård, genom Glooko-molnet, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att andra tillverkares produkter kopplas direkt till vårdgivarens klinik-konto i Glooko eller att vårdgivaren skapar egna hälsokonton och tillhandahåller användaruppgifter åt enskilda individer i Glooko. Så är inte fallet nu med undantag för vårdgivare som laddar upp glukosdata till sin dator via Glookos transmitter vid ett vårdbesök av en patient.

6 Den av Glooko valda juridiska lösningen för Glooko-molnet ger upphov till otydliga ansvarsförhållanden för personuppgiftsbehandlingen när en vårdgivare vid en egenvård får direktåtkomst till en enskild persons hälsokonto, som den enskilde skapat själv. Det är inte uteslutet att vårdgivaren i det läget anses personuppgiftsansvarig för alla data i kontot, även sådana som invånaren registrerat utan inblandning av en vårdgivare för att monitorera sin diabetes, trots löfte från Glooko om det motsatta. Det är i sådant fall inte Glooko som är personuppgiftsansvarig för den enskilda individens användarkontot utan en vårdgivare.

7 Rättsläget är emellertid oklart. Genom tydligare information i avtalsvillkoren för enskilda användare respektive vårdgivare torde Glooko kunna reducera väsentligen de risker som föreligger för registrerade vid ett otydligt personuppgiftsansvar på beskrivet sätt. Det är inte uteslutet att det finns ett visst ”spelrum” i brist på vägledning i lagstiftningen för både Glooko och vårdgivare att reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke. Ett annat alternativ som ska ses som en rekommendation är att Glooko

överväger en lösning i framtiden som innebär att vårdgivare inte får direktåtkomst till enskildas Glooko-konton vid distanssjukvård utan i stället skapa en lösning med två logiskt eller t.o.m. fysiskt separerade lagringslösningar – en för vårdgivare respektive en för patienter – i Glooko-molnet för att åstadkomma en tydlig ”separation of duties”. Glooko bör eftersträva att utlämnande mellan patientens lagringslösning (konto) och vårdgivarens sker genom s.k. ADB-utlämnande, dvs. filöverföring, t.ex. via API:er där data efterfrågas och lämnas ut mellan kontona. Patienter däremot får enligt patientdatalagen ha direktåtkomst till en vårdgivares vårddokumentation, om vårdgivaren så tillåter, dvs. en direktåtkomst från sitt användarkonto i Glooko till vårdgivarens klinikkonto i Glooko-molnet.

8 Beträffande vårdgivares inloggning till sitt klinik-konto på Glooko-molnet lever Glooko upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Det är dock inte en standardfunktion i tjänsten utan aktiveras på vårdgivares begäran. Glooko rekommenderas att alltid ha stark autentisering aktiverad så att svenska vårdgivare inte gör sig skyldighet till brott mot regelverket. Beträffande sedan en enskild persons inloggning till sitt konto på www.glooko.com lever Glooko inte upp till kraven på stark autentisering. Beträffande slutligen Glooko-appen omfattas dessa förvisso inte av Socialstyrelsens föreskrifter. Något krav på stark autentisering i författning finns inte. Rekommendationen är dock att enskilds inloggning till hälsodata i apparna bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i Glooko-molnet ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.

9 En vårdgivare kan skicka en inbjudan och delningskod till patienter via e-post. En inbjudan i klartext om att dela glukosdata med en vårdgivare i Glooko utgör inte en kallelse eller påminnelse till vård- och behandling enligt Socialstyrelsens föreskrifter. Att dessutom skicka en delningskod via e-post i ett öppet nät innebär stora risker för obehörigt röjande av delningskoden, och därmed hälsorelaterade uppgifter, med en tredje part. Användning av e-post för att skicka en delningskod med en patient är i strid med Socialstyrelsens föreskrifter. Det är vårdgivaren i rollen som personuppgiftsansvarig som gör sig skyldig till den otillåtna behandlingen av personuppgifter. Å andra sidan bär Glooko i rollen som personuppgiftsbiträde och tjänsteleverantör ett ansvar för att ge ”tillräckliga garantier” för skyddet av personuppgifter och registrerades fri- och rättigheter i sina tjänster och produkter. Att funktionen är frivillig för vårdgivaren att använda ”släcker” inte de krav på skydd och säkerhet som ställs på personuppgiftsbiträden i dataskyddsförordningen. Glooko rekommenderas att åtminstone informera vårdgivare om riskerna med att använda funktionen eller att lämna delningskoden till patienten vid ett personligt besök på kliniken eller i inloggat läge i avvaktan på en säkrar lösning för delning, t.ex. sms eller push-notis i den mobila enheten om att användaren har ett meddelande från en vårdgivare som denne tar del av i inloggat läge i appen. Glooko har låtit meddela att man utvärderar potentiell användning av 1177 och andra meddelandetjänster för att göra andra lösningar tillgängliga för svenska vårdgivare i syfte att bjuda in patienter att aktivera sina konton.

Innehållsförteckning

1 Bakgrund

1.1 Diabetes är ett samlingsnamn för några sjukdomar som alla ger förhöjda sockervärden (glukos) i blodet. Vid typ 1-diabetes har kroppen helt slutat tillverka insulin och kan inte bryta ner sockret. Typ 1-diabetes är en sjukdom som består hela livet och ofta debuterar i unga år. Tillståndet behandlas med basinsulin i kombination med korttidsverkande insulin och andra läkemedel. Typ 2-diabetes kan uppträda senare i livet. Kroppens produktion av insulin har av någon anledning reducerats. Kroppen har svårt att hålla sockerhalten i blodet tillräckligt låg. Symtomen kommer ofta långsamt och kan ibland vara svåra att märka. I bästa fall kan typ 2-diabetiker reglera blodsockret med särskild kost och motion. Ibland behövs dock läkemedel, t.ex. regelbunden användning av långtidsverkande insulin. Målet vid behandling av diabetes är att personen ska uppnå en så låg nivå av blodsocker som möjligt utan att samtidigt få biverkningar av de blodglukossänkande läkemedlen.

1.2 Att kontrollera glukoshalten i blodet regelbundet är viktigt för diabetiker, oavsett typ av sjukdom. Eftersom kontrollen behöver göras regelbundet, således även i hemmet, överlåter vårdgivare som regel den medicinska arbetsuppgiften att kontrollera glukoshalten i blodet på patienten via ett egenvårdsbeslut. Det finns en mängd produkter som låter patienter att i hemmet kontrollera blodsockret. De mest basal produkterna kräver ett stick i fingret och en teststicka där blodet appliceras för analys i en apparat. Med hjälp av egenmätning av glukos kan insulindoser, fysisk aktivitet och kolhydratintag anpassas så att risken för hypoglykemi minskar. Även värdet på markören för medelglukosvärdet, HbA1c, brukar förbättras med regelbunden och frekvent glukosmätning hos insulinbehandlade personer med diabetes.

1.3 På marknaden finns emellertid produkter som kan anbringas i underhuden och som regelbundet eller kontinuerligt via en sensor registrera blodsockret, s.k. CGM-system (Continuous Glucos Monitoring). Vissa CGM-system erbjuds patienter bara via vårdgivare medan andra kan köpas av vem som helst på konsumentmarknaden. Blodsockret kan avläsas i en app med stöd av en molnbaserad portal som både patient och vårdgivare har tillgång till. CGM-system används framför allt av personer med dels typ 1-diabetes, dels typ 2-diabetes som är föremål för insulinbehandling. Dessa personer har behov av tätare kontroller av glukosnivån. Många system har larmfunktion vid för lågt eller högt glukosvärde. De flesta CGM-system kräver även kalibrering dagligen med blodglukosmätning med SMBG. Ett undantag är LibreView.

1.4 När en insulinpump kombineras med en CGM som skickar blodglukosvärden till pumpen, benämns ett sådant system SAP (Sensor Augumenterad Pump). Pumpar kan avbryta insulintillförseln när glukosnivåerna når en programmerad nivå, alternativt predikteras sjunka under en programmerad nivå inom 30 minuter, för att sedan automatiskt återuppta insulintillförseln när blodglukosnivån har kommit över lägsta nivån. Hybrid Closed Loop (HCL) insulinpumpar är en utvecklad form av SAP. Skillnaden är att dessa pumpar även har ett automatläge som reglerar blodglukosnivåerna

utifrån ett förprogrammerat målvärde genom att insulintillförsel upp- eller nedregleras utefter behov. Även dessa produkter kan stödjas av en molntjänst och en app.

1.5 Tandvårds- och läkemedelsförmånsverket (TLV) har sedan i april 2012 haft i uppdrag av regeringen att genomföra hälsoekonomiska bedömningar av medicintekniska produkter. Uppdraget har förlängts i flera gånger. De hälsoekonomiska bedömningarna bygger på bästa tillgängliga kunskap och publiceras i form av ett kunskapsunderlag. TLV publicerade i november 2013 ett kunskapsunderlag med en hälsoekonomisk utvärdering gällande CGM-system.

1.6 I januari 2020 publicerade TLV en kartläggning av regionernas upphandling, distribution och användning av insulinpumpar och glukosmonitoreringssystem. Syftet med kartläggningen var att öka kunskapen kring regionernas hantering av diabeteshjälpmedel. Bakgrunden till att arbetet var att andelen patienter som använder olika diabeteshjälpmedel varierar i landet och att regionerna bedömer att det finns ett behov av att få en samlad bild över olika inköps- och införandeprocesser av hjälpmedlen. I TLV:s uppdrag ingår för övrigt inte att granska frågor om dataskydd och andra integritetsfrågor.

1.7 Många diabeteshjälpmedel bedöms vara förbrukningsartiklar och ingår i läkemedelsförmånerna. Exempel är teststickor för blodglukosmätning, insulinpennor, pennkanyler, delar av CGM-system och tillbehör till insulinpumpar. Diabeteshjälpmedel inom läkemedelsförmånerna omsatte cirka 460 miljoner kronor år 2018.[1] Exempel på delar av CGM-system som idag ingår i läkemedelsförmånerna är sändare och glukossensorer. Vad gäller insulinpumpar, har TLV tidigare bedömt att insulinpumpar med slang har en för lång livslängd för att produkterna ska kunna betraktas som förbrukningsartiklar. Detta förklarar varför inga av dessa ingår i läkemedelsförmånerna. Däremot ingår i många fall tillbehören, såsom reservoar och infusionsset. Vad gäller slanglösa insulinpumpar, patchpumpar, ingår vissa av dess komponenter i läkemedelsförmånerna.

1.8 Medicintekniska produktrådet (MTP-rådet) är en samverkan mellan regionerna inom medicinteknikområdet. MTP-rådet ger rekommendationer om ordnat införande av medicintekniska produkter. MTP-rådets tidigare rekommendationer har bidragit till att regionerna har ökat sin kunskap på området, men det finns fortfarande stor osäkerhet hur lagstiftningen inom dataskyddsområdet ska tolkas, främst när det gäller hur risker ska bedömas i samband överföring av personuppgifter till tredjeland. Detta har inneburit att Sveriges Kommuner och Regioner (SKR), som koordinerar rådet, har tagit initiativet till att granska dataskydd och andra integritetsfrågor för ett urval CGM-produkter och molntjänsten Glooko och Glooko-appen för glukosmonitorering. Följande produkter ingår i granskningen:

- FreeStyle LibreLink-appen och LibreView-molnet
- Carelink System/Personal och appar

[1] TLV, Hjälpmedel vid diabetes En kartläggning av regionernas upphandling, distribution och användning av insulinpumpar och glukosmonitoreringssystem, januari 2020, s. 16.

- Dexcom Clarity och appar
- Glooko

1.9 I denna promemoria utreds molntjänsten Glooko för glukosmonitorering och appen Glooko.

1.10 Glooko är en molnbaserad tjänst som låter enskilda användare och vårdgivare ladda upp och dela glukosdata från mer än 190 olika glukosmätare, insulinpumpar, CGM-system och aktivitetsmätare. Det gör det möjligt för patienter och vårdgivare att få tillgång till exakt samma information. Glooko är både CE-märkt och godkänt av FDA.

1.11 Glooko var ursprungligen en ren svensk produkt som tillhandahölls av det Göteborgsbaserade företaget Diasend AB. I september 2016 såldes verksamheten i Diasend AB till det amerikanska bolaget Glooko, Inc. (Glooko). Glookos huvudkontor finns i Kalifornien, USA. Sedermera omvandlades Diasend AB till dotterbolaget Glooko AB, tillika Europa-kontor inom Glooko-koncernen med säte i Göteborg, Sverige. Det finns också ytterligare Glookos-kontor i Storbritannien, Tyskland och Frankrike.

1.12 Glookos verksamhet förenas således under företagsnamnet Glooko med undantag för produkten Diasend som behållit produktnamnet inom Europa. Glooko planerar dock att gradvis avveckla Diasend till förmån för molntjänsten Glooko. Eftersom Diasend ska avvecklas i framtiden, granskas i denna laglighetsprövning molntjänsten Glooko och tillhörande app.

1.13 Det ska framhållas att Glooko inte tillhandahåller egna CGM eller SAP-system. Vad Glooko erbjuder är en transmitter som ger vårdgivare möjligheten att ladda upp glukosdata från majoriteten av glukosmätare, CGM-system och insulinpumpar på marknaden till Glooko-molnet via GMS. Avläsning av diabetesprodukter kan ske med USB-kabel (USB-port eller USB-hubb), infrarött (Inbyggd IR-mottagare eller för vissa enheter en SmartPix-kabel), NFC (Near field communication) och BLE (Bluetooth Low Energy).

1.14 Glooko har som nämnts funktionalitet för att koppla upp och läsa av ett flertal diabetesrelaterade produkter från olika tillverkare. Som regel krävs att användaren av Glooko-molnet har ett ytterligare konto i tillverkarens molntjänst, t.ex. i Abbots LibreView-moln eller Dexcoms Clarity-moln. Vad som krävs är att användaren kopplar och godkänner andra tillverkares diabetes-appar/konton till sitt Glooko-konto. Konfigureringen sker i Glooko-kontot i molntjänsten Glooko. Som ett alternativ kan användare även överföra glukosdata till molntjänsten Glooko via en programvara, Glooko Uploader, som installeras lokalt på en dator (klient). Till datorn kan sedan kopplas avläsare från olika tillverkare och produkter som sedan överför glukosdata till Glooko-molnet.

1.15 Som framhållits erbjuds dessutom vårdgivare möjlighet att skapa klinik-konton i Glooko-molnet i syfte att dela diabetesrelaterad hälsoinformation inom Glooko-kliniken (exempelvis med sjuksköterskor, läkare, terapeuter och nutritionister). Det är således

Glookos tjänst för vårdgivare som vill monitorera en patient eller ta del av data om glukosvärden för ändamålet hälso- och sjukvård eller egenvård avseende patienter med sjukdomen diabetes. En vårdgivare kan också, med patientens godkännande, skapa profiler för sina patienter och ladda upp glukosdata från patientens avläsare till sitt Glooko-konto via Glookos egen transmitter. Yrkesutövare kan också bjuda in sina patienter att ansluta till vårdgivarens Glooko-konto för att dela sin glukosdata per distans. Vårdgivarens inbjudan sker per e-post och med ett unikt klinik-ID (ProConnect-kod) som användaren anger. Patienter kan ansluta och dela sin glukosdata med obegränsat antal vårdgivare via Glooko-molnet eller Glooko-appen..

2 Uppdrag och frågeställningar

2.1 SKR har begärt en laglighetsprövning av Glooko-appen och Glooko-molnet. Laglighetsprövningen är avgränsad till själva behandlingen och skyddet av personuppgifter i Glooko-appen och inkluderar bl.a. eventuella tredjepartsapplikationer, datahantering och lagring av personuppgifter. Uppdraget är att redovisa om personuppgiftsbehandlingen i produkten är förenlig med gällande rätt.

2.2 En laglighetsprövning kan i flera avseenden beskrivas som en process för att identifiera eller hantera risker. Den övergripande risken vid behandling av personuppgifter är att den som använder tjänsten behandlar dessa på ett otillåtet sätt och i strid med gällande rätt.

2.3 Dataskyddet i Sverige består av dels sekretess- och tystnadspliktsbestämmelser, dels dataskyddsbestämmelser. Bestämmelser om sekretess och tystnadsplikt finns i offentlighets- och sekretesslagen (2009:400) och andra författningar. Behandling av personuppgifter regleras i dataskyddsförordningen, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) samt i ett flertal olika registerförfattningar beroende på huvudman eller verksamhet. Vid behandling av personuppgifter för brottsutredande syften gäller brottsdatalagen i stället för dataskyddsförordningen.

2.4 Den som obehörigen röjer personuppgifter i strid med lagstadgad sekretess- och tystnadsplikt riskerar böter eller fängelse. Underlåtenhet att uppfylla författningsenliga krav för behandling av personuppgifter kan medföra skadestånd och kraftfulla administrativa vitessanktioner. Mot den bakgrunden är en laglighetsprövning nödvändig för att kunna fastställa om behandling av hälsorelaterade personuppgifter i molnet är tillåten eller inte enligt gällande rätt.

2.5 Dataskyddsförordningen ställer bl.a. krav på den personuppgiftsansvarige att i vissa fall genomföra dataskyddskonsekvensbedömningar (artikel 35). Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En konsekvensbedömning är alltid obligatorisk vid hantering i stor

omfattning av särskilda kategorier av personuppgifter (känsliga personuppgifter) eller av personuppgifter som rör fällande domar.

2.6 Föreliggande promemoria utgör inte en dataskyddskonsekvensbedömning. Det är en laglighetsprövning, dvs. en bedömning huruvida den planerade personuppgiftsbehandlingen är laglig eller inte, och vilka åtgärder som ska vidtas för att säkerställa regelefterlevnad och därmed minska risken för att fysiska personers rättigheter och friheter kränks. En dataskyddskonsekvensbedömning ska bl.a. innehålla ”de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs”. Denna laglighetsprövning innefattar t.ex. inte hot- och riskanalyser av specifika tekniska lösningar, system eller utrustning utan enbart regelefterlevnad. Den kan emellertid utgöra ett led eller underlag för en dataskyddskonsekvensbedömning enligt dataskyddsförordningen.

2.7 Genom en laglighetsprövning identifieras således juridiska risker, vilka kan reduceras eller elimineras genom tekniska eller organisatoriska förändringar i den grundläggande tjänsten samt olika slag av överenskommelser mellan berörda aktörer. *De juridiska riskerna kategoriseras som låga, medel eller höga*.

2.8 Granskade tjänster har ett tydligt medicinskt syfte. I uppdraget ingår inte att göra en behovs- eller nyttoanalys av produkterna och tjänsterna ur ett hälso- eller sjukdomsperspektiv. Det är förvisso viktiga perspektiv för granskade produkter. Huruvida nyttan uppväger eventuella risker för den personliga integriteten ingår inte heller i uppdraget.

3 Gällande rätt

3.1 Grundläggande bestämmelser om skyddet för privatlivet och den personliga integriteten vid behandling av personuppgifter finns i EU:s dataskyddsförordning (dataskyddsförordningen), lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och i ett flertal s.k. registerförfattningar. Från regelverket undantas bl.a. behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll, det s.k. privatundantaget (artikel 2.1 c).

3.2 Dataskyddsförordningen kompletteras på ett stort antal verksamhetsområden av särskilda registerförfattningar, t.ex. patientdatalagen (2008:355; PDL) inom hälso- och sjukvårdsverksamhet.

3.3 Socialstyrelsen har meddelat kompletterande föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter inom hälso- och sjukvården.

3.4 Bestämmelser om sekretess och tystnadsplikt i hälso- och sjukvården respektive socialtjänsten finns i 25 kap. offentlighets- och sekretesslagen (2009:400; OSL). OSL är

tillämplig på myndigheter inom dessa verksamheter. Bestämmelser om tystnadsplikt inom privat driven hälso- och sjukvård finns i 6 kap. patientsäkerhetslagen (2010:659.

3.5 Normalt råder sekretess och tystnadsplikt inom hälso- och för uppgift om enskilds hälsotillstånd och personliga förhållanden. Röjande av uppgift i en patientjournal inom en vårdgivare får ske för dem som deltar i vården eller behöver uppgifterna för att fullgöra sina arbetsuppgifter. En patient kan emellertid spärra elektroniska uppgifter om sig själv som finns på en vårdenhet eller i en vårdprocess för elektronisk åtkomst från andra vårdenheter eller vårdprocesser. Utlämnande av uppgift i en patientjournal mellan vårdgivare kräver antingen patientens samtycke eller att den som har journalen i sitt förvar finner vid en menprövning att uppgiften kan lämnas ut utan men eller skada för patienten eller anhöriga. Ett tyst samtycke är också godtagbart.

3.6 Det finns ett flertal undantag från sekretessen och tystnadsplikten inom både den allmänna och enskilda hälso- och sjukvården. Undantagsbestämmelserna är spridda på flera lagar. De flesta undantagen är samlade i 25 och 26 kap. OSL och patientsäkerhetslagen. De berör olika slags fallsituationer där rättsordningen ansett att det är befogat att lämna ut uppgifter om vård- och omsorgstagare för olika ändamål utan en föregående menprövning.

3.7 I lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktsagen) finns bestämmelser om tystnadsplikt för tjänsteleverantörer. Tystnadspliktslagen blir tillämplig när en myndighet uppdrar åt ett företag eller en annan enskild (tjänsteleverantör) att tekniskt bearbeta eller tekniskt lagra uppgifter (1 §). Med tjänsteleverantör jämställs en underleverantör som medverkar till att fullgöra tjänsteleverantörens uppdrag (3 §). Med en myndighet ska också jämställas yrkesmässigt bedriven enskild verksamhet som till någon del är offentligt finansierad och som tillhör skola och utbildning samt vård, omsorg och tandvård. Den som på grund av anställning eller på något annat sätt har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet endast tekniskt bearbeta eller lagra uppgifter får inte obehörigen röja eller utnyttja dessa uppgifter (4 §).

4 Vilka registerförfattningar är tillämplig på Glooko-appen och Glooko-molnet?

4.1 Som redovisats är Glooko en tjänst för både patienter och konsumenter att kontinuerligt överföra och spara glukosvärden. Tjänsten analyserar data och presenterar sammanställningar över insulinkonsumtion och glukos över tid.

4.2 Vårdgivare har också möjlighet att skapa konton i Glooko-molnet och dela information inom Glooko-kliniken. Det är Glookos tjänst för vårdgivare som vill monitorera en patient eller ta del av data om glukosvärden för ändamålet hälso- och sjukvård eller egenvård avseende patienter med sjukdomen diabetes. En vårdgivare kan däremot inte skapa Glooko-konton åt sina patienter – dessa måste erbjudas alternativt förfoga över en klinik-kod. Därutöver krävs att användaren skapar ett eget Glooko-konto och delar sina glukosdata med vårdgivaren.

4.3 Av PDL framgår att lagen är tillämplig på vårdgivares behandling av personuppgifter inom hälso- och sjukvården (1 kap. 1 §). Om en vårdgivare förskriver t.ex. en glukosmätare eller insulinpump i syfte att bedriva kontinuerlig glukosmonitorering av en patient på distans (**distanssjukvård**) för en viss bestämd tid är PDL i huvudsak tillämplig på behandlingen av personuppgifter i produkten och stödjande digitala tjänster, t.ex. Glooko. Såvida lagen är tyst i en fråga gäller i stället dataskyddsförordningen för personuppgiftsbehandlingen.

4.4 Ett CGM-system kan även förskrivas inom ramen för **egenvård**. Bestämmelser om egenvård finns i Socialstyrelsens föreskrifter (SOSFS 2009:6) om bedömningen av om en hälso- och sjukvårdsåtgärd kan utföras som egenvård. Med egenvård avses enligt föreskrifterna en hälso- och sjukvårdsåtgärd som legitimerad hälso- och sjukvårdspersonal bedömt att en patient själv kan utföra. Av föreskrifterna framgår vidare att egenvård inte är hälso- och sjukvård enligt hälso- och sjukvårdslagen. Föreskrifterna ska tillämpas i samband med att en legitimerad yrkesutövare

- gör en bedömning av, om en hälso- och sjukvårdsåtgärd kan utföras som egenvård,
- planerar egenvården, och
- följer upp och omprövar bedömningen.

4.5 Egenvård är således medicinska arbetsuppgifter som förskrivaren bedömt att patienten kan utföra själv eller av någon annan som ska bistå patienten. Vårdgivaren ansvarar enbart för egenvårdsbedömningen och uppföljningen av egenvårdsbeslutet – det är hälso- och sjukvård. PDL är tillämplig på en vårdgivares behandling av personuppgifter i den delen. Individens egen vård faller utanför PDL:s tillämpningsområde. Den personuppgiftsbehandlingen får betraktas som ett led i en verksamhet av rent privat natur. Dataskyddsförordningen är inte tillämplig på behandling av personuppgifter som är av rent privat natur (artikel 2.1 c dataskyddsförordningen). Leverantören av tjänsten är inte personuppgiftsansvarig. Se dock nedan avsnitt 4.8.

4.6 En annan form av självhjälp är **egenmonitorering**. Det finns idag ett stort utbud av konsumentprodukter, och CE-märkta medicintekniska produkter, som vänder sig till konsumenter med intresse för sin egen hälsa. Det rör sig om klockor och appar som låter konsumenter monitorera sin egen hälsa och livsstil över tid. Produkterna är som regel molntjänstbaserade och kräver att konsumenter ingår ett avtal och tecknar ett hälsokonto hos tillverkaren där data kan sparas och analyseras. Glooko är en tjänst till vilken molnbaserade diabetesprodukter kan anslutas, såsom aktivitetsmätare, insulinpennor och CGM-system. Som exempel kan nämnas att Abbotts Freestyle-sensor kan köpas för konsumentbruk, dvs. utan någon förskrivning av läkare. Freestyle-sensorn är förvisso en CE-märkt medicinteknisk produkt. Enligt 1 kap. 3 § lagen (2021:600) med kompletterande bestämmelser till EU:s förordning om medicintekniska produkter gäller emellertid produktsäkerhetslagen för medicintekniska produkter som är avsedda för konsumenter eller som kan antas komma att användas av konsumenter. För konsumentprodukter gäller vidare konsumentlagstiftningen. Privatundantaget i dataskyddsförordningen är tillämplig (se föregående stycke).

4.7 Om leverantören av tjänsten däremot använder konsumentens personuppgifter för egna ändamål, t.ex. för att utveckla tjänsten eller möjliggöra för användaren att dela sina uppgifter med andra, t.ex. en vårdgivare, är tillverkaren personuppgiftsansvarig för behandlingen av konsumentens personuppgifter i produkten.[2] Dataskyddsförordningen är tillämplig på personuppgiftsbehandlingen.

4.8 Egenmonitorering aktualiseras också vid egenvård med stöd av förskrivna hjälpmedel som kan, men inte nödvändigtvis alltid, innefattar en digital tjänst och ett hälsokonto. Insamlade uppgifter kan sedan lämnas ut till en vårdgivare. Hjälpmedelsanvändarens egenmonitorering är inte hälso- och sjukvård. Vårdgivarens behandling av mottagna personuppgifter är däremot hälso- och sjukvård.

5 Vem är personuppgiftsansvarig?

5.1 Av 2 kap. 6 § PDL följer att en vårdgivare, oavsett om den är offentlig eller privat, är personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. I regioner och kommuner är varje myndighet (nämnd) som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

5.2 Vid användning av Glooko för distanssjukvård samt för uppföljning av egenvård (egenmonitorering) är patientansvarig vårdgivare personuppgiftsansvarig. För all annan personuppgiftsbehandling inom EU/EES som är hänförliga till Glooko-tjänster (www.Glooko.com och relaterade Glooko-produkter) är Glooko AB personuppgiftsansvarig[3], t.ex. för Glooko-konton som enskilda individer skapar i Glooko-molnet i rollen som konsument eller inom ramen för ett egenvårdsbeslut av en vårdgivare. Personuppgiftsansvaret för vårdgivare respektive Glooko behandlas närmare i avsnitt 15.

6 Rättslig grund och tillåtna ändamål för behandling av personuppgifter

Bedömning: Glooko åberopar samtycke som huvudsaklig rättslig grund för att behandla enskilda privatpersoners personuppgifter i Glooko-appen och Glooko-molnet. Det är inte en tillåten rättslig grund när samma behandling är nödvändig för att fullgöra ett avtal, i detta fall Glookos användarvillkor för privatpersoners användning av Glookos tjänster.[4] Glooko har emellertid meddelat att bolaget avser att revidera sin integritetspolicy av den 26 mars 2021 så att det tydligt framgår att Glooko samlar in personuppgifter för ändamålet att tillhandahålla tjänsten, inklusive användaruppgifter och trafikuppgifter, genom en frivillig överenskommelse (allmänna villkoren) mellan parterna i syfte att låta invånare primärt komma i åtnjutande av bolagets molntjänst, vilket är den korrekta rättsliga grunden.

Vid tidpunkten för denna granskning kunde inte ett uttryckligt samtycke som krävs för behandling av känsliga personuppgifter om enskild användare särskiljas från dennes

[2] Artikel 29-gruppen, vägledning om appar på smarta enheter (02/2013), s. 9.
[3] Glookos integritetspolicy den 26 mars 2021.
[4] Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, antagen 4 maj 2020, s. 10 och 18.

samtycke Glooko inhämtar och åberopar till stöd för att tillhandahålla primära funktioner i tjänsterna. Glooko har emellertid meddelat att bolaget arbetar aktivt för att skapa ett uttryckligt, separat samtycke för användare i produkten för att lösa problemet. Glooko uppger att bolaget siktar på att ha den här funktionen tillgänglig inom de kommande månaderna. Till dess avser Glooko att justera sin integritetspolicy för enskilda användare av den 21 mars 2021 genom att lägga till ytterligare text i Glookos integritetspolicy som klargör att den enskilde användarens tillhandahållande av hälsodata till Glooko utgör ett sådant uttryckligt samtycke för behandling av känsliga personuppgifter som avses i artikel 9.2 a i dataskyddsförordningen. Även om Glookos åtgärd på kort sikt inte är helt i linje med kraven i dataskyddsförordningen, skapar den dock en förbättrad transparensen som gynnar användarna i avvaktan på den långsiktiga lösningen.

Glooko åberopar de rättsliga grunderna ”avtal” alternativt ”intresseavvägning” (artikel 6.1 b och f i dataskyddsförordningen) för att behandla personuppgifter om anställd personal hos vårdgivare som använder Glooko-molnet, bl.a. för att förvalta www.glooko.com, tillhandahålla Glooko-tjänster, garantera säkerheten på webbplatsen och tjänster, skapa säkerhetskopior av databaser och kommunicera med användaren. Emellertid är en vårdgivare personuppgiftsansvarig för sina medarbetares personuppgifter, inte Glooko. Den rättsliga grunden för Glookos behandling av personuppgifter om enskilda medarbetare och patienter hos en vårdgivare följer av det kundavtal som bolaget tecknar med envar vårdgivare (artikel 28.3 i dataskyddsförordningen) om nyttjande av Glooko-molnet. Informationen i Glookos integritetspolicy för enskilda användare är således missvisande och bör ändras så att det tydligt framgår att den rättsliga grunden för bolagets behandling av vårdgivares medarbetares personuppgifter och patientuppgifter är personuppgiftsbiträdesavtalet mellan vårdgivaren (personuppgiftsansvarig) och Glooko (personuppgiftsbiträde). Glooko har dock låtit meddela att man avser att justera integritetspolicyn för enskilda användare av den 26 mars 2021 så att det tydligt framgår att den inte är tillämpligt på vårdgivare och deras medarbetares användning av Glookos molntjänst, och som klargör vilka avtal som gällerför Glookos användning av uppgifter som tillhör anställd personal hos vårdgivarna.

6.1 En vårdgivare får – om det är nödvändigt – behandla personuppgifter enligt PDL för bl.a. ändamålen dokumentation av vård och behandling, patientadministration i samband med individnära vård, uppföljning, utvärdering och kvalitetssäkring (2 kap. 4 §). Något samtycke krävs inte av en patient för att en vårdgivare ska få behandla personuppgifter för dessa ändamål. Inget hindrar heller att en vårdgivare samlar in personuppgifter direkt för ändamålen uppföljning, utvärdering och kvalitetssäkring, t.ex. genom utskick av enkäter till patienter. Ändamålen i 2 kap. 4 § PDL utgör samtidigt den rättsliga grunden för en vårdgivares behandling av personuppgifter.[5]

[5] SOU 2017:66 s. 227.

6.2 Vårdgivares distanssjukvård av patient med stöd av ett Glooko klinikkonto eller Glooko-molnet är således en tillåten behandling enligt PDL, såvida behandlingen är nödvändig för det ändamålet och de grundläggande dataskyddsprinciperna i dataskyddsförordningen beaktas (se avsnitt 7). Även behandling av personuppgifter i samband med en egenvårdsbedömning och egenvårdsuppföljning är tillåten. Något samtycke krävs alltså inte av patienten för att en vårdgivare ska få behandla dennes personuppgifter inom ramen för distanssjukvård eller egenvårdsbedömning respektive egenvårduppföljning. Att en vårdgivare enbart förskriver en glukosmätare åt en invånare för egenvård eller självhjälp konstituerar inte automatiskt ett personuppgiftsansvar för vårdgivaren för all behandling av personuppgifter i Glooko-appen och Glooko-molnet. Däremot torde en vårdgivare anses som personuppgiftsansvarig för hälsokonton som vårdgivaren skapar åt en invånare med hjälp av en tredjepartstjänst; det får presumeras att i dessa fall avser vårdgivaren att bedriva hälso- och sjukvård (distanssjukvård) med hjälp av tjänsten och ingenting annat. I Glooko kan emellertid vårdgivare inte skapa Glooko-konton åt patienter – dessa måste skapas av patienten själv. Avböjer en enskild person att upprätta ett sådant konto återstår möjligheten för en vårdgivare att ta del av en invånares glukosdata via Glooko transmittern och läsa in den i Glooko på vårdgivarens klinik-konto.

6.3 Vid egenvård och självhjälp (egenmonitorering) genom hälsoappar m.m. utan inblandning av en vårdgivare samlar leverantören in och behandlar individens personuppgifter normalt med stöd av den rättsliga grunden ”avtal” (användarvillkor för tjänsten) för behandlingen av hälsorelaterade uppgifter (artikel 6.1 b i dataskyddsförordningen). Individen har rätt att när som helst säga upp avtalet, varvid uppgifter på ett hälsokonto hos leverantören ska raderas. Individen kan vidare begära dataportabilitet av uppgifter som denne själv tillfört hälsokontot till sig själv eller till en annan personuppgiftsansvarig. Någon annan relevant rättslig grund i artikel 6.1 i dataskyddsförordningen för Glookos *insamling* av enskilda användares personuppgifter som avser att nyttja bolagets tjänster för glukosövervakning och insulinbehandling är inte tillämplig. Här bortses från rättsliga grunder för andra ändamål, såsom marknadsföring, kvalitets- och säkerhetsövervakning av medicintekniska produkter och forskning.

6.4 Glooko åberopar samtycke som huvudsaklig rättslig grund för att behandla enskilda privatpersoners personuppgifter i Glooko-appen och Glooko-molnet. Det är inte en tillåten rättslig grund när samma behandling är nödvändig för att fullgöra ett avtal, i detta fall Glookos användarvillkor för privatpersoners användning av Glookos tjänster.[6] Glooko har meddelat att bolaget avser att revidera sin integritetspolicy av den 26 mars 2021 så att det tydligt framgår att Glooko samlar in personuppgifter för ändamålet att tillhandahålla tjänsten, inklusive användaruppgifter och trafikuppgifter, genom en frivillig överenskommelse (allmänna villkoren) mellan parterna i syfte att låta invånare primärt komma i åtnjutande av bolagets molntjänst, vilket är den korrekta rättsliga grunden. Glooko har presenterat en ny version av sin integritetspolicy varav det framgår att ”avtal” är den rättsliga grunden för tillhandhållande av Glookos tjänster. Det innebär

[6] Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, antagen 4 maj 2020, s. 10 och 18.

att om en invånare säger upp sitt Glooko-konto, och därmed den rättsliga grunden för Glookos insamling av personuppgifter för ändamålet glukosmonitorering, nämligen avtalet för tjänsten, får bolaget fortsättningsvis behandla vissa insamlade personuppgifter för vissa ändamål, t.ex. regulatoriska krav med stöd av den rättsliga grunden ”rättslig förpliktelse”.

6.5 Utöver den rättsliga grunden ”avtal” krävs ytterligare rättsligt stöd för att få behandla känsliga personuppgifter, såsom uppgifter om hälsa (artikel 9.1). Utgångspunkten enligt dataskyddsförordningen är att det är förbjudet att behandla känsliga personuppgifter, såvida inte något av undantagen i dataskyddsförordningen från förbudet är tillämpliga. För leverantörers del som tillhandahåller hälsoappar eller liknande kommer det bara i fråga att använda undantaget ”uttryckligt samtycke” för att få behandla hälsorelaterade personuppgifter (artikel 9.2 a i dataskyddsförordningen). Övriga undantag i artikel 9.2 kan inte åberopas av leverantören i rollen som personuppgiftsansvarig för en molntjänst och berörs därför inte här. Vid tidpunkten för denna granskning kunde inte ett uttryckligt samtycke som krävs för behandling av känsliga personuppgifter om enskild användare särskiljas från dennes samtycke Glooko inhämtar och åberopar till stöd för att tillhandahålla primära funktioner i tjänsterna. Glooko har meddelat att bolaget arbetar aktivt för att skapa ett uttryckligt, separat samtycke för användare i produkten för att lösa problemet. Glooko uppger att bolaget siktar på att ha den här funktionen tillgänglig inom de kommande månaderna. Till dess avser Glooko justerat sin integritetspolicy för enskilda användare av den 21 mars 2021 genom att lägga till ytterligare text i Glookos sekretessmeddelande som klargör att den enskilde användarens tillhandahållande av hälsodata till Glooko utgör ett sådant uttryckligt samtycke för behandling av känsliga personuppgifter som avses i artikel 9.2 a i dataskyddsförordningen.

6.6 Även om Glookos åtgärd på kort sikt inte är helt i linje med kraven i dataskyddsförordningen, skapar den dock en förbättrad transparensen som gynnar användarna i avvaktan på den långsiktiga lösningen.

6.7 Därutöver inhämtar Glooko ett separat samtycke för behandling av användarens personuppgifter för ändamålen, meddelanden via e-post, liksom nyhetsbrev, feedbackdata inklusive publicering i social medier och marknadsföringssyfte, tredjeparts-appar och kakor. Användaren går inte miste om primära funktioner i appen och Glooko-molnet, om denne inte lämnar sitt samtycke för dessa typer av personuppgiftsbehandlingar eller återkallar det.

6.8 I Glookos integritetspolicy för enskilda användare[7] redogör bolaget för de rättsliga grunderna för att behandla enskilda personers personuppgifter. Av denna framgår att Glooko kan komma att behandla användarens affärsrelaterade kontouppgifter. Affärskontouppgifter kan vara sådant som namn, e-postadress och annan information användaren har lämnat till Glooko. Av policyn framgår vidare att källan till affärskontouppgifterna kan vara ”din arbetsgivare eller någon av dina branschpartners”. Affärskontouppgifterna används av Glooko för att driva www.glooko.com, tillhandahålla

[7] Glookos integritetspolicy den 26 mars 2021.

bolagets tjänster, garantera säkerheten för webbplatsen och tjänster, upprätthålla säkerhetskopior av databaser och kommunicera med användaren. Dessutom anges följande i policyn: ”*Om behandlingen sker i syfte att fullgöra ett avtal som har ingåtts mellan dig (eller din arbetsgivare) och oss, och/eller i syfte att på din begäran vidta åtgärder för att ingå ett sådant avtal, är den rättsliga grunden för denna behandling fullgörande av avtal*.”

6.9 När det gäller behandling av personuppgifter med stöd av den rättsliga grunden ”avtal” (artikel 6.1 b i dataskyddsförordningen) krävs det att den registrerade själv är avtalspart, inte bara berättigad enligt ett (tredjemans)avtal. Ett avtal mellan Glooko och en juridisk person, t.ex. en vårdgivare, kan således inte enligt denna bestämmelse rättfärdiga behandling av personuppgifter, t.ex. uppgifter om de fysiska personer som är anställda hos vårdgivaren. I stället är den rättsliga grunden för Glookos behandling av hälso- och sjukvårdspersonal hos en vårdgivare som använder Glooko-molnet det personuppgiftsbiträdesavtal (artikel 28.3 i dataskyddsförordningen) som upprättas när vårdgivaren tecknar en licens för tjänsten (se Glookos huvudavtal för vårdgivare den 1 december 2021).

6.10 Lika missvisande är informationen i Glookos integritetspolicy för enskilda användare[8] där det bl.a. framgår att ”*Om du är en personuppgiftsansvarig som representerar registrerade personer är den rättsliga grunden för behandlingen vårt berättigade intresse*.”[9] Här torde avses den rättsliga grunden intresseavvägning i artikel 6.1 i dataskyddsförordningen.

6.11 Glooko har låtit meddela att man avser att justera integritetspolicyn för enskilda användare av den 26 mars 2021 så att det tydligt framgår att den inte är tillämpligt på vårdgivare och deras medarbetares användning av Glooko, och som klargör vilka avtal som gällerför Glookos användning av uppgifter som tillhör anställd personal hos vårdgivarna.

6.12 Glookos vidareutnyttjande av vårdgivares personuppgifter, både personalens och patienters, regleras för övrigt i ett standardiserat kundavtal om nyttjande av Glooko-tjänsterna.[10] Av kundavtalet för vårdgivare, under rubriken Villkor för mjukvara, punkt 14, upplåter vårdgivare en nyttjanderätt för Glooko att använda anonymiserad, avidentifierad och aggregerad data, data som härrör från denna data samt relaterade uppgifter, inbegripet bl.a. uppgifter om enheter, system, tillhörande mjukvara, tjänster eller kringutrustning som genereras av och är förbundna med Kundens användning av Mjukvaran (”Analysdata”). Denna analysdata kan användas av Glooko för att underlätta produktutveckling, förbättring, mjukvaruuppdateringar, licensautentisering, support, rapportering, analys och andra affärssyften. ”Affärskontouppgifter” (se punkt 6.8 ovan) finns inte omnämnd i Glookos beskrivning av nyttjanderätt av kundens (vårdgivarens) data i kundavtalet. Glooko saknar förvisso inte stöd för att behandla personuppgifter om

[8] Glookos integritetspolicy den 26 mars 2021.
[9] Glookos integritetspolicy den 26 mars 2021, avsnitt 2.2.
[10] Glookos huvudavtal med vårdgivare den 1 december 2021.

medarbetare hos vårdgivare för att tillhandahålla tjänsten Glooko och support, men villkoren skapar förvirring och är motsägelsefulla.

6.13 I Glookos integritetspolicy för enskilda användare[11] redogör bolaget för de rättsliga grunderna för att behandla enskilda personers personuppgifter för ändamålet regulatoriska krav. Regulatoriska uppgifter kan komma att behandlas av Glooko i syfte att skapa interna rapporter och register som kan göras tillgängliga för myndigheter på dessas begäran. Den rättsliga grunden för denna behandling är rättsliga förpliktelser enligt artikel 6.1 i dataskyddsförordningen. Skälet för att använda denna rättsliga grund är enligt Glooko EU:s förordning om medicintekniska produkter (MDR). Eftersom Glooko är en CE-märkt medicinteknisk produkt har bolaget skyldigheter som följer av bestämmelser om kvalitets- och säkerhetsövervakning av medicintekniska produkter, dvs. regulatoriska krav. Det får anses utgöra en relevant rättslig grund för insamling av personuppgifter för det specifika ändamålet. Det är emellertid inte helt klart vilka specifika personuppgifter som samlas in för det ändamålet. Glooko samlar i huvudsak in personuppgifter för ändamålet att tillhandahålla tjänsten genom en frivillig överenskommelse (avtal) mellan parterna i syfte att låta enskilda användare (patienter och konsumenter) primärt komma i åtnjutande av bolagets tjänster. Det innebär att om en enskild användare säger upp sitt Glooko-konto, och därmed den rättsliga grunden för Glookos insamling av personuppgifter för ändamålet egenmonitorering, nämligen avtalet för tjänsten, får bolaget fortsättningsvis behandla vissa insamlade personuppgifter för ändamålet regulatoriska krav med stöd av den rättsliga grunden ”rättslig förpliktelse”.

6.14 Utöver den rättsliga grunden ”avtal” behöver leverantören ytterligare rättsligt stöd för att få behandla känsliga personuppgifter, såsom uppgifter om hälsa (artikel 9.1 i dataskyddsförordningen). Utgångspunkten enligt dataskyddsförordningen är att det är förbjudet att behandla känsliga personuppgifter, såvida inte något av undantagen i dataskyddsförordningen från förbudet är tillämpligt. För leverantörers del som tillhandahåller hälsoappar eller liknande kommer det bara i fråga att använda undantaget ”uttryckligt samtycke” för att få behandla hälsorelaterade personuppgifter (artikel 9.2 a i dataskyddsförordningen) för att tillhandahålla tjänsten. Övriga undantag från förbudet kan inte åberopas av leverantören i rollen som personuppgiftsansvarig och berörs därför inte här.

Som konstaterats saknar emellertid Glooko ett ”uttryckligt” separat samtycke för behandlingen av enskilda användares hälsorelaterade uppgifter. Det generella samtycke som Glooko inhämtar för de primära funktionerna i tjänsten torde inte uppfylla kraven på ett uttryckligt samtycke för behandling av känsliga personuppgifter. Som framhållits har Glooko meddelat att bolaget arbetar aktivt för att skapa ett uttryckligt, separat samtycke för användare i produkten för att lösa problemet. Glooko uppger att bolaget siktar på att ha den här funktionen tillgänglig inom de kommande månaderna. Till dess har Glooko justerat sin integritetspolicy för enskilda användare av den 21 mars 2021 genom att lägga till ytterligare text i Glookos sekretessmeddelande som klargör att den enskilde användarens tillhandahållande av hälsodata till Glooko utgör ett sådant uttryckligt

[11] Glookos integritetspolicy den 26 mars 2021, avsnitt 2.11.

samtycke för behandling av känsliga personuppgifter som avses i artikel 9.2 a i dataskyddsförordningen.

6.15 Glooko använder vidare enskilda användares uppgifter för framtida forskning då denne tecknar ett Glooko-konto, dock oklart på vilken rättslig grund. Uppgifterna är emellertid anonymiserade. Framställningen återkommer till denna fråga i avsnitt 15.

7 Grundläggande krav, information och rättigheter för enskilda

7.1 Dataskyddsförordningen innehåller i artikel 5 grundläggande krav för all behandling av personuppgifter som alltid ska beaktas. Personuppgifterna ska bl.a. vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålen med behandlingen får inte behandlas. Personuppgifter som behandlas ska vidare enligt de grundläggande principerna vara korrekta och aktuella. Dessutom har nya principer tillkommit i förhållande till det tidigare dataskyddsdirektivet. En sådan är principen om öppenhet (transparens) gentemot den registrerade som kommer till uttryck i skyldigheten för personuppgiftsansvariga att informera registrerade om personuppgiftsbehandlingen (artikel 12, 13 och 14). Integritet och konfidentialitet har också lyfts in i de grundläggande principerna.

7.2 Den personuppgiftsansvarige inte bara ansvarar för att de grundläggande principerna följs utan ska också kunna ”visa” att de efterlevs, s.k. ansvarsskyldighet (artikel 5.2). Ansvarsskyldigheten innebär mer precist att den personuppgiftsansvarige med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med förordningen. De åtgärder som vidtas ska ses över och uppdateras vid behov (artikel 24.1). Ett sätt för den personuppgiftsansvarige att visa att denne fullgör sina skyldigheter är att tillämpa godkända uppförandekoder eller godkända certifieringsmekanismer (artikel 24.3).

7.3 Den information om personuppgiftsbehandlingen som ska tillhandahållas den registrerade har preciserats och utvidgats i dataskyddsförordningen, och det anges uttryckligen att den *personuppgiftsansvarige* ska tillhandahålla informationen om sin behandling av personuppgifter i en begriplig och lättillgänglig form. Det ska enligt förordningen aldrig komma som en överraskning för en registrerad att någon hanterar dennes personuppgifter och för vilka ändamål. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandling av personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används (skäl 39 i dataskyddsförordningen).

7.4 Patienters och konsumenters rättigheter vid behandling av deras personuppgifter regleras i huvudsak i dataskyddsförordningen – inte i PDL med något undantag. Registrerades rättigheter har förstärkts i dataskyddsförordningen i syfte att ge den registrerade ökad

kontroll över sina personuppgifter. Det finns åtta rättigheter i rättighetskatalogen. Flera rättigheter är nya. Inom hälso- och sjukvård är vissa av dessa rättigheter i dataskyddsförordningen beskurna eller reglerade i särskild ordning. Bl.a. får en patient inte motsätta sig behandling av personuppgifter inom hälso- och sjukvård. Vidare kan de inte åberopa rätten att bli bortglömd. I hälso- och sjukvården får en patient i stället begära journalförstöring med stöd av PDL hos Inspektionen för vård och omsorg (IVO).

8 Anlitande av personuppgiftsbiträden

8.1 Personuppgiftsansvaret innebär ett ansvar både för att efterleva dataskyddsförordningen och de nationella regler som meddelats med stöd av den, och att dokumentera de överväganden som görs och åtgärder som vidtas på ett sådant sätt att efterlevnaden kan påvisas. Detta följer av ansvarsskyldigheten (se avsnitt 7.2).

8.2 Med personuppgiftsbiträde avses någon som behandlar personuppgifter ”för den personuppgiftsansvariges räkning”.

8.3 När en personuppgiftsansvarig, t.ex. en vårdgivare, anlitar ett personuppgiftsbiträde ska det ske i enlighet med de regler som uppställs i dataskyddsförordningen. Det finns med utgångspunkt i ansvarsskyldigheten även anledning att dokumentera de överväganden som görs, avseende exempelvis val av biträde, på lämpligt sätt. När det gäller val av biträde framgår det av dataskyddsförordningen att om en behandling ska genomföras för en personuppgiftsansvarigs räkning ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som kan ge ”tillräckliga garantier” om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas (artikel 28.1). Av skäl 81 framgår att tillräckliga garantier ska ges i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser.

8.4 Den personuppgiftsansvarige har med andra ord en omsorgsplikt vid val av biträde, som innefattar att göra en riskbedömning. Omsorgsplikten innebär att den personuppgiftsansvarige behöver utreda vilka förutsättningar personuppgiftsbiträdet har att efterleva sina skyldigheter enligt dataskyddsregelverket.

8.5 Eventuella skyldigheter som personuppgiftsbiträdet omfattas av enligt tredjelands lagstiftning att lämna ut personuppgifter till det landets myndigheter i strid med bestämmelserna om tredjelandsöverföring i dataskyddsförordningen bör således tas i beaktande vid bedömningen av om personuppgiftsbiträdet kan ge tillräckliga garantier.

8.6 Av dataskyddsförordningen framgår att när uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige (artikel 28.3). Sådana avtal brukar enligt svenskt språkbruk benämnas personuppgiftsbiträdesavtal.

8.7 Personuppgiftsbiträdesavtalet ska vara skriftligt (artikel 28.9) och kan helt eller delvis baseras på sådana standardavtalsklausuler som beslutas av kommissionen eller en tillsynsmyndighet (artikel 28.6–8). I personuppgiftsbiträdesavtalet ska föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges (artikel 28.3).

8.8 I dataskyddsförordningen föreskrivs dessutom följande rörande avtalets innehåll.

- Det ska framgå att biträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation (artikel 28.3, led a).

- Avtalet ska till sitt innehåll säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt (artikel 28.3, led b).

- Det ska framgå av avtalet att personuppgiftsbiträdet ska vidta alla de tekniska och organisatoriska åtgärder som krävs enligt dataskyddsförordningen för att säkerställa en lämplig säkerhetsnivå (artikel 28.3 led c och artikel 32).

- Personuppgiftsbiträdet ska vidare i avtalet åta sig att respektera de villkor som uppställs i avtalet för anlitande av ett annat personuppgiftsbiträde (underbiträde) (artikel 28.3, led d).

- I avtalet ska biträdet även åläggas att hjälpa den personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder och om detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter (artikel 28.3, led e).

- Det ska av avtalet framgå att personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att se till att vissa i förordningen angivna skyldigheter avseende bl.a. säkerhet uppfylls (artikel 28, led f).

- Avtalet ska reglera hanteringen av personuppgifter när biträdets uppdrag att behandla personuppgifter upphört (artikel 28, led g).

- Personuppgiftsbiträdet ska dessutom i avtalet åläggas att ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige (artikel 28, led h).

8.9 Personuppgiftsbiträdets uppgift är att behandla personuppgifter enligt den personuppgiftsansvariges instruktioner (artikel 29). Sådan personuppgiftsbehandling som går utöver den ansvariges instruktioner är inte tillåten. I personuppgiftsbiträdesavtalet regleras ytterligare skyldigheter för biträdet gentemot den ansvarige. Utöver skyldigheten att enbart behandla personuppgifter enligt den ansvariges instruktioner och de skyldigheter som framgår av biträdesavtalet så innehåller dataskyddsförordningen vissa skyldigheter som direkt åligger personuppgiftsbiträdet.

- Personuppgiftsbiträdet ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning (artikel 30).

- Personuppgiftsbiträdet ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dennes uppgifter (artikel 31).

- Personuppgiftsbiträdet har ett självständigt ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (artikel 32).

- Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident (artikel 33.2). Personuppgiftsbiträdet ska också under vissa omständigheter utse ett dataskyddsombud (artikel 37).

- Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde (underbiträde) utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar (artikel 28.2). Personuppgiftsbiträdet ska genom ett avtal eller en annan rättsakt ålägga underbiträdet samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

- Om personuppgiftsbiträdet inte uppfyller sina skyldigheter enligt dataskyddsförordningen kan biträdet bli föremål för administrativa sanktionsavgifter (artikel 83). Det finns även möjlighet för en registrerad att väcka talan mot ett personuppgiftsbiträde (artikel 79). Den registrerade har också rätt till ersättning från personuppgiftsbiträdet när skada inträffar som en följd av överträdelse av förordningens bestämmelser (artikel 83).

9 Skydd av personuppgifter

9.1 En allmän bestämmelse om den personuppgiftsansvariges ansvar för personuppgifter finns i artikel 24 i dataskyddsförordningen. Av den följer att den personuppgiftsansvarige, med beaktande av behandlingens art, omfattning, sammanhang

och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen (se punkt 7.2). Rutiner för dataskydd, dokumenterade riskbedömningar, dokumentation på förändringar i digitala tjänster är exempel på åtgärder för att kunna visa ansvarsskyldighet. Tekniska och organisatoriska åtgärder ska ses över och uppdateras vid behov, vilket ska dokumenteras. Vidare anges i dataskyddsförordningen att om det står i proportion till behandlingen, ska åtgärderna omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

9.2 En precisering av det nämnda ansvaret finns i artikel 25 i dataskyddsförordningen som handlar om inbyggt dataskydd och dataskydd som standard. Enligt den artikeln ska den personuppgiftsansvarige, med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering. Åtgärderna ska vara utformade för ett effektivt genomförande av dataskyddsprinciper, såsom uppgiftsminimering, och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Åtgärderna ska vidtas både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen.

9.3 I dataskyddsförordningen finns i artikel 32 en bestämmelse som preciserar de säkerhetsåtgärder som bör vidtas av både personuppgiftsansvariga och personuppgiftsbiträden.

- De åtgärder som ska vidtas ska, när det är lämpligt, inbegripa pseudonymisering och kryptering av personuppgifter, förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna, förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

- Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

- Anslutning till en godkänd uppförandekod som avses i artikel 40 i dataskyddsförordningen eller en godkänd certifieringsmekanism som avses i artikel 42 i dataskyddsförordningen får användas för att visa att kraven följs.

- Åtgärder ska vidtas för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som

får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

10 Tredjelandsöverföring

10.1 Som allmän princip gäller enligt artikel 44 i dataskyddsförordningen att överföring av personuppgifter till ett tredjeland eller en internationell organisation bara får ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i dataskyddsförordningen, uppfyller villkoren i artikel 45–49.

10.2 Av artikel 45 i dataskyddsförordningen framgår att personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. Artikeln förutsätter alltså ett beslut från kommissionen.

10.3 I avsaknad av ett beslut från kommissionen får en personuppgiftsansvarig eller ett personuppgiftsbiträde enligt artikel 46 i dataskyddsförordningen endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga. Lämpliga skyddsåtgärder får bl.a. ta formen av bindande företagsbestämmelser, för vilka förutsättningarna anges i artikel 47 i dataskyddsförordningen, eller standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2. Kommissionen har beslutat standardavtalsklausuler som kan användas mellan personuppgiftsansvariga eller mellan personuppgiftsansvariga och personuppgiftsbiträden i tredje land.

10.4 Artikel 48 i dataskyddsförordningen slår fast att domstolsbeslut eller beslut från myndigheter i tredjeland om krav på att lämna ut personuppgifter får erkännas eller genomföras endast om det grundar sig på en internationell överenskommelse, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat.

10.5 Om det inte finns något beslut om adekvat skyddsnivå enligt artikel 45 eller vidtagna lämpliga skyddsåtgärder enligt artikel 46, får personuppgifter överföras till ett tredjeland eller en internationell organisation endast om minst ett av flera – i artikel 49 i dataskyddsförordningen angivna – villkor är uppfyllt. Personuppgifter får överföras om överföringen sker med stöd av samtycke från den registrerade (a), om överföringen är nödvändig för att fullgöra ett avtal mellan den personuppgiftsansvarige och den registrerade eller en annan fysisk eller juridisk person som agerar i den registrerades intresse (b och c), om överföringen är nödvändig av viktiga skäl som rör allmänintresset (d), om överföringen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk (e), om överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke (f), eller om överföringen görs från ett register som enligt

unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information (g).

10.6 Av artikel 49.3 i dataskyddsförordningen framgår att åtgärder som vidtas av offentliga myndigheter som ett led i myndighetsutövning inte får vidtas med stöd av samtycke eller för att överföringen är nödvändig för att fullgöra ett avtal mellan den personuppgiftsansvarige och den registrerade eller en annan fysisk eller juridisk person som agerar i den registrerades intresse.

10.7 Kravet på ett allmänintresse, om överföringen sker för att den är nödvändig av viktiga skäl som rör allmänintresset, ska enligt artikel 49.4 i dataskyddsförordningen vara erkänd i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av.

10.8 I artikel 49.5 i dataskyddsförordningen ges möjlighet att i unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland eller en internationell organisation, om beslut om adekvat skyddsnivå saknas.

10.9 Om en överföring inte har stöd i artikel 45 eller 46 och inget av undantagen i artikel 49.1 första stycket i dataskyddsförordningen är tillämpligt, får en överföring till ett tredjeland eller en internationell organisation enligt artikel 49.1 andra stycket äga rum endast om överföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre, och den personuppgiftsansvarige har bedömt samtliga omständigheter kring överföringen av uppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifter. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om överföringen.

10.10 Europeiska dataskyddsstyrelsen (EDPB) har publicerat rekommendationer om adekvata skyddsåtgärder för tredjelandsöverföring. Rekommendationerna är ett svar på EU-domstolens dom i Schrems II.[12] EDPB har vidare publicerat ett utkast till riktlinjer som klargör vad som utgör, och inte utgör, en överföring av personuppgifter till tredjeland.[13] Riktlinjerna är i skrivande stund föremål för synpunkter.

11 Sanktionsavgifter

11.1 Genom dataskyddsförordningen införs ett nytt gemensamt system med administrativa sanktionsavgifter som ska tas ut vid vissa typer av överträdelser av förordningen (artikel 83). Sanktionsavgifter beslutas av Integritetsskyddsmyndigheten (f.d. Datainspektionen) och kan omfatta både personuppgiftsansvariga och personuppgiftsbiträden.

[12] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021.
[13] Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

11.2 Registrerade kan vidare utkräva skadestånd från den personuppgiftsansvarige (artikel 82). Även personuppgiftsbiträden kan bli skadeståndsansvariga.

12 Applikationen Glooko och Glooko-molnet

12.1 Glooko är leverantör av Glooko-appen och Glooko-molnet. Glooko är både en FDA-godkänd och CE-märkt produkt. Glooko är en molnbaserad tjänst som låter enskilda användare och vårdgivare ladda upp och dela glukosdata från mer än 190 olika glukosmätare, insulinpumpar, CGM-system och aktivitetsmätare. Det gör det möjligt för patienter och vårdgivare att få tillgång till exakt samma information. Analys av data och larm vid överskridande av godtagbara blodsockervärden sker i Glookos moln.

12.2 Enligt Glooko har hela Glooko-systemet byggts med säkerhet i åtanke.[14] Systemet använder Amazon Web Services (AWS) infrastruktur (se vidare avsnitt 13). Teknisk support tillhandahålls av både Glooko AB och Glooko, Inc. i USA. All data i Glooko-molnet är krypterad, både i vila och vid transport. Européers kundinformation lagras inom EU (Irland respektive Frankrike – i det senare fallet enbart franska användare) för bättre integritetsskydd. Glooko uppfyller vidare krav i HIPAA som bl.a. innefattar strikta åtkomstkontroller för Glookos personal och fortlöpande säkerhetsutbildning för alla medarbetare.

12.3 Programvaran Glooko Uploader och Glooko-appen överför personliga glukosvärden som registreras med produkter från andra tillverkare på ett säkert sätt till Glooko-molnet med hjälp av en mängd avläsartekniker, såsom IR, NFC-teknik (närfältskommunikation) och Bluetooth-teknik. NFC har en utökad skyddsnivå på så sätt att omedelbar fysisk närhet krävs. Krypterade Bluetooth-anslutningar upprättas under NFC-kommunikation med Glooko-app och avläsare.

12.4 EU-medborgare och medborgare inom ESS garanteras av Glooko en rätt att få utöva sina rättigheter enligt dataskyddsförordningen. Glooko garanterar även andra användare över hela världen samma rättigheter. Amazon betraktas av Glooko som en betrodd molntjänstleverantörer. Amazon har en serie av säkerhetscertifieringar inklusive:

- ISO 27001 Ledningssystem för informationssäkerhet
- PCI-överensstämmelse (nivå 1)
- AICPA och SOC
- HIPAA

12.5 Glooko-appen sparar ovillkorligen användarens glukosvärden i molnet, dvs. i Glooko-molnet. En användare kan således inte begränsa överföring av data från appen till molnet. En användare kan således inte välja huruvida värden ska sparas i molnet eller lokalt i appen.

[14] Glookos personuppgiftsbiträdesavtal (standardavtal) med vårdgivare februari 2022.

12.6 Privatpersons inloggning till Glooko-appen och Glooko-molnet sker utan någon stark autentisering. Vårdgivares åtkomst till egen data i Glooko-molnet (www.glooko.com) sker dock med stark autentisering genom engångslösenord via e-post. Svenska vårdgivare kan dock inte nyttja SITHS-kort eller annat slag av e-legitimation. I Glooko-kontot, liksom i appen, kan en användare ta del av glukosvärden över tid såsom dagliga mönster, tid i målvärdesområde, medelvärde för glukos. I www.glooko.com kan användaren även skriva ut rapporter i pdf-format.

12.7 En användare kan dela sina glukosvärden med en vårdgivare via Glooko-appen eller Glooko-kontot på www.glooko.com. Vårdgivare kan bjuda in sina patienter att ansluta till vårdgivarens Glooko-konto för att dela sin glukosdata per distans. Vårdgivarens inbjudan sker per e-post och med ett unikt klinik-ID som användaren anger. Patienter kan ansluta och dela sin glukosdata med obegränsat antal vårdgivare via Glooko-molnet eller Glooko-appen. Vårdgivares åtkomst till en invånares Glooko-konto sker såvitt förstås genom s.k. direktåtkomst. En vårdgivare kan däremot inte skapa ett Glooko-konto åt en patient. Information saknas dock i Glookos integritetspolicy för enskilda användare[15] och på Glookos supportsida om att en vårdgivare är personuppgiftsansvarig för de personuppgifter om en enskild individ som denne behandlar i sitt Glooko klinik-konto.

12.8 Glooko hävdar att bolaget använder sig av kommissionens standardavtalsklausuler vid överföring av privatpersoners respektive hälso- och sjukvårdspersonal och patienters personuppgifter från EU till USA.[16] Det innebär att Glooko åtar sig att respektera de rättigheter som EU-medborgare kommer i åtnjutande av enligt dataskyddsförordningen. I integritetspolicyn för enskilda användare[17] hänvisas emellertid till kommissionens äldre standardavtalsklausuler (SCC). Dessa har ersatts av nya SCC 2021 bestående av olika moduler beroende på vem som är avsändare och mottagare av personuppgifter inom EU respektive tredjeland. Vidare hänvisas i integritetspolicyn för enskilda användare till en överenskommelse mellan EU och USA om skydd för personuppgifter vid överföringar till USA benämnd Safe Harbor, medan användarvillkoren för enskilda användare hänvisar till en annan överenskommelse benämnd Privacy Shield. Enligt domar från EU-domstolen är båda överenskommelserna otillåtna eftersom de inte garanterar ett tillräckligt skydd för européers personuppgifter när de hanteras av amerikanska myndigheter.

12.9 Glooko har låtit meddela att man avser att justera integritetspolicyn av den 26 mars 2021 så att det inte längre framgår några hänvisningar till att Glooko använder Privacy Shield eller Safe Harbour som instrument för att överföra personuppgifter till ett USA. Glooko har också i ett utkast till ny integritetspolicy som ska ersätta den nuvarande från 26 mars 2021 inkluderat länkar till kommissionens nuvarande godkända standardavtalsklausuler. Kommissionens standardavtalsklausuler finns numera inte bilagda eller inbäddade i varken Glookos användarvillkor för enskilda användare eller i Glookos

[15] Glookos integritetspolicy den 26 mars 2021 och Glookos personuppgiftsbiträdesavtal (standardavtal) med vårdgivare februari 2022.
[16] Glookos integritetspolicy den 26 mars 2021 och Glookos användarvillkor för vårdgivare den 1 december 2020.

personuppgiftsbiträdesavtal. I det senare fallet är standardavtalsklausulerna inte nödvändiga för överföringen av svenska vårdgivares medarbetares och patienters personuppgifter till Irland (AWS). Däremot sker en tredjelandsöverföring när dotterbolaget Glooko AB överför personuppgifter till bl.a. Glooko, Inc. i USA. Modul 3 i kommissionens standardavtalsklausuler ska appliceras vid en sådan tredjelandsöverföring (personuppgiftsbiträde till personuppgiftsbiträde). Standardavtalsklausulen ska tecknas mellan Glooko AB i Sverige och Glooko, Inc. i USA och med andra underbiträden i världen.

12.10 I Glookos personuppgiftsbiträdesavtal med vårdgivare, benämnd ”Standardavtal” (februari 2022), hänvisas emellertid korrekt till att bolaget använder kommissionens standardavtalsklausuler från 2021. Emellertid saknar personuppgiftsbiträdesavtalet tydliga dokumenterade instruktioner från vårdgivaren till Glooko och bolagets underbiträden om för vilka ändamål bolaget får behandla vårdgivarens patientuppgifter, såsom för teknisk support, regulatoriska krav, tillhandhållande av tjänsten, teknisk support, produktutveckling och mycket mer. Vidare har Glooko uteslutit klausulerna 14 (Local laws and practices affecting compliance with the Clauses) och 15 (Obligations of the data importer in case of access by public authorities), genom att ange att dessa inte är tillämpbara. Glookos överföringsmekanismer av personuppgifter till USA och andra länder samt regleringen mellan bolaget och vårdgivare avseende dataskydd och instruktioner behandlas i avsnitt 15. Det ska nämnas att Glooko presenterat korrigerande åtgärder i avtalsvillkoren inklusive personuppgiftsbiträdesavtal. Dessa berörs också i avsnitt 15.

Av Glookos integritetspolicy för enskilda användare av Glooko[18] framgår att om användaren begär support av Glooko och delar sina felsökningsuppgifter (däribland frågeuppgifter, tjänsterelaterade uppgifter och korrespondensuppgifter), överförs dessa uppgifter till USA i den mån det är nödvändigt för att bolaget ska kunna ge teknisk support och utföra bredare analys för att upptäcka systemproblem och den lokala supporten i Sverige inte kan lösa frågan. Vem eller vilka som är ansvariga för supporten i USA framgår inte. Glooko har emellertid i ett utkast till ny integritetspolicy som ska ersätta den från 26 mars 2021 tydligare beskrivit vem eller vilka som är ansvariga för supporten i USA.

12.11 Av integritetspolicy för enskilda användare[19] framgår vidare att bolaget delar personuppgifter med ett flertal tjänsteleverantörer: ”*Vi använder tjänsteleverantörer för leverans av olika delar av tjänsterna. Vissa av dessa tjänsteleverantörer finns utanför EES. Eventuella internationella överföringar av personuppgifter skyddas av tillämpliga säkerhetsåtgärder, nämligen användning av standardiserade kontraktsbestämmelser som har antagits eller godkänts av Europeiska kommissionen, ett beslut om adekvat skydd från Europeiska kommissionen eller bindande företagsregler eller ditt uttryckta samtycke*.” Det framgår emellertid inte, bortsett från dotterbolaget Glooko AB i Sverige,

[19] Glookos integritetspolicy den 26 mars 2021.

AWS och Cegedim SA (franska medborgare), vilka andra aktörer Glooko delar registrerades ”personuppgifter” med och vilka slag av personuppgifter som delas.

12.12 Det framgår inte heller med all önskvärd tydlighet i vilken utsträckning Glooko tillämpar principerna om uppgiftsminimering eller lagringsminimering enligt artikel 5.1 i dataskyddsförordningen vid delning av personuppgifter med andra aktörer och myndigheter. Av Glookos integritetspolicy för enskilda användare[20] framgår å ena sidan att Glooko kan komma att lämna ut registrerades ”personuppgifter” till sina leverantörer eller underentreprenörer i den mån det rimligtvis krävs för att kunna tillhandahålla tjänsterna. ”Tjänsterelaterade uppgifter”, såsom namn, e-postadress, kön, födelsedatum, biometriska uppgifter och medicinsk information samt andra typer av inlämnad eller uppladdad information, omfattas dock enligt Glooko av ytterligare restriktioner och får inte lämnas ut till någon sådan tredjepartsleverantör om de inte först har avidentifierats, dvs. krypterats med en säkerhetsnyckel.[21] Glooko tillämpar i Glooko-molnet en s.k. Bring-Your-Own-Key-lösning (BYOK).

12.13 Å andra sidan framgår det av integritetspolicyn att ”tjänsterelaterade uppgifter” och användningsuppgifter används av Glooko och dess underleverantörer när användare begär teknisk support för att kunna diagnostisera ett problem.[22] Det hade varit önskvärt med en tydligare beskrivning vad för slags information Glooko och dess underleverantörer tar del av i dessa lägen och i vilken utsträckning man strävar efter pseudonymisering. Samma oklarheter om vilka uppgifter som används av Glooko och i vilken utsträckning de pseudonymiseras eller anonymiseras råder vid behandling av registrerades personuppgifter för andra ändamål, såsom t.ex. regulatoriska krav. Glooko har emellertid i ett utkast till ny integritetspolicy som ska ersätta den från 26 mars 2021 tydligare beskrivit bolagets insatser avseende uppgiftsminimering och lagringsminimering, tillika vilka uppgifter som överförs till tredjeland såsom USA för olika ändamål. Det finns därmed inget att erinra mot i dessa delar.

12.14 Av Glookos integritetspolicy för enskilda användare[23] framgår att bolaget kan lämna ut information som samlas in från användare, inklusive hälsouppgifter, för att uppfylla ”*en rättslig förpliktelse som vi* är *ålagda eller för att vi ska kunna skydda intressen som är av grundläggande betydelse för dig eller någon annan fysisk person*.” Och vidare: ”*Vi kan även komma att lämna ut dina personuppgifter när så krävs för fastställande, verkställande eller försvar av rättsliga anspråk, oavsett om detta sker i domstol, i en förvaltningsdomstol eller utanför domstol*”. Samma besked lämnas däremot inte i Glookos standardiserade personuppgiftsbiträdesavtal med vårdgivare (februari 2022). Skyldigheten att bestrida tredjelandets myndigheter regleras i kommissionens SCC, klausul 15, oavsett modul (som inte har angetts av Glooko). SCC:n är bilagd Glookos personuppgiftsbiträdesavtal, men artikel 14 och 15 har angetts som inte tillämpliga. Av varken integritetspolicyn för enskilda användare eller personuppgiftsbiträdesavtalet

[20] Glookos integritetspolicy den 26 mars 2021.
[21] Punkt 4.4.
[22] Punkt 2:10.
[23] Glookos integritetspolicy den 26 mars 2021.

framgår om Glooko informerar användare om domstolar eller myndigheter som söker tillgång till dennes information.

12.15 Glooko har emellertid i ett utkast till integritetspolicy som ska ersätta den från 26 mars 2021 tydliggjort att såvida utländsk myndighet eller domstol begär att utfå uppgifter om en användare, bolaget kommer att underrätta användaren. Glooko har också låtit meddela att bolaget justerar sitt personuppgiftsbiträdesavtal på så sätt att kommissionens standardavtalsklausuler inte utgör del av huvudavtalet mellan vårdgivare och Glooko AB eftersom det inte sker några tredjelandsöverföringar från kunden (vårdgivare) till Glooko Inc. varför standardavtalsklausulerna har tagits bort från det uppdaterade personuppgiftsbiträdesavtalet. Däremot gör Glooko AB tredjelandsöverföringar av kundens personuppgifter, och ska följaktligen teckna kommissionens standardavtalsklausuler med bl.a. Glooko, Inc. i USA.

12.16 Glooko erinrar i integritetspolicyn för enskilda användare[24] att bolaget överför personuppgifter från det fasta driftsstället på Irland till USA. Däremot informerar inte Glooko om vilka risker detta medför för de registrerade, t.ex. att USA saknar dataskydd- eller sekretessförfattningar som motsvarar skyddet i dataskyddsförordningen och nationella integritetsbestämmelser inom EU/EES. Glooko framhåller dock i ett utkast till en ny integritetspolicy som ska ersätta den från 26 mars 2021 att bolaget vidtar tillämpliga ”säkerhetsåtgärder” med stöd av kommissionens SCC för att skydda användarnas personuppgifter och strukit Privacy Shield respektive Safe Harbour helt som överföringsmekanismer. Glooko informerar också i utkastet till ny integritetspolicy att kommissionen för närvarande inte har beviljat ett beslut om adekvat skyddsnivå på grund av att USA inte har dataskyddslagar för utlänningar som motsvarar skyddet i dataskyddsförordningen och nationella dataskyddsförordningar inom EU/EES.

12.17 I Glookos personuppgiftsbiträdesavtalet för vårdgivare[25] upplyser Glooko om följande: “*Den personuppgiftsansvarige samtycker till att, om personuppgiftsbiträdet [Glooko AB] anlitar en underleverantör i enlighet med klausul 7.7 för att utföra specifik behandling (för den personuppgiftsansvariges räkning) och denna behandling omfattar en överföring av personuppgifter i den mening som avses i kapitel V i förordning (EU) 2016/679, personuppgiftsbiträdet och underleverantören kan säkerställa att kapitel V i förordning (EU) 2016/679 efterlevs genom att använda standardavtalsklausuler som antagits av kommissionen i enlighet med artikel 46.2 i förordning (EU) 2016/679, förutsatt att villkoren för att använda dessa standardavtalsklausuler är uppfyllda*.”

12.18 Enligt Glookos integritetspolicy för enskilda användare[26] skyddas personuppgifter internt inom koncernen och vid tredjelandsöverföring av bindande företagsbestämmelser (Binding Corporate Rules). Sådana företagsbestämmelser godkänns av de nationella tillsynsmyndigheterna och EDPB. I det register som förs av EDPB över godkända bindande företagsbestämmelser finns inga registrerade bindande företagsbestämmelser

[24] Glookos integritetspolicy den 26 mars 2021.
[25] Glookos personuppgiftsbiträdesavtal (standardavtal) med vårdgivare februari 2022, klausul 7.8 Internationella överföringar.
[26] Glookos integritetspolicy den 26 mars 2021.

för vare sig Glooko AB eller Glooko, Inc.[27] Glooko har emellertid förklarat att Glooko själv använder inte bindande företagsbestämmelser samt presenterat ett utkast till integritetspolicy som ska ersätta den från 26 mars 2021 där det numera framgår att tredjelandsöverföringar inte genomförs av bolaget med stöd av bindande företagsbestämmelser. Glooko upplyser dock att bolagets tjänsteleverantörer själva kan använda bindande företagsbestämmelser som är korrekt registrerade hos EDPB, vilket återspeglas i den uppdaterade integritetspolicyn.

12.19 Enligt Glookos integritetspolicy för enskilda användare[28] används registrerades uppgifter för framtida forskning: ”*När vi får personuppgifter från dig kan vi komma att avidentifiera dessa uppgifter permanent och använda dem för statistisk analys, klinisk forskning, demografisk analys, profilering av användarbeteenden inom appen och it-egenskaper samt mäta intresset för och hanteringen av fysiska tillstånd och liknande behandling. Permanent avidentifierade uppgifter innehåller inga personuppgifter och kan därför inte spåras tillbaka till dig. Permanent avidentifierade uppgifter kan komma att exporteras till länder i eller utanför EU, USA eller andra områden. Inom USA kan både anonymisering med HIPAA ’Safe Harbor’ och tokenisering med hjälp av en expertbestämningsmetod användas för att anonymisera data. För personuppgifter som samlats in inom EES används GDPR-kompatibla anonymiseringsmetoder.”* Framställningen återkommer till frågan om forskning i avsnitt 15.

12.20 Enligt integritetspolicyn för enskilda användare använder Glooko kakor. Kakor används enligt Glooko för följande syften:

- autentisering – kakor för att identifiera användare vid besök på Glookos webbplats, vid navigering på webbplats och vid användning av Glookos tjänster
- status – för att avgöra huruvida användaren är inloggad på Glookos tjänster
- personlig anpassning – för att lagra information om preferenser och för att kunna anpassa webbplats och tjänster (t.ex. språkval)
- säkerhet – kakor som en del av säkerhetsåtgärder som används för att skydda användarkonton.
- analys – kakor som kan hjälpa Glooko att analysera användandet av webbplats och tjänster samt att de fungera som de ska
- samtycke till användning av kakor – kakor för att lagra användarens mer allmänna preferenser när det gäller användning av kakor.

12.21 Glooko informerar om att bolaget även använder tredjepartskakor, dvs. kakor som tillhandahålls och placeras i användarens dator eller app av en tredje part som anlitas av Glooko. Glooko använder Twilio Segment. Segment är en analystjänst. Den samlar in information om webbplatsanvändningen med hjälp av kakor. Den information som samlas in av Glooko med hjälp av Segment används för att skapa rapporter om användningen av webbplatsen. Glooko informerar i sin integritetspolicy för enskilda användare om att kakor kan regleras och begränsas i användarens webbläsare.

[27] https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_sv
[28] Glookos integritetspolicy den 26 mars 2021.

12.22 Det finns ingen information i Glookos kundavtal med vårdgivare inklusive personuppgiftsbiträdesavtal huruvida kakor används vid vårdgivares och deras medarbetares användning av Glookos tjänster. Det är en brist.

13 Tredjepartsapplikationer och tredjepartsleverantörer i Glooko-molnet

13.1 Som redovisas i avsnitt 12 driftas Glookos backend för Glooko-appen och Glooko-molnet (www.glooko.com) av det amerikanska bolaget Amazon Web Service (AWS). Som många andra amerikanska leverantörer erbjuder AWS lagring av data i Europa. När det gäller support m.m. tillhandahålls det av Glooko AB i Sverige och Glooko, Inc i USA.

13.2 Som också redovisas i avsnitt 12 överför Glooko både användares och hälso- och sjukvårdspersonals personuppgifter till bl.a. USA.. Såvitt kan utläsas av relevanta dokument överförs enskilda användares personuppgifter, både privatpersoners och hälso- och sjukvårdspersonals i både anonymiserad och identifierbar form, till bl.a. USA för ändamålen support, regulatoriska krav för medicintekniska produkter och framtida forskning. Någon absolut garanti för att européers personuppgifter stannar i Europa ges inte av Glooko.

13.3 Glooko anger i sitt personuppgiftsbiträdesavtal för vårdgivareavseende tjänsten Glooko-molnet att bolaget stödjer sin tredjelandsöverföring till USA av personuppgifter om verksamhet och personal på kommissionens standardavtalsklausuler (SCC). Beträffande tredjelandsöverföring av invånares personuppgifter till USA stödjer sig Glooko också här på SCC och inte på bestämmelserna om undantagssituationer i särskilda situationer i dataskyddsförordningen, artikel 49.

13.4 Lagring i AWS sker på bolagets datacenter i Dublin, Irland. AWS agerar här i rollen som personuppgiftsbiträde åt Glooko. Av AWS integritetspolicy[29] framgår bl.a. under rubriken ”Location of Personal Information” följande: “*Amazon Web Services, Inc. is located in the United States, and our affiliated companies are located throughout the world. Depending on the scope of your interactions with AWS Offerings, your personal information may be stored in or accessed from multiple countries, including the United States. Whenever we transfer personal information to other jurisdictions, we will ensure that the information is transferred in accordance with this Privacy Notice and as permitted by applicable data protection laws*.”

13.5 I AWS kan kunden, t.ex. Glooko, välja region där data ska tekniskt lagras.[30] AWS skriver: “*We will not move or replicate your content outside of your chosen AWS Region(s) without your consent, except in each case as necessary to comply with the law or a binding order of a governmental body*. AWS skriver vidare följande: “*We will not disclose customer content unless we're required to do so to comply with the law or a binding order of a government body. If a governmental body sends AWS a demand for*

[29] https://aws.amazon.com/privacy/
[30] https://aws.amazon.com/compliance/data-privacy-faq/?nc=sn&loc=4

customer content, we will attempt to redirect the governmental body to request that data directly from the customer. If compelled to disclose customer content to a government body, we will give customers reasonable notice of the demand to allow the customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so."

13.6 AWS informerar att tredjelandsöverföringen till USA inte sker med stöd av kommissionens beslut om skölden för privatlivet (Privacy Shield, se avsnitt 14). Under rubriken EU-US Privacy Shield anför AWS följande[31]: "*Since the Court of Justice of the European Union has validated the use of Standard Contractual Clauses (SCCs) as a mechanism for transferring data outside the European Union, our customers can continue to rely on the SCCs included in the AWS GDPR Data Processing Addendum if they choose to transfer their data outside the European Union in compliance with GDPR. The AWS GDPR Data Processing Addendum with Standard Contractual Clauses is part of the AWS Service Terms and is available automatically for all customers transferring personal data from the EU to any of the AWS regions around the world, including in the US*."

13.7 Glooko tillämpar enligt egen uppgift en Bring-Your-Own-Key-lösning (BYOK) i AWS.[32] Det innebär att personuppgifter krypteras och dekrypteras av AWS som förfogar över nyckeln i det specifika datacenter där Glooko driftas (Irland).

13.8 Glooko använder Twilio Segment och inloggnings-, funktions- och säkerhetsprogramvaror i sina appar och på www.glooko.com, vilka kräver kakor. Glooko använder även Zendesks tjänster. Applikationen Zendesk används för ärendehantering och kundsupport. I denna laglighetsprövning har valet fallit på att enbart granska Twilio Segment. Enligt Twilios integritetspolicy för Segment[33] samlas bl.a. följande information om användarna: klient, t.ex. PC eller mobil enhet, operativsystem, tillverkare och modell, webbläsare, IP- adress, "unika identifierare", och geografisk information såsom geografisk plats. Vidare användardata, såsom besökt webbsida före besök av aktuell webbsida, sidor som användaren tittat på, hur lång tid som spenderades på en särskild sida, navigationslänkar, inloggningstid och tid tagen i anspråk på webbplatsen.

13.9 Såvitt kunnat utrönas ansvarar Glooko ensam för inloggnings-, funktions- och säkerhetskakorna. Överföring av personuppgifter till USA genom Glookos egna kakor kan inte uteslutas. Twilio Segments kakor används för att föra statistik och göra analyser över användningen av tjänsten. Överföring av personuppgifter till USA eller till annat tredjeland via Glookos underleverantörer Twilio kan inte uteslutas.

14 Molntjänster och rättsläge

14.1 Molnbaserade tjänster har blivit allt vanligare, för både företag och privatpersoner. Bland nyttorna med molntjänster, jämfört med lokala installationer av programvara eller

[31] https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/
[32] Mejlkorrespondens med Glooko AB.
[33] https://segment.com/docs/legal/privacy/.

traditionell outsourcing, brukar framhållas flexibilitet och skalbarhet, kostnadseffektivitet, tillgänglighet och ökad säkerhet. Molntjänster kan också minska behovet av egen IT-personal eller viss spetskompetens.

14.2 Vid outsourcing måste ett flertal olika regelverk beaktas. Det gäller t.ex. sådana som rör offentlighet och sekretess, behandling av personuppgifter, arkivhantering, upphandling, informationssäkerhet och säkerhetsskydd samt upphovs- och avtalsrättsliga frågor. Behovet av säkerhetsskydd och informationssäkerhet är centralt.

14.3 Vid utkontraktering försvåras emellertid de rättsliga bedömningarna som en följd av t.ex. leverantörers komplexa affärsmodeller och en allt mer globaliserad marknad. Det gäller inte minst i fråga om kraven på hanteringen av sekretesskyddade uppgifter, t.ex. uppgifter inom hälso- och sjukvård, och bedömningen av när en uppgift ska anses röjd i offentlighets- och sekretesslagens mening. Samma sak gäller för hur det kan säkerställas att regelverket om dataskydd följs.

14.4 Röjandeproblematiken handlar om huruvida en myndighet, t.ex. vårdgivare, som anlitar en privat aktör (Glooko och dess underleverantörer) för hantering av vissa arbetsuppgifter som innefattar sekretessbelagda uppgifter, t.ex. uppgifter om patienter, har lämnat ut dem i juridisk mening, dvs. röjt dem. eSam – ett statligt myndighetsnätverk för dataskyddsfrågor - har i två rättsliga uttalanden bytt uppfattning från att det sannolikt inte sker ett röjande vid outsourcing till att det inte är osannolikt att ett röjande sker när utländska molntjänstleverantörer anlitas. I det senare fallet bygger eSam sin uppfattning på att utländska bolag kan omfattas av en extraterritoriell lagstiftning som innebär en skyldighet för leverantören att lämna ut kunduppgifter till brottsutredande och andra myndigheter med yppandeförbud mot kunden, dvs. myndigheten.

14.5 Ett exempel på sådan extraterritoriell lagstiftning är amerikanska US Cloud Act (Clarifying Lawful Overseas Use of Data Act) som kompletterar SCA (Stored Communications Act). Lagstiftning medger amerikanska myndigheter att under vissa förutsättningar begära hos domstol att privata tjänsteleverantörer som är underkastade amerikansk jurisdiktion ska bevara eller lämna ut uppgifter som är under tjänsteleverantörens kontroll utan att gå vägen via internationell rättshjälp, oavsett var leverantören bedriver sin verksamhet i världen, t.ex. Sverige. En begäran kan vidare beläggas med yppendeförbud för tjänsteleverantören, vilket innebär att leverantörens kund, en svensk myndighet, aldrig får kännedom om begäran.

14.6 Problematiken kan tyckas akademisk, men handlar om vad leverantören får göra med förvaltade uppgifter. Får leverantören disponera över svenska myndighetens uppgifter och överträda eventuella restriktioner i avtal för att hemlandets rättsordning lägger skyldigheter på leverantören som kan föranleda sanktioner om de inte följs? Om leverantörens hemland är ett tredjeland utgör utlämnandet ett brott mot förbudet i dataskyddsförordningen mot tredjelandsöverföring, om inget av undantagen i förordningen är uppfyllda.

14.7 De amerikanska rättsakterna FISA 702 och Executive Order 12333 innebär en rätt för underrättelsemyndigheter i USA att samla in underrättelser i bl.a. kommunikationslösningar som erbjuds allmänheten för ändamål som är relaterade till nationell säkerhet. Metoderna som får användas av amerikanska myndigheter i detta syfte är bl.a. avlyssning av kommunikation och tillgång till data som lagras i exempelvis molntjänster. FISA erbjuder vissa rättigheter för amerikanska medborgare, men inte för utländska. Utländska medborgare har således inga bindande rättigheter som kan göras gällande mot amerikanska myndigheter, vilket innebär att enskilda inte har någon rätt till effektiva rättsmedel vad gäller kontrollen av deras personuppgifter i USA.

14.8 En ytterligare dimension är skyddet för uppgifterna hos leverantören, oavsett om de är röjda eller inte. Känsligheten kvarstår, och rimligen kräver uppgifterna ett motsvarande straffsanktionerat skydd hos leverantören, likaväl som hos myndigheten. I Sverige finns idag en lagstadgad, straffsanktionerad tystnadsplikt för vård- och omsorgspersonal som kan rendera böter eller fängelse i upp till ett år. Tjänsteleverantörer verksamma i Sverige har sedan 1 januari 2021 också en lagstadgad, straffsanktionerad tystnadsplikt (se avsnitt 3.7) om de hanterar sekretessbelagda myndighetsuppgifter enligt uppdrag. Tystnadsplikten är begränsad till teknisk bearbetning och teknisk lagring.

14.9 För utländska tjänsteleverantörer med verksamhet utanför Sverige måste bristen på straffrättsligt skydd för sekretessbelagda personuppgifter kompenseras med att myndigheten träffar en avtalsreglerad tystnadsplikt med leverantören. Det är oklart dock huruvida en avtalad tystnadsplikt ”duger” som skydd för sekretessbelagda personuppgifter. Alternativt kan lagstiftningen i det land där leverantören bedriver sin verksamhet innehålla bestämmelser om tystnadsplikt för tjänsteleverantörer som sanktioneras med böter eller fängelse vid överträdelse. Sådan utländsk straffsanktionerad tystnadsplikt kan vägas in vid bedömningen om leverantören kan ge ”tillräckliga garantier för dataskydd” enligt artikel 28 i dataskyddsförordningen.

14.10 Dataskyddsförordningen tar i och för sig höjd för röjandeproblematiken genom att ställa krav på både personuppgiftsansvarig och personuppgiftsbiträde om skydd av personuppgifter, såsom krav på personuppgiftsbiträdesavtal med tydliga instruktioner till leverantören om vad denne får göra med uppgifter, krav på tystnadsplikt i avtal och krav på biträdet att skydda uppgifter och ge tillräckliga garantier för skyddet. Men offentlighets- och sekretessregleringen är en svensk företeelse, och det går inte att komma ifrån att myndigheter måste åtlyda bestämmelserna i regleringen och säkerställa den kontroll och det skydd för känsliga uppgifter som följer av exempelvis offentlighets- och sekretesslagen. Debatten handlar således om de ”instrument” som dataskyddsförordningen erbjuder räcker hela vägen för att skydda sekretessbelagda eller andra känsliga personuppgifter. Offentlighets- och sekretesslagen saknar nämligen hanteringsregler i termer av olika skyddsåtgärder. Den närmaste regleringen i det hänseendet finns i säkerhetsskyddslagen som avser skydd av uppgifter som rör Sveriges säkerhet och ligger utanför frågeställningarna i denna rättsutredning. Uppgifter som omfattas av säkerhetsskyddslagen innefattar sådana risker att de inte bör hanteras i en molntjänst. Utländska molntjänstleverantörer får som huvudregel inte heller anlitas enligt säkerhetsskyddslagen.

14.11 Man får alltid utgå från att sekretessbelagda eller andra känsliga uppgifter som lämnas ut till en leverantör av molntjänst får anses röjda. För att kunna röja sekretessbelagda uppgifter krävs en sekretessbrytande bestämmelse. Skulle en region finna att sekretess lägger hinder i vägen för att överlåta arbetsuppgifter till en leverantör som innefattar sekretessbelagda uppgifter återstår fem alternativ.

- Är leverantören ett svenskt bolag kan dennes anlitas av en myndighet såvida en menprövning ger vid handen att sekretessbelagda uppgifter kan lämnas ut till denna, vilket mycket talar för eftersom leverantören omfattas av en straffsanktionerad tystnadsplikt.

- Är leverantören utländsk men ett europeiskt bolag eller ett bolag verksamt i ett tredjeland som enligt beslut av kommissionen anses ha en adekvat skyddsnivå kan denne anlitas av en myndighet såvida en menprövning ger vid handen att sekretessbelagda uppgifter kan lämnas ut till denna; en straffsanktionerad tystnadsplikt för leverantörens medarbetare enligt hemlandets lagstiftning underlättar ett utlämnande.

- Omfattas leverantören av en extraterritoriell hemlandslagstiftning som omfattar verksamhet i Sverige och som innebär en skyldighet att lämna ut kundens (myndighetens) uppgifter till hemlandets myndigheter utan att behöva begära internationell rättshjälp gäller följande:

    - Det första alternativet är att inte anlita eller upphandla tjänsten.
    - Det andra alternativet är att myndigheten/kunden förfogar över en egen krypteringsnyckel för att ta del av och behandla personuppgifter hos leverantören och som leverantören inte har tillgång till (se EDPB:s rekommendationer om tredjelandsöverföring, bilaga 2, Användarfall nr 1[34]).
    - Det tredje alternativet är att ändå ta i anspråk molntjänsten därför att det inte finns några andra realistiska alternativ för myndigheten att bedriva sin verksamhet effektivt och acceptera riskerna som kan medföra vitessanktioner från tillsynsmyndighet och/eller skadeståndsanspråk från registrerade.

14.12 Offentlighets- och sekretesslagen innehåller en bestämmelse som tar i beaktande sådana situationer; en bestämmelse som bryter sekretessen. Enligt 10 kap. 2 § i lagen hindrar sekretess inte att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Syftet med bestämmelsen är att förhindra att sekretessregleringen gör det omöjligt för en myndighet och dess personal att sköta sina uppgifter, dvs. att fullgöra det uppdrag som följer av myndighetens instruktion, andra författningar, regleringsbrevet och särskilda regeringsbeslut.

[34] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021.

14.13 I sådant läge handlar molntjänster om vilken kontroll en myndighet kan utöva över uppgifterna och vilka tekniska och organisatoriska skyddsåtgärder som kan vidtas, utöver dataskyddsförordningens skyddsåtgärder i form av personuppgiftsbiträdesavtal och krav på tystnadspliktsavtal.

14.14 I syfte att klargöra statliga myndigheters, kommuners och regioners möjligheter att anlita leverantörer inom Sverige, inom EU och utanför EU har de rättsliga förutsättningarna för sådan utkontraktering kartlagts och analyserats av it-driftsutredningen (SOU 2021:1). It-driftsutredningen har bl.a. granskat frågor om överföring av personuppgifter till tredjeland. Enligt utredningen sker en tredjelandsöverföring när en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland (s. 228).

14.15 EU-domstolen har i Schrems II-domen uttalat att överföring av personuppgifter till ett tredjeland förutsätter att landet har en skyddsreglering som är i allt väsentligt likvärdig dataskyddsförordningen, och såvida sådan saknas lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda de registrerade fri- och rättigheter.

14.16 En lämplig skyddsåtgärd som står till buds är Kommissionens standardavtalsvillkor för tredjelandsöverföring i syfte att binda t.ex. leverantör att effektuera rättsmedel för registrerade motsvarande de som finns i dataskyddsförordningen. Sådana villkor omnämns i Glookos avtalsvillkor för vårdgivare, men refererar till äldre, upphävda standardavtalsvillkor.[35] Amerikanska myndigheter är emellertid inte bundna av standardavtalsvillkoren, vilket innebär en risk för otillåten behandling i strid med dataskyddsförordningen om uppgifter hamnar i myndigheternas förvar. En annan teknisk skyddsåtgärd skulle vara krypterad överföring och teknisk lagring där myndigheten, dvs. den personuppgiftsansvarige enbart förfogar över krypteringsnyckeln och inte tjänsteleverantören.

14.17 Kommissionen har i juni 2021 presenterat nya standardavtalsklausuler. Kravet kvarstår dock enligt Schrems II-domen för att kunna använda standardavtalsklausulerna att det tredjelandet har en skyddsreglering som är likvärdig dataskyddsförordningen, och såvida sådan saknas lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda de registrerade fri- och rättigheter.

14.18 När det gäller val av biträde framgår det av dataskyddsförordningen att om en behandling ska genomföras för en personuppgiftsansvarigs räkning ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger ”tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas” (artikel 28.1). Av skäl 81 i dataskyddsförordningen framgår att tillräckliga garantier ska ges i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser.

[35] Glookos användarvillkor för vårdgivare den 1 december 2020.

14.19 Integritetsskyddsmyndigheten har uttalat att en personuppgiftsansvarig måste följa de krav som ställs upp i artikel 28. Den personuppgiftsansvarige behöver därför ta ställning till vilka garantier i form av tekniska och organisatoriska åtgärder som krävs för att säkerställa att det inte sker en otillåten tredjelandsöverföring, till exempel hur man ska se till att personuppgiftsbiträdet inte lämnar ut uppgifter i strid med kapitel V i dataskyddsförordningen (överföring av personuppgifter till tredjeland). Om personuppgiftsansvarig inte i enlighet med artikel 28 kan få tillräckliga garantier från ett avsett personuppgiftsbiträde att inte överföra personuppgifter till tredjeland, kan denne inte anlita det personuppgiftsbiträdet.[36]

14.20 Den personuppgiftsansvarige har enligt it-driftsutredningen (SOU 2021:1) en omsorgsplikt vid val av biträde, som innefattar att göra en riskbedömning (s. 202). Omsorgsplikten innebär att den personuppgiftsansvarige behöver utreda vilka förutsättningar personuppgiftsbiträdet har att efterleva sina skyldigheter enligt dataskyddsregelverket. Eventuella skyldigheter som personuppgiftsbiträdet omfattas av enligt tredjelands lagstiftning att lämna ut personuppgifter till det landets myndigheter i strid med bestämmelserna om tredjelandsöverföring bör enligt it-driftsutredningen tas i beaktande vid bedömningen av om personuppgiftsbiträdet kan ge tillräckliga garantier.

14.21 Motsvarande bedömning ska göras av den personuppgiftsansvarige beträffande underleverantörer som personuppgiftsbiträdet anlitar. Dataskyddsförordningen förutsätter att den personuppgiftsansvarige godkänner underbiträden (artikel 28:2). Det finns två förfaranden: allmänt och särskilt förhandhandstillstånd

14.22 Som framhållits inledningsvis är kontroll en viktig faktor i sammanhanget. Den personuppgiftsansvarige måste kunna ha kontroll över ett personuppgiftsbiträdes behandling av uppgifterna för att tillse att behandling är korrekt och säker. Även möjligheten att ha en sådan kontroll måste bedömas utifrån vilka krav som kan ställas på företaget i nationell lagstiftning.

14.23 Kravet på kontroll gäller även beträffande reglerna i Sverige om sekretess och tystnadsplikt. Det är viktigt att den myndighet som ansvarar för sekretessbelagt material gör en bedömning av vad som krävs utifrån de reglerna för att någon annan ska få behandla uppgifterna. Problemet är, som nämnts, att den utländska leverantörens lagstiftning kan ge myndigheter större befogenheter än svenska att få ta del av uppgifter. Vidare kan det vara svårt för en svensk myndighet eller ett svenskt företag att ha en faktisk kontroll över sekretessbelagda uppgifter som hanteras helt eller delvis av en utländsk aktör. En svensk åklagare kan dessutom få svårigheter att åtala en utländsk leverantörs personal som obehörigen röjt eller missbrukat känsliga personuppgifter, t.ex. patientuppgifter. Missbruket eller röjandet kanske inte ens enligt den utländska leverantörens lagstiftning är straffbart. Det är omständigheter som en myndighet måste väga in i sin skadeprövning när utländska molntjänstleverantörer övervägs i verksamheten.

[36] IMY, Förhandssamråd om Azure AD och Teams, 2 juni 2021, dnr DI-2021-1513.

15 Har personuppgifter i Glooko-appen Glooko-molnet ett godtagbart skydd?

Bedömning: Glookos molntjänst Glooko används av enskilda användare och vårdgivare för att ladda upp och dela glukosdata från mer än 190 olika glukosmätare, insulinpumpar, CGM-system och aktivitetsmätare. Tjänsten inklusive app kan användas för flera ändamål, såsom hälso- och sjukvård enligt hälso- och sjukvårdslagen, egenvård och för rent konsumentbruk (självhjälp).

Glooko, Inc är ett amerikanskt bolag. Bolaget har ett fast verksamhetsställe i Sverige genom Glooko AB. Avtalspart för Glookos tjänster i Sverige och inom EU/EES är emellertid Glooko AB i Sverige. Drift av Glookos data sker på Irland. I Glookos fall överförs personuppgifter i både identifierbar och anonymiserad form till USA för bl.a. ändamålen teknisk support, kvalitets- och säkerhetsövervakning av medicintekniska produkter (myndigheter) och framtida forskning (Glooko, Inc). Överföringen är reglerad i Glooko AB:s villkor för molntjänsten Glooko, både i villkoren för enskilda privata användare respektive vårdgivare.

Glooko AB anlitar underleverantören Amazon Web Services (AWS) för applikationsförvaltning och lagring av hälsorelaterade personuppgifter i Glooko-appen och Glooko-molnet. Lagring av data sker på Irland. Glooko AB anlitar dessutom, såvitt är känt, underleverantörerna Twilio, Inc. respektive Zendesk i USA. Lagring av den analysdata som Twilio samlar in sker i USA. Zendesk lagrar data på uppdrag av Glooko i både EU och USA. I denna laglighetsprövning har valet fallit på att enbart granska Twilio, Inc.

Glooko, AWS och Twilio är emellertid amerikanska företag som, såvitt kan bedömas, enligt avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Glookos, AWS och Twilios avtal innehåller bl.a. ansvarsfriskrivningar för det fallet att de skulle tvingas av amerikansk myndighet eller domstol att lämna ut uppgifter enligt bl.a. FISA 702 eller Cloud Act. Det finns således en risk, trots organisatoriska och tekniska åtgärder från Glookos sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av Glookos kunduppgifter genom Glooko eller Twilio får dock betraktas som mycket låg med hänsyn till Glookos kärnverksamhet (diabetesmonitorering). Det finns andra risker, t.ex. cyberattacker mot molntjänster, som får betraktas som högre och mer allvarliga.

Glooko uppger inte i sin integritetspolicy för enskilda användare[37] på vad sätt bolagets leverantörer av tredjepartstjänster i tredjeländer uppfyller dataskydds- och säkerhetsbestämmelser enligt dataskyddsförordningen. Glooko har inte heller i sin integritetspolicy uttömmande beskrivit till vilka tredjeländer man överför användarens

[37] Glookos integritetspolicy den 26 mars 2021.

uppgifter, till vilka mottagare eller kategorier av mottagare, på vilken rättslig grund och på vilket sätt dessa länder brister i sitt, t.ex. att utlänningar i USA saknar rättsliga och effektiva möjligheter att utöva kontroll över sina personuppgifter som är förvarade hos myndigheter.. Det har förvisso inte föreskrivits i dataskyddsförordningen något visst innehåll i informationen till den registrerade om riskerna med tredjelandsöverföring baserad på standardavtalsvillkor, men enligt artikel 12.1 i dataskyddsförordningen ska informationen till den registrerade i samband med insamling av personuppgifter vara i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Som minimum ska anges i informationen till registrerade om tredjeländernas namn liksom kategorier av mottagare. Det är oklart, bortsett från Glooko AB, AWS, Cegedom SA (franska användare) och Twilio, vilka andra aktörer Glooko delar registrerades ”personuppgifter” med. Glooko har emellertid presenterat ett utkast till en ny integritetspolicy för enskilda användare som ska ersätta integritetspolicyn av den 26 mars 2021 och där bolaget på ett tydligare sätt anger att den avser att överföra personuppgifter till ett tredjeland och hänvisar till rättsliga grunder och lämpliga skyddsåtgärder för överföringen inklusive länkar till överföringsmekanismerna. Glooko informerar vidare om att USA saknar ett dataskydd motsvarande dataskyddsförordningen. Glooko redovisar dock alltjämt inte som minimikrav till vilka länder användares personuppgifter överförs eller kategorier av mottagare. Denna brist på information om tredjelandsöverföringen bedöms alltjämt innebära en hög risk för registrerades fri- och rättigheter.

I Glookos personuppgiftsbiträdesavtal med vårdgivare, benämnd ”Standardavtal” (februari 2022), informeras om att Glooko använder kommissionens standardavtalsklausuler från 2021 för tredjelandsöverföring. Emellertid saknar personuppgiftsbiträdesavtalet tydliga dokumenterade instruktioner från vårdgivaren till Glooko och bolagets underbiträden om för vilka ändamål bolaget får behandla vårdgivarens patientuppgifter, såsom för teknisk support, regulatoriska krav, tillhandhållande av tjänsten, teknisk support, produktutveckling och mycket mer. Vidare har Glooko uteslutit klausulerna 14 (Local laws and practices affecting compliance with the Clauses) och 15 (Obligations of the data importer in case of access by public authorities), genom att ange att dessa inte är tillämpbara. Tvärtom är dessa klausuler centrala för personuppgiftsbiträdens eller underbiträdens agerande och transparens vid tredjelands myndigheters begäran om utfående av uppgifter av en svensk vårdgivare. Att utesluta klausulerna 14 och 15 i SCC:n är en allvarlig brist i skyddet av enskilda patienters och vårdgivares medarbetares personuppgifter vid tredjelandsöverföring. Bristen innebär en hög risk för enskildas fri- och rättigheter.. Glooko har emellertid låtit meddela att exkluderingen av klausulerna 14 och 15 i SCC:n är ett fel från deras sida. Glooko har också meddelat att bolaget justerar sitt personuppgiftsbiträdesavtal på så sätt att kommissionens standardavtalsklausuler inte utgör del av huvudavtalet mellan vårdgivare och Glooko AB eftersom det inte sker några internationella överföringar från kunden till Glooko Inc. varför standardavtalsklausulerna

har tagits bort från det uppdaterade personuppgiftsbiträdesavtalet. Tredjelandsöverföringar sker i stället av Glooko AB till Glooko, Inc.

Glooko har även tydliggjort i sitt personuppgiftsbiträdesavtal med svenska vårdgivare för vilka ändamål bolaget får behandla personuppgifter åt vårdgivare i rollen som personuppgiftsbiträde. Klargörandet innebär att svenska vårdgivare kan lämna klar och koncis information till sina medarbetare om för vilka ändamål Glooko behandlar deras personuppgifter och i vilken utsträckning tredjelandsöverföring sker av dessa.

Det framgår inte heller av Glookos integritetspolicy för enskilda användare i vilken utsträckning Glooko AB i rollen som personuppgiftsansvarig tillämpar eller beaktar principerna om uppgiftsminimering eller lagringsminimering enligt artikel 5.1 i dataskyddsförordningen vid vidareanvändning och delning med andra aktörer av personuppgifter. I vissa fall delar Glooko endast krypterade uppgifter om användare med sina underleverantörer, såsom tjänsterelaterade uppgifter. I andra fall delas personuppgifter med leverantörer och myndigheter, t.ex. för ändamålen teknisk support och regulatoriska krav, men oklart i vilken omfattning. Det hade varit önskvärt med en tydligare beskrivning i dessa delar vad för slags information Glooko och dess underleverantörer tar del av och i vilken utsträckning man strävar efter pseudonymisering. Glooko har emellertid presenterat ett utkast till ny integritetspolicy som ska ersätta den från 26 mars 2021. Av denna framgår tydligare bolagets insatser avseende uppgiftsminimering och lagringsminimering, tillika vilka uppgifter som överförs till tredjeland såsom USA för olika ändamål. Det finns därmed inget att erinra mot i dessa delar.

Glookos integritetspolicy för enskilda användare och Glookos kundavtal inklusive personuppgiftsbiträdesavtal vidlåder också andra brister i informationshänseende vad gäller registrerade. Av integritetspolicyn för enskilda användare framgår exempelvis inte att en vårdgivare är personuppgiftsansvarig för de personuppgifter som en enskild individ tillgängliggör via direktåtkomst och som vårdgivaren behandlar i sitt Glooko klinik-konto. Det är synnerligen viktigt att en patient är medveten om att kliniskt ansvarig vårdgivare är personuppgiftsansvarig för de uppgifter en enskild användare överför till dennes klinik-konto och att Glooko inte är personuppgiftsansvarig för dessa. Glooko har emellertid i ett utkast till integritetspolicy som ska ersätta den från 26 mars 2021 tydliggjort vårdgivares personuppgiftsansvar vid överföring av uppgifter i användarens Glooko-konto till vårdgivaren och att Glooko inte längre är personuppgiftsansvarig för den behandlingen.

Av integritetspolicyn för enskilda användare framgår vidare inte huruvida Glooko informerar registrerade om myndigheter eller domstolar som söker tillgång till deras personuppgifter, och vilka risker registrerade löper i integritetshänseende vid Glookos tredjelandsöverföring av personuppgifter till länder som saknar en motsvarighet till dataskyddsförordningen. Glooko har emellertid i ett utkast till integritetspolicy som ska

ersätta den från 26 mars 2021 tydliggjort att såvida utländsk myndighet eller domstol begär att utfå uppgifter om en användare, bolaget kommer att underrätta användaren.

Det finns också information i integritetspolicyn för enskilda användare om skyddsåtgärder som inte verkar vara korrekta, såsom att Privacy Shield är ett instrument för en säker tredjelandsöverföring, trots att EU-domstolen ogiltigförklarat den överenskommelsen i Schrems II-domen, och att godkända bindande företagsbestämmelser existerar för Glooko, trots att så inte är fallet enligt EDPB:s register över godkända bindande företagsbestämmelser. Glooko har låtit meddela att bolaget avser att justera integritetspolicyn av den 26 mars 2021 så att det inte längre framgår några hänvisningar till att Glooko använder Privacy Shield som ett instrument för att överföra personuppgifter till ett tredjeland. Glooko har också i ett utkast till ny integritetspolicy som ska ersätta den nuvarande från 26 mars 2021 inkluderat länkar till kommissionens nuvarande godkända standardavtalsklausuler. Vidare har Glooko låtit meddela att Glooko själv inte använder bindande företagsbestämmelser samt förklarat att i utkastet till integritetspolicy som ska ersätta den från 26 mars 2021 framgår det numera att tredjelandsöverföringar inte genomförs av bolaget med stöd av bindande företagsbestämmelser. Glooko upplyser dock att bolagets tjänsteleverantörer själva kan använda bindande företagsbestämmelser som är korrekt registrerade hos EDPB, vilket återspeglas i den uppdaterade integritetspolicyn.

Samma brister om information till vårdgivare om att myndigheter i tredjeländer söker tillgång till vårdgivarnas uppgifter om patienter eller medarbetare i Glooko-molnet noteras också i Glookos kundavtal inklusive personuppgiftsbiträdesavtal för vårdgivare. Skyldigheten att bestrida tredjelandets myndigheter regleras i kommissionens standardavtalsklausuler från 2021 (SCC), klausul 15, oavsett modul (som inte har angetts av Glooko). SCC:n är bilagd Glookos personuppgiftsbiträdesavtal, men artikel 14 och 15 har angetts som inte tillämpliga. Som framhållits har Glooko låtit meddela att bolaget justerar sitt personuppgiftsbiträdesavtal på så sätt att kommissionens standardavtalsklausuler inte utgör del av huvudavtalet mellan vårdgivare och Glooko AB eftersom det inte sker några tredjelandsöverföringar från kunden (vårdgivare) till Glooko Inc. varför standardavtalsklausulerna har tagits bort från det uppdaterade personuppgiftsbiträdesavtalet. Det är en korrekt åtgärd.

Informationen i Glookos nuvarande integritetspolicy för enskilda privatpersoner respektive Glookos nuvarande personuppgiftsbiträdesavtal för vårdgivare samt annan dokumentation når inte helt upp till kravet på koncis, klar, tydlig och begriplig information till registrerade enligt artikel 12.1 i dataskyddsförordningen. Informationen bryter därmed också mot principen om öppenhet i artikel 5.1 i samma förordning. Bl.a framgår det inte till vilka tredjeländer Glooko överför enskilda privata användares personuppgifter, liksom namngivna mottagare eller kategorier av mottagare. Denna brist i informationsskyldigheten enligt dataskyddsförordningen och principen om öppenhet bedöms innebära en hög risk för enskildas fri- och rättigheter eftersom registrerade i

Glookos tjänster, både enskilda som medarbetare hos vårdgivare, inte kan utöva sina rättigheter på ett effektivt sätt. Alla brister har emellertid åtgärdats av Glooko genom presenterade utkast till ny integritetspolicy. Mot bakgrund av de kompletteringar Glooko presenterat under laglighetsprövningen bedöms sammanfattningsvis informationen i Glookos integritetspolicy för enskilda privatpersoner nå upp till kravet på koncis, klar, tydlig och begriplig information till registrerade enligt artikel 12.1 i dataskyddsförordningen. Adekvata tydliggöranden har också gjorts i ett utkast till nytt personuppgiftsbiträdesavtal med svenska vårdgivare.

Glookos lösning för datadelning mellan invånare och vårdgivare är närmast att betrakta som egenvård enligt Socialstyrelsens egenvårdsföreskrifter, och inte distanssjukvård, och där vårdgivaren är personuppgiftsansvarig enbart för den uppföljning som sker av data inom ramen för egenvårdsbeslutet som den enskilde personen har godkänt får automatiskt lämnas ut till vårdgivarens lagringsyta i Glooko när denne efterfrågar uppgifterna. Glooko är personuppgiftsansvarig för den enskilda individens användarkonto och lämnar ut uppgifterna till vårdgivare enligt samtycke från användaren. För att en vårdgivare ska kunna bedriva hälso- och sjukvård per definition enligt hälso- och sjukvårdslagen, alltså distanssjukvård, genom Glooko-molnet, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att andra tillverkares produkter kopplas direkt till vårdgivarens klinik-konto i Glooko eller att vårdgivaren skapar egna hälsokonton och tillhandahåller användaruppgifter åt enskilda individer i Glooko. Så är inte fallet nu med undantag för vårdgivare som laddar upp glukosdata till sin dator via Glookos transmitter vid ett vårdbesök av en patient.

Den av Glooko valda juridiska lösningen för Glooko-molnet ger upphov till otydliga ansvarsförhållanden för personuppgiftsbehandlingen när en vårdgivare vid en egenvård får direktåtkomst till en enskild persons hälsokonto, som den enskilde skapat själv. Det är inte uteslutet att vårdgivaren i det läget anses personuppgiftsansvarig för alla data i kontot, även sådana som invånaren registrerat utan inblandning av en vårdgivare för att monitorera sin diabetes, trots löfte från Glooko om det motsatta. Det är i sådant fall inte Glooko som är personuppgiftsansvarig för den enskilda individens användarkontot utan en vårdgivare.

Rättsläget är emellertid oklart. Genom tydligare information i avtalsvillkoren för enskilda användare respektive vårdgivare torde Glooko kunna reducera väsentligen de risker som föreligger för registrerade vid ett otydligt personuppgiftsansvar på beskrivet sätt. Det är inte uteslutet att det finns ett visst ”spelrum” i brist på vägledning i lagstiftningen för både Glooko och vårdgivare att reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke. Ett annat alternativ som ska ses som en rekommendation är att Glooko överväger en lösning i framtiden som innebär att vårdgivare inte får direktåtkomst till enskildas Glooko-konton vid distanssjukvård utan i stället skapa en lösning med två logiskt eller t.o.m. fysiskt separerade lagringslösningar –

en för vårdgivare respektive en för patienter – i Glooko-molnet för att åstadkomma en tydlig ”separation of duties”. Glooko bör eftersträva att utlämnande mellan patientens lagringslösning (konto) och vårdgivarens sker genom s.k. ADB-utlämnande, dvs. filöverföring, t.ex. via API:er där data efterfrågas och lämnas ut mellan kontona. Patienter däremot får enligt patientdatalagen ha direktåtkomst till en vårdgivares vårddokumentation, om vårdgivaren så tillåter, dvs. en direktåtkomst från sitt användarkonto i Glooko till vårdgivarens klinikkonto i Glooko-molnet

Beträffande vårdgivares inloggning till sitt klinik-konto på Glooko-molnet lever Glooko upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Det är dock inte en standardfunktion i tjänsten utan aktiveras på vårdgivares begäran. Glooko rekommenderas att alltid ha stark autentisering aktiverad så att vårdgivare inte gör sig skyldighet till brott mot regelverket. Beträffande sedan en enskild persons inloggning till sitt konto på www.glooko.com lever Glooko inte upp till kraven på stark autentisering. Beträffande slutligen Glooko-appen omfattas dessa förvisso inte av Socialstyrelsens föreskrifter. Något krav på stark autentisering i författning finns inte. Rekommendationen är dock att enskilds inloggning till hälsodata i apparna bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i Glooko-molnet ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.

En vårdgivare kan skicka en inbjudan och delningskod till patienter via e-post. En inbjudan i klartext om att dela glukosdata med en vårdgivare i Glooko utgör inte en kallelse eller påminnelse till vård- och behandling enligt Socialstyrelsens föreskrifter. Att dessutom skicka en delningskod via e-post i ett öppet nät innebär stora risker för obehörigt röjande av delningskoden, och därmed hälsorelaterade uppgifter, med en tredje part. Användning av e-post för att skicka en delningskod med en patient är i strid med Socialstyrelsens föreskrifter och en otillåten behandling av personuppgifter. Det är vårdgivaren i rollen som personuppgiftsansvarig som gör sig skyldig till den otillåtna behandlingen av personuppgifter. Å andra sidan bär Glooko i rollen som personuppgiftsbiträde och tjänsteleverantör ett ansvar för att ge ”tillräckliga garantier” för skyddet av personuppgifter och registrerades fri- och rättigheter i sina tjänster och produkter. Att funktionen är frivillig för vårdgivaren att använda ”släcker” inte de krav på skydd och säkerhet som ställs på personuppgiftsbiträden i dataskyddsförordningen. Glooko rekommenderas att åtminstone informera vårdgivare om riskerna med att använda funktionen eller att lämna delningskoden till patienten vid ett personligt besök på kliniken eller i inloggat läge i avvaktan på en säkrar lösning för delning, t.ex. sms eller push-notis i den mobila enheten om att användaren har ett meddelande från en vårdgivare som denne tar del av i inloggat läge i appen. Glooko har låtit meddela att man utvärderar potentiell användning av 1177 och andra meddelandetjänster för att göra andra lösningar tillgängliga för svenska vårdgivare i syfte att bjuda in patienter att aktivera sina konton.

I Glooko kan en användare välja att samtycka till framtida forskning. Behandlingen har bedömts utgöra en otillåten behandling eftersom ändamålet inte är tillräckligt preciserat. Det saknar betydelse att det rör sig om oidentifierbara uppgifter eftersom framtagandet av anonymiserade uppgifter kräver en behandling av individbaserade personuppgifter för det specifika ändamålet. Erbjudandet till enskilda användare om att dela sina data för framtida forskning bör avskaffas. Glooko har låtit meddela att begreppet ”forskning” egentligen avser aggregerad statistisk analys och andra analyser, t.ex. användarbeteende och ”fysiska tillstånd”, som är nödvändiga för bolagets affärsverksamhet. Glooko har presenterat ett utkast till en ny integritetspolicy för enskilda användare som ska ersätta integritetspolicyn av den 26 mars 2021 och där alla hänvisningar till ordet "forskning" har tagits bort. Den rättsliga grunden är alltjämt ett frivilligt samtycke. Ändamålen får anses tillräckligt specificerade. Behandlingen bedöms därför utgöra en tillåten behandling.

15.1 Föreliggande laglighetsprövningen av Glooko-appen och Glooko-molnet är enligt uppdrag avgränsad till själva behandlingen och skyddet av personuppgifter i appen och tredjepartsapplikationer. Uppdraget är att redovisa om personuppgiftsbehandlingen i produkten är förenlig med gällande rätt.

15.2 Som konstaterats har vårdgivare en rätt att behandla personuppgifter, inklusive känsliga sådana, för distanssjukvård samt egenvårdsbedömningar och egenvårdsuppföljningar, såvida de grundläggande dataskyddsprinciperna i dataskyddsförordningen (artikel 5.1) är iakttagna, såsom principen om korrekthet, öppenhet och uppgiftsminimering.

15.3 En ytterligare dataskyddsprincip är principen om integritet och konfidentialitet (artikel 5.1 f). Enligt principen ska personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet). Principen relaterar till ett flertal artiklar i förordningen som berör skydd av personuppgifter, bl.a. artikel 32 (skyddsåtgärder), artikel 28 (anlitande av personuppgiftsbiträden), och även artiklarna 44 – 50 om tredjelandsöverföring. Den personuppgiftsansvarige ska ansvara för och kunna visa att principen (liksom övriga dataskyddsprinciper) efterlevs, s.k. ansvarsskyldighet (artikel 5.2).

15.4 Glookos molntjänst Glooko används av enskilda användare och vårdgivare för att ladda upp och dela glukosdata från mer än 190 olika glukosmätare, insulinpumpar, CGM-system och aktivitetsmätare. Tjänsten inklusive app kan användas för flera ändamål, såsom hälso- och sjukvård enligt hälso- och sjukvårdslagen, egenvård och för rent konsumentbruk (självhjälp).

15.5 Glooko, Inc är ett amerikanskt bolag. Bolaget har ett fast verksamhetsställe i Sverige genom Glooko AB. Avtalspart för Glookos tjänster i Sverige och inom EU/EES är

emellertid Glooko AB i Sverige. I rollen både som personuppgiftsansvarig, vilken roll Glooko AB (Glooko om inte annat specificeras) har beträffande behandling av personuppgifter i konsumentförhållanden (självhjälp) respektive egenvård, och personuppgiftsbiträde åt vårdgivare, är dataskyddsförordningen tillämplig på personuppgiftsbehandlingen i Glooko tjänster och appar enligt artikel 3.2 a i dataskyddsförordningen eftersom bolaget utbjuder varor och tjänster till enskilda inom unionen, oavsett om bolaget inte är etablerat i unionen.

15.6 Det s.k. privatundantaget i artikel 2.2 c i dataskyddsförordningen bedöms inte vara tillämplig i konsumentfallet eftersom Glooko använder konsumentens personuppgifter för egna ändamål, t.ex. för att utveckla tjänsten och rapportera avvikelser i produkterna till tillsynsmyndigheter, eller möjliggöra för användaren att dela sina uppgifter med andra, t.ex. anhöriga och vårdgivare. Glooko är därmed personuppgiftsansvarig för all behandling av konsumentens personuppgifter i produkterna. Dataskyddsförordningen är tillämplig på den personuppgiftsbehandlingen av det skälet.

15.7 Det erinras att vad gäller bestämmelserna om tredjelandsöverföring ska de beaktas av både personuppgiftsansvariga och personuppgiftsbiträden.

Tystnadsplikt

15.8 Personalen verksamma i Glooko AB i Sverige omfattas av en lagreglerad och straffsanktionerad tystnadsplikt enligt lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. Det innebär ett godtagbart skydd av hälsorelaterade personuppgifter som hanteras av Glooko AB. Medarbetare hos Glooko, Inc. i USA omfattas däremot inte av en lagreglerad och straffsanktionerad tystnadsplikt enligt lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. Lagen gäller i praktiken bara för aktörer vars medarbetare är fysiskt verksamma i Sverige. Tystnadsplikt för bolagen och dess medarbetare måste i stället avtalsregleras. En sådan avtalad tystnadsplikt finns reglerad i både Glookos integritetspolicy för enskilda användare av Glooko-appen och Glooko-molnet, liksom i Glookos standardiserade personuppgiftsbiträdesavtal för vårdgivare och dess medarbetare som använder Glooko-molnet.[38]

15.9 Glooko har för övrigt uppgivit att alla Glooko-anställda är skyldiga att underteckna sekretessavtal vid anställning. Alla Glooko-anställda är vidare föremål för utbildning för att respektera Glookos säkerhets- och integritetsskyldigheter. Endast de Glooko-anställda som har fått specialiserad utbildning och chefs godkännande har tillåtelse att få tillgång till system som innehåller personuppgifter. Alla anställda hos Glooko som bryter mot gällande policyer är föremål för disciplinära åtgärder, vilket även kan innebära uppsägning av anställning. Det innebär generellt sett att kunduppgifter, inklusive hälsorelaterade personuppgifter, får anses ha ett tämligen starkt skydd hos Glooko i tystnadspliktshänseende.

[38] Glookos integritetspolicy den 26 mars 2021 och Glookos användarvillkor för vårdgivare den 1 december 2020.

15.10 Glooko anlitar underleverantören Amazon Web Services (AWS) för applikationsförvaltning och lagring av hälsorelaterade personuppgifter i Glooko-appen och Glooko-molnet. Lagring av data sker på Irland. Lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter är inte tillämplig heller på AWS eftersom data förvaltas i annat land än Sverige.

15.11 På Irland kompletteras dataskyddsförordningens av en nationell dataskyddslag, Data Protection Act 2018. Enligt 144 § kan enskilda medarbetare hos ett personuppgiftsbiträde som röjt eller lämnat ut personuppgifter till en tredje person utan godkännande av den personuppgiftsansvarige dömas upp till fem års fängelse eller 50.000 euro i böter. Det finns således en straffsanktionerad individuell tystnadsplikt på Irland för anställda hos molntjänstleverantörer som har verksamhet i det landet. I Sverige renderar brott mot en lagstadgad tystnadsplikt upp till ett års fängelse, vilket är ett lägre straff än den irländska straffpåföljden. Irland får därmed anses har ett fullgott skydd mot obehörigt röjande av personuppgifter hos personuppgiftsbiträden verksamma på Irland. I detta fall AWS personal på Irland.

15.12 Glooko AB anlitar, såvitt är känt, underleverantörerna Twilio, Inc i respektive Zendesk i USA. Lagring av den analysdata som Twilio samlar in sker i USA.[39] Zendesk är en molnbaserad applikation för support och ärendehantering. Zendesk lagrar personuppgifter på uppdrag av Glooko i både EU och USA. I denna laglighetsprövning har valet fallit på att enbart granska Twilio Segment. Lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter är inte tillämplig på Twilio, Inc. eftersom data förvaltas i annat land än Sverige. I USA finns inte, såvitt är känt, en straffsanktionerad tystnadsplikt specifikt för personuppgiftsbiträden som ska motverka obehörigt röjande av kunddata. Avtalsreglerad tystnadsplikt finns i avtalen med både enskilda användare och vårdgivare, men innebär ett svagare skydd, åtminstone för identifierbara personuppgifter. Det innebär att när en vårdgivare använder Glookos tjänster för att bedriva hälso- och sjukvård eller egenvård, enskilda individers hälsorelaterade uppgifter har ett svagare skydd vid förvar hos underbiträdet Twilio än när de är fysiskt förvarade hos en svenska vårdgivare.

Information till registrerade om personuppgiftsbehandlingen

15.13 Av Glookos integritetspolicy för enskilda användare av Glooko-molnet[40] framgår att om användaren begär support av Glooko och delar sina felsökningsuppgifter (däribland frågeuppgifter, tjänsterelaterade uppgifter och korrespondensuppgifter), överförs dessa uppgifter till USA i den mån det är nödvändigt för att bolaget ska kunna ge teknisk support och utföra bredare analys för att upptäcka systemproblem och den lokala supporten i Sverige inte kan lösa frågan. Vem eller vilka som är ansvariga för supporten i USA är dock oklart. Glooko har emellertid presenterat ett utkast till ny integritetspolicy som ska ersätta den från 26 mars 2021 och som tydligare beskriver vem eller vilka som är ansvariga för supporten i USA. Det finns därmed inget att erinra mot i dessa delar.

[39] https://segment.com/legal/privacy/
[40] Glookos integritetspolicy den 26 mars 2021.

15.14 Av integritetspolicy för enskilda användare[41] framgår vidare att bolaget delar personuppgifter med ett flertal tjänsteleverantörer: ”*Vi använder tjänsteleverantörer för leverans av olika delar av tjänsterna. Vissa av dessa tjänsteleverantörer finns utanför EES. Eventuella internationella överföringar av personuppgifter skyddas av tillämpliga säkerhetsåtgärder, nämligen användning av standardiserade kontraktsbestämmelser som har antagits eller godkänts av Europeiska kommissionen, ett beslut om adekvat skydd från Europeiska kommissionen eller bindande företagsregler eller ditt uttryckta samtycke*.” Det är emellertid oklart, bortsett från dotterbolaget Glooko AB i Sverige, AWS, Cegedim SA (franska användare), Twilio och Zendesk, vilka andra aktörer Glooko delar registrerades ”personuppgifter” med.

15.15 Det framgår inte heller med all önskvärd tydlighet i vilken utsträckning Glooko tillämpar principerna om uppgiftsminimering eller lagringsminimering enligt artikel 5.1 i dataskyddsförordningen vid delning av personuppgifter med andra aktörer och myndigheter. Av Glookos integritetspolicy för enskilda användare[42] framgår å ena sidan att Glooko kan komma att lämna ut registrerades ”personuppgifter” till sina leverantörer eller underentreprenörer i den mån det rimligtvis krävs för att kunna tillhandahålla tjänsterna. ”Tjänsterelaterade uppgifter”, såsom namn, e-postadress, kön, födelsedatum, biometriska uppgifter och medicinsk information samt andra typer av inlämnad eller uppladdad information, omfattas dock enligt Glooko av ytterligare restriktioner och får inte lämnas ut till någon sådan tredjepartsleverantör om de inte först har avidentifierats, dvs. krypterats med en säkerhetsnyckel.[43] Glooko tillämpar i Glooko-molnet en s.k. Bring-Your-Own-Key-lösning (BYOK).

15.16 Å andra sidan framgår det av integritetspolicyn för enskilda användare att ”tjänsterelaterade uppgifter” och användningsuppgifter används av Glooko och dess underleverantörer när användare begär teknisk support för att kunna diagnostisera ett problem.[44] Det hade varit önskvärt med en tydligare beskrivning vad för slags information Glooko och dess underleverantörer tar del av i dessa lägen och i vilken utsträckning man strävar efter pseudonymisering. Samma oklarheter om vilka uppgifter som används av Glooko och i vilken utsträckning de pseudonymiseras eller anonymiseras råder vid behandling av registrerades personuppgifter för andra ändamål, såsom t.ex. regulatoriska krav. Glooko har emellertid presenterat ett utkast till ny integritetspolicy som ska ersätta den från 26 mars 2021 och som tydligare beskriver bolagets insatser avseende uppgiftsminimering och lagringsminimering, tillika vilka uppgifter som överförs till tredjeland såsom USA för olika ändamål. Det finns därmed inget att erinra mot i dessa delar.

15.17 Det saknas även information i Glookos integritetspolicy för enskilda användare[45] och på Glookos supportsida om att en vårdgivare är personuppgiftsansvarig för de

[41] Glookos integritetspolicy den 26 mars 2021.
[42] Glookos integritetspolicy den 26 mars 2021.
[43] Punkt 4.4.
[44] Punkt 2:10.
[45] Glookos integritetspolicy den 26 mars 2021.

personuppgifter om en enskild individ som denne behandlar i sitt Glooko klinik-konto. Det är synnerligen viktigt att en patient är medveten om att kliniskt ansvarig vårdgivare är personuppgiftsansvarig för de uppgifter en användare överför till dennes klinik-konto och att Glooko inte är personuppgiftsansvarig. Glooko har emellertid i ett utkast till integritetspolicy som ska ersätta den från 26 mars 2021 tydliggjort vårdgivares personuppgiftsansvar vid överföring av uppgifter i användarens Glooko-konto till vårdgivaren och att Glooko inte längre är personuppgiftsansvarig för den behandlingen.

15.18 Av Glookos integritetspolicy för enskilda användare[46] framgår att bolaget kan lämna ut information som samlas in från användare, inklusive hälsouppgifter, för att uppfylla ”*en rättslig förpliktelse som vi* är *ålagda eller för att vi ska kunna skydda intressen som är av grundläggande betydelse för dig eller någon annan fysisk person*.” Och vidare: ”*Vi kan även komma att lämna ut dina personuppgifter när så krävs för fastställande, verkställande eller försvar av rättsliga anspråk, oavsett om detta sker i domstol, i en förvaltningsdomstol eller utanför domstol*”. Samma besked lämnas däremot inte i Glookos standardiserade personuppgiftsbiträdesavtal med vårdgivare (februari 2022). Skyldigheten att bestrida tredjelandets myndigheter regleras i kommissionens SCC, klausul 15, oavsett modul (som inte har angetts av Glooko). SCC:n är bilagd Glookos personuppgiftsbiträdesavtal, men artikel 14 och 15 har angetts som inte tillämpliga. Av varken integritetspolicyn för enskilda användare eller personuppgiftsbiträdesavtalet framgår om Glooko informerar användare om domstolar eller myndigheter som söker tillgång till dennes information.

15.19 Glooko har emellertid i ett presenterat utkast till integritetspolicy som ska ersätta den från 26 mars 2021 tydliggjort att såvida utländsk myndighet eller domstol begär att utfå uppgifter om en användare, bolaget kommer att underrätta användaren. Glooko har också låtit meddela att bolaget justerar sitt personuppgiftsbiträdesavtal på så sätt att kommissionens standardavtalsklausuler inte utgör del av huvudavtalet mellan vårdgivare och Glooko AB eftersom det inte sker några internationella överföringar från kunden (vårdgivare) till Glooko Inc. varför standardavtalsklausulerna har tagits bort från det uppdaterade personuppgiftsbiträdesavtalet. Tredjelandsöverföringar av vårdgivares personuppgifter genomförs i stället av Glooko AB till bl.a. Glooko, Inc. i USA, varför dessa aktörer ska teckna kommissionens standardavtalsklausuler. Avtalet behöver dock inte biläggas kundavtalet mellan Glooko AB och kunden.

15.20 Glooko erinrar i integritetspolicyn för enskilda användare[47] att bolaget överför personuppgifter från det fasta driftsstället på Irland till USA. Däremot informerar inte Glooko om vilka risker detta medför för de registrerade, t.ex. att USA saknar dataskydd- eller sekretessförfattningar som motsvarar skyddet i dataskyddsförordningen och nationella dataskyddsbestämmelser inom EU/EES. Glooko framhåller dock att bolaget vidtar tillämpliga ”säkerhetsåtgärder” med stöd av kommissionens standardavtalsklausuler för att skydda användarnas personuppgifter. Glooko framhåller vidare i en ny integritetspolicy som ska ersätta den nuvarande från den 26 mars 2021 att

[46] Glookos integritetspolicy den 26 mars 2021.
[47] Glookos integritetspolicy den 26 mars 2021.

kommissionen för närvarande inte har beviljat ett beslut om adekvat skyddsnivå på grund av att USA inte har dataskyddslagar för utlänningar som motsvarar skyddet i dataskyddsförordningen och nationella dataskyddsförordningar inom EU/EES.

15.21 Enligt Glookos integritetspolicy för enskilda användare[48] skyddas personuppgifter internt inom koncernen och vid tredjelandsöverföring av bindande företagsbestämmelser (Binding Corporate Rules). Sådana företagsbestämmelser godkänns av de nationella tillsynsmyndigheterna och EDPB. I det register som förs av EDPB över godkända bindande företagsbestämmelser finns inga registrerade bindande företagsbestämmelser för vare sig Glooko AB eller Glooko, Inc.[49] Glooko har emellertid förklarat att Glooko själv inte använder bindande företagsbestämmelser samt presenterat ett utkast till integritetspolicy som ska ersätta den från 26 mars 2021 där det numera framgår att tredjelandsöverföringar inte genomförs av bolaget med stöd av bindande företagsbestämmelser. Glooko upplyser dock att bolagets tjänsteleverantörer själva kan använda bindande företagsbestämmelser som är korrekt registrerade hos EDPB, vilket återspeglas i den uppdaterade integritetspolicyn.

15.22 I Glookos personuppgiftsbiträdesavtal med vårdgivare, benämnd ”Standardavtal” (februari 2022), saknas dock tydliga dokumenterade instruktioner från vårdgivaren till Glooko och bolagets underbiträden om för vilka ändamål bolaget får behandla vårdgivarens patientuppgifter, såsom för teknisk support, regulatoriska krav, tillhandhållande av tjänsten, produktutveckling och mycket mer. Bristerna i personuppgiftsbiträdesavtalet innebär att svenska vårdgivare inte kan lämna klar och koncis information till sina medarbetare för vilka ändamål Glooko behandlar deras personuppgifter och i vilken utsträckning tredjelandsöverföring sker av dessa. Glooko har låtit meddela att bolaget i ett nytt utkast till personuppgiftsbiträdesavtal med svenska vårdgivare tydliggjort för vilka ändamål bolaget får behandla personuppgifter åt vårdgivare i rollen som personuppgiftsbiträde, bl.a. för ändamålet säkerhets- och kvalitetskontroll av medicintekniska produkter.

15.23 Enligt artikel 12.1 i dataskyddsförordningen ska informationen till den registrerade i samband med insamling av personuppgifter vara i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Enligt artikel 13.1 e och f i dataskyddsförordningen ska den personuppgiftsansvarige ange i informationen till registrerade mottagarna eller kategorier av mottagare som ska ta del av den registrerades personuppgifter samt namn på tredjelandet.

15.24 Mot bakgrund av de kompletteringar Glooko presenterat under laglighetsprövningen, i utkast till integritetspolicy för enskilda privata användare, bedöms sammanfattningsvis informationen i Glookos integritetspolicy nå upp till kravet på koncis, klar, tydlig och begriplig information till registrerade enligt artikel 12.1 i dataskyddsförordningen. Adekvata tydliggöranden har också gjorts i ett utkast till nytt personuppgiftsbiträdesavtal

med svenska vårdgivare. Minimikravet att ange i informationen till registrerade kategorier av mottagare och namn på tredjeländer är uppfyllt.

Överföringar av personuppgifter till USA och andra länder

15.25 Glooko och AWS är amerikanska företag som, såvitt kan bedömas, enligt egna källor, policys och avtalsvillkor, inte utesluter att de kan behöva överföra personuppgifter tillhörande både konsumenter, patienter och anställd personal hos vårdgivare till USA och andra tredje länder och med ansvarsfriskrivningar för utlämnanden av uppgifter enligt bl.a. Cloud Act till amerikanska myndigheter (se avsnitt 12 och 14). I Glookos fall kan utläsas att det rör sig om överföring i både identifierbar och anonymiserad form till USA av personuppgifter för bl.a. ändamålet support, regulatoriska krav (medicintekniska produkter) och framtida forskning.

15.26 Beträffande överföringen av användares personuppgifter till USA, dvs. både privatpersoner och medarbetare hos vårdgivare, som använder Glooko-appen eller Glooko-molnet, sker en överföring om användaren begär support av Glooko och delar sina felsökningsuppgifter (däribland hälsorelaterad information) samt i den mån det är nödvändigt för att bolaget ska kunna ge teknisk support och utföra bredare analys för att upptäcka systemproblem samt support från Europa inte kan ges. Ansvarig för felsökning och annan support är Glooko, Inc. i USA. Sådan överföring sker enligt Glooko i enlighet med stöd av kommissionens standardavtalsklausuler.

15.27 Glooko hävdar att bolaget använder sig av kommissionens standardavtalsklausuler vid överföring av personuppgifter från EU till USA. Det innebär att Glooko åtar sig att respektera de rättigheter som EU-medborgare kommer i åtnjutande av enligt dataskyddsförordningen. I integritetspolicyn för enskilda användare hänvisar Glooko emellertid till kommissionens äldre standardavtalsklausuler (SCC). Dessa har ersatts av nya SCC 2021 bestående av olika moduler beroende på vem som är avsändare och mottagare av personuppgifter inom EU respektive tredjeland. Glooko har låtit meddela att man avser att korrigera felaktigheten i en ny integritetspolicy.

15.28 Vidare hänvisas i integritetspolicyn för enskilda användare till en överenskommelse mellan EU och USA om skydd för personuppgifter vid överföringar till USA benämnd Safe Harbor, medan användarvillkoren för vårdgivare hänvisar till en annan överenskommelse benämnd Privacy Shield. Enligt domar från EU-domstolen är båda överenskommelserna otillåtna eftersom de inte garanterar ett tillräckligt skydd för européers personuppgifter när de hanteras av amerikanska myndigheter. Glooko har emellertid låtit meddela att man avser att justera integritetspolicyn av den 26 mars 2021 så att det inte längre framgår några hänvisningar till att Glooko använder Privacy Shield eller Safe Harbour som ett instrument för att överföra personuppgifter till USA.

15.29 Det har inte föreskrivits i dataskyddsförordningen något visst innehåll i informationen till den registrerade om riskerna med tredjelandsöverföring baserad på standardavtalsvillkor, men enligt artikel 12.1 i dataskyddsförordningen ska informationen till den registrerade i samband med insamling av personuppgifter vara i en

koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Glooko uppger dock inte i sin integritetspolicy för enskilda användare på vad sätt bolagets leverantörer av tredjepartstjänster i tredjeländer uppfyller dataskydds- och säkerhetsbestämmelser enligt dataskyddsförordningen. Glooko har inte heller uttömmande beskrivit till vilka tredjeländer man överför användarens uppgifter, till vilka mottagare, på vilken rättslig grund och på vilket sätt dessa länder brister i sitt dataskydd, t.ex. att utlänningar i USA saknar rättsliga och effektiva möjligheter att utöva kontroll över sina personuppgifter som är förvarade hos myndigheter.

15.30 Enligt artikel 13.1 e i dataskyddsförordningen ska den personuppgiftsansvarige ange i informationen till registrerade mottagarna eller kategorier av mottagare som ska ta del av den registrerades personuppgifter. Enligt artikel 13 f ska den personuppgiftsansvarige informera om tredjelandsöverföringar. Av Artikel 29-arbetsgruppens kommentarer till informationskravet i vägledningen om öppenhet, sidorna 39-40 i WP260, framgår bl.a. följande avseende artikel 13.1 f: ”Enligt rättviseprincipen bör den information som ges om överföring till tredjeländer vara så meningsfull som möjligt för de registrerade. Detta innebär generellt sett att tredjeländernas namn ska anges.” Integritetsskyddsmyndigheten har i ett beslut bedömt att ett kreditbolag inte uppfyllt kravet på information om till vilka länder bolaget överför personuppgifter och kategorier av mottagare och vitesbelagt bristen.[50]

15.31 Glooko har emellertid presenterat ett utkast till en integritetspolicy för enskilda användare som ska ersätta integritetspolicyn av den 26 mars 2021 och där bolaget på ett tydligare sätt anger att den avser att överföra personuppgifter till ett tredjeland och hänvisar till lämpliga skyddsåtgärder inklusive länkar till överföringsmekanismer, t.ex. kommissionens standardavtalsklausuler. Glooko redovisar också till vilka tredjeländer användares personuppgifter överförs samt vilka mottagarna eller kategorier av mottagare i dessa länder är.

15.32 Glooko har vidare en lösning på plats som innebär att enskilda användares personuppgifter lagras i krypterad form i AWS:s servrar och databasapplikationer. Dock förfogar AWS och inte endast Glooko AB över krypteringsnyckeln.. All överföring av data är krypterad. All lagring och trafik mellan klient och AWS sker således i krypterad form där AWS dekrypterar respektive krypterar uppgifter på sina servrar.

15.33 Glookos utlämnande av kundens (vårdgivarens) personuppgifter, oavsett om det rör sig om patienter eller medarbetare, ska utformas som en instruktion från vårdgivaren att Glooko får överföra sådana uppgifter till USA för ändamålet support, underhåll och uppdateringar av tjänsterna. Förvisso samtycker en vårdgivare enligt personuppgiftsbiträdesavtalet att Glooko får överföra personuppgifter till en underleverantör i tredje land, men inte för vilka ändamål. En sådan instruktion saknas i dagsläget. Glooko har låtit meddela att bolaget tydliggjort i en ny version av sitt personuppgiftsbiträdesavtal med svenska vårdgivare för vilka ändamål bolaget får behandla personuppgifter åt vårdgivare i rollen som personuppgiftsbiträde. Dessa

[50] Beslut 2022-03-28, dnr DI-2019-4062.

bedöms alltjämt oprecisa. Bl.a. saknas ändamålet säkerhets- och kvalitetskontroll av medicintekniska produkter.

15.34 Glooko har vidare ha ett behov av att överföra personuppgifter tillhörande vårdgivaren i pseudonymiserad form till myndighet i USA på grund av regulatoriska krav. En tillverkare av medicintekniska produkter, såsom Glooko-molnet, har som regel ett ansvar för produktföljning som ska rapporteras till tillsynsmyndigheten, t.ex. incidenter med produkten. Det rör sig här om rapportering av personuppgifter i pseudonymiserad form. Villkoren för en sådan överföring regleras närmare i kommissionens standardavtalsvillkor, modul 2 (personuppgiftsansvarig till personuppgiftsbiträde) och 3 (personuppgiftsbiträde till personuppgiftsbiträde), punkt 8.8. Glookos personuppgiftsbiträdesavtal avsedd för vårdgivare innehåller kommissionens SCC, men punkt 8.8 saknas i Glookos avtal. Glooko har låtit meddela att bolaget justerar sitt personuppgiftsbiträdesavtal på så sätt att kommissionens standardavtalsklausuler inte utgör del av huvudavtalet mellan vårdgivare och Glooko AB eftersom det inte sker några internationella överföringar från kunden till Glooko Inc. varför standardavtalsklausulerna har tagits bort från det uppdaterade personuppgiftsbiträdesavtalet. Sådana standardavtalsklausuler ska i stället tecknas mellan Glooko AB och bl.a. Glooko, Inc., vilket är korrekt. Standardavtalsklausulerna behöver inte tillföras huvudavtalet mellan Kunden (vårdgivare) och Glooko AB. Glooko har även, som framhållits, tydliggjort i sitt personuppgiftsbiträdesavtal med svenska vårdgivare för vilka ändamål bolaget får behandla personuppgifter åt vårdgivare i rollen som personuppgiftsbiträde, men dessa bedöms alltjämt oprecisa. Bl.a. saknas ändamålet säkerhets- och kvalitetskontroll av medicintekniska produkter.

15.35 Emellertid framgår det av aktuell punkt i kommissionens standardavtalsvillkor att en ytterligare förutsättning för en tillåten överföring till tredje part, dvs. en amerikansk myndighet som utövar kvalitets- och säkerhetsövervakning av medicintekniska produkter, är att denna förpliktar sig att följa klausulerna i standardavtalsvillkoren eller att någon av fyra fallsituationer är för handen.[51] Såvitt är känt har ingen amerikansk myndighet öppet deklarerat att de är bundna av standardavtalsklausulerna. Tvärtom är amerikanska myndigheter inte bundna av kommissionens avtalsvillkor, se vidare nedan. Vad som återstår är att någon av de fyra fallsituationerna är för handen. Av intresse är den tredje och fjärde fallsituationen, nämligen att överföringen sker dels för att den är nödvändig för att fastställa, utöva eller försvara rättsliga anspråk inom ramen för särskilda administrativa, lagstiftande eller rättsliga förfaranden, dels för att den är nödvändig för att skydda den registrerades vitala intressen eller någon annan fysisk persons vitala intressen.

[51] De fyra fallsituationerna är som följer: (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer; (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question; (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

15.36 De aktuella villkoren för tredjelandsöverföringen har en motsvarighet eller förebild i dels det särskilda villkoret för att behandla känsliga personuppgifter i artikel 9.2 f, dels den rättsliga grund för behandling av personuppgifter som finns i artikel 6.1 d. Vad gäller den senare talas det i skäl 46 i dataskyddsförordningen om behandling som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Det är därför oklart om bestämmelsen syftar bara på det som är livsviktigt (gäller liv eller död) eller om även sådant som "bara" är av grundläggande betydelse avses. På grund av motsvarande tvetydigheter i dataskyddsdirektivet valde man att i personuppgiftslagen använda uttrycket vitala intressen, som även i svenska språket kan ha såväl en snävare som en bredare innebörd. Den berörda klausulen i standardavtalsvillkoren använder just ordet ”vitala intressen”.

15.37 Det är alltså tillåtet enligt kommissionens standardavtalsklausuler att överföra personuppgifter till en tredje part, i detta fall en amerikansk tillsynsmyndighet, när det är nödvändigt för att antingen fastställa, utöva eller försvara rättsliga anspråk inom ramen för särskilda administrativa, lagstiftande eller rättsliga förfaranden eller för att skydda den registrerades vitala intressen eller någon annan fysisk persons vitala intressen. En tillverkare av medicintekniska produkter har som regel lagstadgad skyldighet att göra marknadsuppföljning som ska rapporteras till tillsynsmyndigheten, t.ex. incidenter kopplade till produkten. Syftet med att rapportera incidenter är att värna om skyddet för patienter som kollektiv när det gäller produktens användning. Allvarliga brister kan bl.a. leda till marknadsförbud. Övervägande skäl tala således att Glooko har rättsligt stöd för överföringen av personuppgifter om både patientuppgifter och hälso- och sjukvårdspersonal i pseudonymiserad form, men även i individform, i rollen som personuppgiftsbiträde åt en vårdgivare under förutsättning att Glooko tillför villkor 8.8 i kommissionens SCC till personuppgiftsbiträdesavtalet och att bolaget säkerställer att det finns en skriftlig instruktion från vårdgivaren till bolaget om att denna överföring får ske till tillsynsmyndighet i bl.a. USA för ändamålet regulatoriska krav inom produktsegmentet medicintekniska. Glooko har, som nämnts, låtit meddela att man har korrigerat bristen avseende villkor 8.8 i SCC genom att teckna modul 3 mellan Glooko AB och Glooko, Inc samt andra underbiträden i tredjeland.

15.38 Kommissionens standardavtalsvillkor för tredjelandsöverföring är en skyddsåtgärd i sig för tredjelandsöverföring i syfte att binda t.ex. leverantör att effektuera rättsmedel för registrerade motsvarande de som finns i dataskyddsförordningen.. Som framhållits är amerikanska myndigheter emellertid inte bundna av standardavtalsvillkoren, vilket innebär en risk för otillåten behandling i strid med dataskyddsförordningen om uppgifter hamnar i myndigheternas förvar. Ytterligare skyddsåtgärder krävs för att förhindra det. Den Europeiska dataskyddsstyrelsen (EDPB) fastställde därför i juni 2021 rekommendationer för tredjelandsöverföring med anledning av Schrems II-domen.[52] EDPB anger i skäl 3 till rekommendationerna att ”… in the absence of an EU adequacy decision, a controller or processor should take measures to compensate for the lack of

[52] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021.

data protection in a third country by way of appropriate safeguards for the data subject". Rekommendationen måste beaktas av både personuppgiftsansvariga och biträden.

15.39 En sådan teknisk skyddsåtgärd skulle vara krypterad överföring och teknisk lagring där myndigheten, dvs. den personuppgiftsansvarige enbart förfogar över krypteringsnyckeln och inte tjänsteleverantören. I bilaga 2 i de nämnda rekommendationerna från EDPB beskrivs olika fallsituationer avseende tredjelandsöverföring som bedöms som antingen tillåtna eller inte. Bl.a. ges exempel på "adekvata skyddsåtgärder" för att kompensera bristen på ett kommissionsgodkännande eller en adekvat skyddsnivå för skyddet av personuppgifter i tredjeland som motsvarar dataskyddsförordningen. I fallsituation 1 beskrivs en situation där nycklarna enbart är under kontroll av dataexportören eller av en aktör som anlitas av dataexportören inom EU/EES. Vad som beskrivs är en s.k. Hold Your Own Key-lösning (HYOK). Glooko använder sig, såvitt förstås, inte av en sådan lösning för utkontrakteringen av drift av glukosdata till AWS i Glooko-molnet. I stället tillämpar Glooko en Bring-Your-Own-Key-lösning (BYOK) där AWS förfogar över krypteringsnyckeln och applicerar den på data i tjänsten.

15.40 En ytterligare fråga är om de personuppgifter som finns i Glooko-molnet innehåller några meddelanden eller någon annan kommunikation som är relevant i förhållande till de nationella säkerhets- och övervakningslagarna i USA (t.ex. FISA och Executive Order 12333) som nämndes som problem i Schrems II. Data i Glooko är relaterade till kunders glukosvärden. Det finns ingen information om Glooko har fått någon övervakningsbegäran från USA. Glooko använder därtill end-to-end kryptering i syfte att skydda överföringar av data och kunddata.

15.41 Endast leverantörer av elektroniska kommunikationstjänster (electronic communication service providers) omfattas av övervakningsåtgärder som sker med stöd av Section 702 FISA, vilket inebergiper telekomoperatörer (telecommunication carriers), tjänsteleverantörer som tillhandahåller olika kommunikationstjänster (t.ex. tjänster för kommunikation över internet, ECS) och molntjänstleverantörer som tillhandhåller sådana tjänster "till allmänheten" (remote computing services, RCS). Till skillnad från leverantörer av fjärrdatortjänster (RCS) behöver en ECS inte tillhandahålla tjänster till allmänheten; att ge eventuella användare – såsom företagets egna anställda – möjlighet att skicka eller ta emot kommunikation är tillräckligt.[53] Det går därför inte att utesluta att Glooko kan komma att omfattas av övervakningsprogram enligt Section 702 FISA på grund av att bolaget tillhandahåller tjänster "till allmänheten".

15.42 Det går därför inte att utesluta att Glooko kan komma att omfattas av övervakningsprogram enligt Section 702 FISA på grund av att bolaget tillhandahåller tjänster "till allmänheten". Det går inte heller att utesluta att Twilio, Inc.- leverantör av kunddataanalysplattformen Segment - omfattas av reglering.

[53] Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, Prof. Stephen I. Vladeck, den 15 november 2021 till de tyska dataskyddsmyndigheterna (DSK). Se även amerikanska justitiedepartemenets PM, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, https://www.justice.gov/file/442111/download

15.43 Det innebär att det finns en kvarstående risk för att amerikanska myndigheter kan begära eller ta del av svenska vårdgivares uppgifter om främst svenska patienter, antingen genom Cloud Act eller genom underrättelseinhämtning av data som överförs till landet, trots end-to-end kryptering. Glookos BYOK-lösning vad gäller krypteringsnyckeln är inte en adekvat skyddsåtgärd eftersom AWS förfogar över krypteringsnyckeln. Enligt EU-domstolen saknar USA en skyddslagstiftning motsvarande dataskyddsförordningen och effektiva rättsmedel för EU-medborgare vad gäller behandlingen av deras personuppgifter hos amerikanska myndigheter. Kommissionens nya standardavtalsvillkor ”släcker” inte på något sätt dessa brister, såvida det inte finns adekvata skyddsåtgärder som effektivt förhindrar att amerikanska myndigheter från att ta del av svenska vårdgivares personuppgifter.

15.44 I Glookos personuppgiftsbiträdesavtal med vårdgivare, benämnd ”Standardavtal” (februari 2022), hänvisas korrekt till kommissionens SCC från 2021. Emellertid saknar personuppgiftsbiträdesavtalet tydliga dokumenterade instruktioner från vårdgivaren till Glooko och bolagets underbiträden om för vilka ändamål bolaget får behandla vårdgivarens patientuppgifter, såsom för teknisk support, regulatoriska krav, tillhandhållande av tjänsten, teknisk support, produktutveckling och mycket mer. Vidare har Glooko uteslutit klausulerna 14 (Local laws and practices affecting compliance with the Clauses) och 15 (Obligations of the data importer in case of access by public authorities), genom att ange att dessa inte är tillämpbara. Tvärtom är dessa klausuler centrala för personuppgiftsbiträdens eller underbiträdens agerande och transparens vid tredjelands myndigheters begäran om utfående av uppgifter av en svensk vårdgivare**.** Att utesluta klausulerna 14 och 15 i SCC:n är en allvarlig brist i skyddet av enskilda patienters och vårdgivares medarbetares personuppgifter vid tredjelandsöverföring. Bristen innebär en hög risk för enskildas fri- och rättigheter. Som framhållits har Glooko låtit meddela att exkluderingen av klausulerna 14 och 15 i SCC:n är ett fel från deras sida. Glookos personuppgiftsbiträdesavtal har uppdaterats och består nu enbart av bilagan till kommissionens genomförandebeslut (EU) 2021/915 av den 4 juni 2021 om standardklausuler modul 3. Detta är korrekt eftersom endast Glooko AB är part i personuppgiftsbiträdesavtalet med kunden och inga personuppgifter överförs av kunden till Glooko Inc. utanför Europeiska ekonomiska samarbetsområdet (EES) medan däremot Glooko AB gör det. Glooko har även tydliggjort i sitt personuppgiftsbiträdesavtal med svenska vårdgivare för vilka ändamål bolaget får behandla personuppgifter åt vårdgivare i rollen som personuppgiftsbiträde. Klargörandet i personuppgiftsbiträdesavtalet innebär att svenska vårdgivare kan lämna klar och koncis information till sina medarbetare om för vilka ändamål Glooko behandlar vårdgivares personuppgifter om patienter och medarbetare.

15.45 **Det finns således en kvarstående risk, trots organisatoriska och tekniska åtgärder från Glookos sida för en otillåten behandling av personuppgifter i bolagets tjänster. Risken att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Glooko eller Twilio, Inc. får dock betraktas som mycket låg med hänsyn till Glookos kärnverksamhet (diabetesmonitorering)**. **Det finns andra risker, t.ex. cyberattacker mot molntjänster, som får betraktas som högre och mer allvarliga.** Som påtalats finns dock brister i andra delar av i Glookos behandling av personuppgifter

inklusive tredjelandsöverföring. Bristerna hänför sig till tydligare information till registrerade och tydligare instruktioner från vårdgivare till Glooko AB. **Merparten av dessa brister har emellertid åtgärdats av Glooko genom presenterade utkast till ny integritetspolicy respektive personuppgiftsbiträdesavtal med svenska vårdgivare.**

Personuppgiftsansvaret i trepartsförhållandet vårdgivare, Glooko och enskild användare

15.46 Glooko har skapat en lösning som inte har en helt tydlig separation mellan behandlingen av enskildas hälsokonton och vårdgivares konton i Glooko-molnet.

15.47 Glooko-molnet är verktyg för vårdgivare för att bedriva diabetesvård med andra tillverkares produkter. Glooko har inga egna CGM eller SAP-produkter. Det kan röra sig om produkter som förskrivs av en läkare. Produkterna är då avsedda att användas i enlighet med en ordination av läkare inom ramen för antingen hälso- och sjukvård (distanssjukvård) eller egenvård enligt ett egenvårdsbeslut av en vårdgivare. Men Glooko kan även användas av privatpersoner utan inblandning av en vårdgivare för egenbruk eller självhjälp. I alla dessa tillämpliga fall behöver den enskilde teckna ett Glooko-konto.

15.48 Vårdgivare förfogar över egna klinikkonton i Glooko-molnet. Enligt Glooko upprätthålls en logisk separation mellan vårdgivares klinik-konton respektive enskilda användares användarkonton. Vårdgivare kan således enbart ta del av en enskild persons glukosdata via en delning av data från användarkontot till vårdgivarens konto. En vårdgivare kan inte koppla molnbaserade diabetesprodukter direkt till vårdgivarens klinikkonto utan måste gå ”omvägen” via ett Glooko användarkonto.

15.49 Vid behandling av patientuppgifter i ett Glooko klinikkonto är patientansvarig vårdgivare personuppgiftsansvarig. Vårdgivare skapar inte egna hälsokonton åt patienter i Glooko-molnet. Det enda tillämpliga användarfallet är att en patient skapar ett användarkonto i Glooko och ger vårdgivaren tillgång till användarkontot för att vårdgivaren ska kunna behandla dennes personuppgifter.

15.50 För att en svensk vårdgivare ska kunna ta del av en patients glukosvärden och annan relevant data under en vårdepisod måste patienten således skapa ett konto i Glooko och aktivt möjliggöra delning av sina glukosvärden med vårdgivaren via Glooko-appen eller www.glooko.com. Oklarheten om personuppgiftsansvaret handlar om vårdgivarens direktåtkomst till en enskild individs upprättade konto i Glooko-molnet.

15.51 Det råder ingen tvekan om att Glooko är personuppgiftsansvarig för individens konto och personuppgifter i Glooko. Det är Glooko som tillhandahåller kontot, tecknar avtal om användandet och faktiskt bestämmer över behandlingen av personuppgifter som sker däri. Det s.k. privatundantaget i dataskyddsförordningen är inte tillämpligt eftersom Glooko använder den registrerades personuppgifter för egna ändamål, t.ex. för att utveckla tjänsten och möjliggöra för användaren att dela sina uppgifter med andra, t.ex. en vårdgivare. Då är Glooko personuppgiftsansvarig för behandlingen av patientens

personuppgifter i produkten.[54] Dataskyddsförordningen är tillämplig på personuppgiftsbehandlingen.

15.52 De uppgifter som överförs till vårdgivarens konto i Glooko är vårdgivaren personuppgiftsansvarig för. Glooko är personuppgiftsbiträde i denna del. Men är vårdgivaren personuppgiftsansvarig även för de personuppgifter som överförs via direktåtkomsten? Och för vilka personuppgifter i den enskildes användarkonto blir vårdgivaren personuppgiftsansvarig för genom direktåtkomsten i Glooko? Bara de data som samlas in av individen via sensor och pump, överförs och förvaras av vårdgivare i Glooko klinikkonto? Eller även annan data i den enskildes användarkonto, dvs. sådana uppgifter som inte överförs?

15.53 **Glookos lösning för datadelning mellan invånare och vårdgivare är närmast att betrakta som egenvård enligt Socialstyrelsens egenvårdsföreskrifter, och inte distanssjukvård**, och där vårdgivaren är personuppgiftsansvarig enbart för den uppföljning som sker av data inom ramen för egenvårdsbeslutet som den enskilde personen har godkänt får automatiskt lämnas ut till vårdgivarens lagringsyta i Glooko när denne efterfrågar uppgifterna. Glooko är personuppgiftsansvarig för den enskilda individens användarkonto i Glooko och lämnar ut uppgifterna enligt samtycke från användaren. För att en vårdgivare ska kunna bedriva hälso- och sjukvård per definition enligt hälso- och sjukvårdslagen, alltså distanssjukvård, genom Glooko, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att andra tillverkares produkter kopplas direkt till vårdgivarens klinik-konto i Glooko eller att vårdgivaren skapar konton och tillhandahåller användaruppgifter åt patienter i Glooko. Så är inte fallet nu med undantag för glukosdata som en vårdgivare laddar upp i sin dator via Glookos transmitter.

15.54 Vad beträffar direktåtkomsten är vårdgivaren personuppgiftsansvarig för den behandlingen av personuppgifter. Det finns emellertid en påtaglig risk att vårdgivare med direktåtkomst till enskild individs Glooko-konto blir personuppgiftsansvariga för alla personuppgifter i kontot. Genom direktåtkomsten blir uppgifterna i kontot enligt svensk rätt att betrakta som inkomna allmänna handlingar hos en myndighet, t.ex. en nämnd i en region (2 kap. 6 § tryckfrihetsförordningen).

15.55 Det finns andra tveksamheter med direktåtkomsten. Direktåtkomst är enligt förarbetena till patientdatalagen (PDL) en form av elektroniskt utlämnande till en extern mottagare. Begreppet direktåtkomst är inte definierat i lag. Med direktåtkomst menas vanligen att någon har direkt tillgång till någon annans databas eller register och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i databasen eller registret. Begreppet brukar också anses innefatta att den som är ansvarig för databasen eller registret inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av. Vid direktåtkomst anses de uppgifter som omfattas av åtkomsten utlämnade i och med att åtkomsten medges.

[54] Artikel 29-gruppen, vägledning om appar på smarta enheter (02/2013), s. 9.

15.56 Det följer nämligen av PDL att vårdgivares personuppgiftsansvar omfattar även sådan behandling av personuppgifter som vårdgivaren, eller den myndighet i en region eller en kommun som är personuppgiftsansvarig, utför när vårdgivaren eller myndigheten genom direktåtkomst i ett enskilt fall bereder sig tillgång till personuppgifter om en patient hos en annan vårdgivare eller annan myndighet i samma landsting eller kommun (2 kap. 6 § PDL). Av bestämmelsen går inte att utläsa om en vårdgivare är personuppgiftsansvarig för de personuppgifter som görs tillgängliga från ett hälsokonto genom direktåtkomst som en leverantör tillhandahåller. Faktum är att PDL inte reglerar direktåtkomst till hälsokonton som erbjuds av tillverkare. Det skulle innebära att sådan direktåtkomst inte alls är tillåten eftersom lagen uttömmande reglerar när en vårdgivare får ta del av patientuppgifter genom direktåtkomst (5 kap. 4 § PDL). En vårdgivare kan därmed inte heller med stöd av patientens samtycke få direktåtkomst till dennes personuppgifter i ett hälsokonto.

15.57 Om en behandling av personuppgifter är otillåten, måste ansvar utkrävas av någon. Personuppgiftsansvaret är styrande för vem som ska ställas till svars. Det ligger i farans riktning att det är vårdgivaren som bär ansvaret för den otillåtna direktåtkomsten, såvida inte vårdgivaren anses därigenom även ansvara för behandlingen av personuppgifter i hälsokontot. Då är det en tillåten direktåtkomst om vårdgivaren är personuppgiftsansvarig även för alla personuppgifter i kontot. Ett sätt att undvika osäkerhet om en vårdgivares direktåtkomst är laglig eller inte är att lämna ut uppgifter via ADB-utlämnande.

15.58 I princip anses allt elektroniskt utlämnande som inte görs genom direktåtkomst ske genom utlämnande på medium för automatiserad behandling (ADB-utlämnande). Som exempel på ADB-utlämnande kan nämnas att personuppgifter överförs mellan mottagare genom e-post, USB-minne eller dator till dator. Begreppet anses omfatta överlämnande av elektroniskt lagrade uppgifter via alla slags medium för lagring och överföring.

15.59 En form av elektroniskt informationsutbyte som är vanlig mellan myndigheter är fråga-svar-funktioner. Högsta förvaltningsdomstolen (HDF) har i den s.k. Lefi-onlinedomen (HFD 2015 ref. 61) ansett att gränsdragningen mellan vad som är direktåtkomst och annat utlämnande på medium för automatiserad behandling beror på om den aktuella uppgiften kan anses förvarad hos den mottagande myndigheten enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen. Avgörande är således om uppgiften är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. HFD:s dom kan tolkas så att den tekniska utformningen av en myndighets system för utlämnande av uppgifter kan bli avgörande för om utlämnandet ska anses som direktåtkomst eller som annat utlämnande på medium för automatiserad behandling. I domen fann HDF mottagande myndighets åtkomst till uppgifter hos den utlämnande myndigheten genom ett system som utformats med en fråga-svar-funktionalitet inte utgjorde direktåtkomst. På motsvarande sätt fungerar Inera AB:s tjänstekontrakt i de nationella tjänsterna som bolaget förvaltar, t.ex. i Nationell Patientöversikt (NPÖ).

15.60 **Den av Glooko valda juridiska lösningen för Glooko-molnet ger upphov till otydliga ansvarsförhållanden för personuppgiftsbehandlingen när en vårdgivare vid en egenvård får direktåtkomst till en enskild persons hälsokonto, som den enskilde skapat själv**. Det är inte uteslutet att vårdgivaren i det läget anses personuppgiftsansvarig för alla data i kontot, även sådana som invånaren registrerat utan inblandning av en vårdgivare för att monitorera sin diabetes, trots löfte från Glooko om det motsatta. Det är i sådant fall inte Glooko som är personuppgiftsansvarig för den enskilda individens användarkontot utan en vårdgivare.

15.61 Rättsläget är emellertid oklart. Genom tydligare information i avtalsvillkoren för enskilda användare respektive vårdgivare torde Glooko kunna reducera väsentligen de risker som föreligger för registrerade vid ett otydligt personuppgiftsansvar på beskrivet sätt. Det är inte uteslutet att det finns ett visst ”spelrum” i brist på vägledning i lagstiftningen för både Glooko och vårdgivare att reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke. Ett annat alternativ som ska ses som en rekommendation är att Glooko överväger en lösning i framtiden som innebär att vårdgivare inte får direktåtkomst till enskildas Glooko-konton vid distanssjukvård utan i stället skapa en lösning med två logiskt eller t.o.m. fysiskt separerade lagringslösningar – en för vårdgivare respektive en för patienter – i Glooko-molnet för att åstadkomma en tydlig ”separation of duties”. Glooko bör eftersträva att utlämnande mellan patientens lagringslösning (konto) och vårdgivarens sker genom s.k. ADB-utlämnande, dvs. filöverföring, t.ex. via API:er där data efterfrågas och lämnas ut mellan kontona. Patienter däremot får enligt patientdatalagen ha direktåtkomst till en vårdgivares vårddokumentation, om vårdgivaren så tillåter, dvs. en direktåtkomst från sitt användarkonto i Glooko till vårdgivarens klinikkonto i Glooko-molnet.

Autentisering av användare

15.62 Inloggning i Glooko-appen sker utan någon autentisering, bortsett från PIN-kod till den mobila enheten. Användares åtkomst till egen data i Glooko-molnet (www.glooko.com) sker med användarnamn och lösenord, dvs. enfaktorsautentisering. Åtkomst kan än så länge inte ske med Bank-ID eller annat elektroniskt ID. Vårdgivare däremot loggar in på sitt klinik-konto i Glooko med användarnamn och engångslösenord via e-post, om vårdgivaren begär det De kan inte nyttja SITHS-kort eller annat slag av e-legitimation.

15.63 Autentisering som bygger på enbart användarnamn och ett statiskt lösenord har en fundamental svaghet; alla som har kännedom om, kan räkna ut eller gissa sig till lösenordet kan bli verifierade som den registrerade (behöriga) användaren i elektronisk bemärkelse. Det finns inga praktiska möjligheter för varken den enskilde eller den personuppgiftsansvarige att upptäcka att lösenordet kommit någon annan till kännedom, om inte denne avslöjar det på något sätt. Att enbart använda lösenordet avslöjar inte den obehörige användaren. Vidare kan ett statiskt lösenord som kommit på avvägar användas av flera personer eller vid upprepade tillfällen, utan att det föreligger någon egentlig möjlighet för upptäckt.

15.64 Oavsett hur användarnamnet och lösenordet har kommit på avvägar kan vidare spridning eller otillåten användning av dem inte kontrolleras av vare sig den behörige användaren eller den personuppgiftsansvarige. Det är på grund av dessa risker som åtkomst via internet till integritetskänsliga personuppgifter behöver en högre nivå av autentisering än att användarens identitet verifieras enbart med hjälp av något som användaren vet (lösenordet/PIN-koden). Stark autentisering av en användare kan uppnås genom att använda två eller flera autentiseringshjälpmedel, kategoriserade utifrån minst två av följande tre faktorer; något som användaren vet (lösenord/PIN-kod), har (kort) eller är (biometrisk egenskap).

15.65 Syftet med stark autentisering är bl. a. att användaren ska kunna förlora kontrollen över ett autentiseringshjälpmedel utan att säkerheten för personuppgifterna därmed går förlorad. Det ska också gå att upptäcka och vidta åtgärder om ett autentiseringshjälpmedel går förlorat. Den teoretiska utgångspunkten för att förlita sig på ett autentiseringshjälpmedel som kategoriseras som en ”har”- eller ”är”-faktor är att det finns en, och endast en instans av hjälpmedlet i sinnevärlden, och att enbart den registrerade användaren har tillgång till det. Det ger en högre grad av sannolikhet att den uppgivna identiteten är den rätta än om användarens identitet verifieras enbart med hjälp av något som användaren ”vet”.

15.66 BankID är en av de vanligaste metoderna för e-legitimation och består av en fil som laddas ner från banken där användaren är kund och som kombineras med en pinkod för att styrka identiteten. Med Mobilt BankID knyts e-legitimationen till den telefon som det hämtats till. Kombinationen av ett digitalt certifikat och en pinkod skapar en tvåfaktorsautentisering som ger en högre säkerhetsnivå, eftersom man styrker sin identitet både med något man vet eller kan och med något man har. Hälso- och sjukvården använder en egen autentiseringslösning benämnd SITHS och kan beställas av leverantörer som har ett uppdrag åt en offentlig aktör. Förvaltare av SITHS är Inera AB.

15.67 Av 3 kap. 15 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården (föreskrifterna) framgår att vårdgivare som använder öppna nät för att hantera patientuppgifter ansvarar för att det i ledningssystemet finns rutiner som säkerställer att överföring av patientuppgifter görs på ett sådant sätt att ingen obehörig kan ta del av uppgifterna, och åtkomst till patientuppgifter föregås av stark autentisering. Av 4 kap. 11 § i samma föreskrifter och allmänna råd framgår att vårdgivaren ska ansvara för att en enskilds direktåtkomst till uppgifter om sig själv och till dokumentation om åtkomst tillåts endast efter att den enskildes identitet har säkerställts genom stark autentisering.

15.68 Beträffande först vårdgivares inloggning till sitt klinik-konto på Glooko-molnet lever Glooko upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Det är dock inte en standardfunktion i tjänsten utan aktiveras på vårdgivares begäran. Glooko rekommenderas att alltid ha stark autentisering aktiverad så att vårdgivare inte gör sig skyldighet till brott mot regelverket. Beträffande sedan en enskild persons inloggning till sitt konto på www.glooko.com lever Glooko inte upp till kraven på stark autentisering. Beträffande slutligen Glooko-appen omfattas dessa förvisso inte

av Socialstyrelsens föreskrifter. Något krav på stark autentisering i författning finns inte. **Rekommendationen är dock att enskilds inloggning till hälsodata i apparna bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i Glooko-molnet ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.**

Vårdgivares inbjudan via e-post till användare

15.69 När en patient läggs till i klinikens patientlista i Glooko skapas inte ett användar-konto automatiskt för denna patient. Patienter måste i stället skapa sitt eget konto i Glooko om de vill dela glukosdata med vårdgivaren. En inbjudan innehåller en delningskod som patienterna anger i sitt personliga användarkonto eller i Glooko-appen. När patienten har angett koden och födelsedatum börjar kontona automatiskt att dela information sinsemellan. Delningskoden och inbjudan till att dela data skickas via e-post till patienten.

15.70 Av 3 kap. 15 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården (föreskrifterna) framgår som framhållits ovan att om vårdgivaren använder öppna nät vid behandling av personuppgifter, ska denne ansvara för att överföring av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dem. Enligt 3 kap. 16 § Socialstyrelsens föreskrifter får en vårdgivare, efter att ha gjort en behovs- och riskanalys, besluta om undantag från kraven vid överföring av påminnelser och kallelser i öppna nät till vård och behandling som riktar sig till patienter. Vårdgivaren ska i sådant fall dokumentera beslutet och behovs- och riskanalysen. Av 3 kap. 17 § Socialstyrelsens föreskrifter framgår att en överföring av en påminnelse eller en kallelse i klartext via t.ex. sms och e-post får endast göras efter att patienten har gett sitt medgivande, och inte avslöja detaljer om patientens hälsotillstånd eller andra personliga förhållanden.

15.71 Av Socialstyrelsens föreskrifter framgår således att en vårdgivare får skicka påminnelser och kallelser i klartext till en patient via sms och e-post. I sin handbok till föreskrifterna anför Socialstyrelsen att undantaget från kraven i 3 kap. 15 § har tillkommit då det anses praktiskt och smidigt både för vårdgivare och patienter med kallelser och påminnelser om besök i vården per sms eller e-post. Det innebär att uppgifter om patienter i elektroniska påminnelser och kallelser som kommuniceras över öppna nätverk, exempelvis via sms eller e-post, inte behöver krypteras. Meddelandet får dock inte avslöja diagnoser eller sjukdomar. Namn på klinik (t.ex. ”KBT-kliniken” eller ”Hörselkliniken”) kan röja patientens diagnos eller sjukdom och kan därmed förhindra en vårdgivare att använda påminnelser och kallelser via e-post och sms.

15.72 Enligt 3 kap. 16 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling v personuppgifter i hälso- och sjukvården får en vårdgivare, efter att ha gjort en behovs- och riskanalys, skicka påminnelser och kallelser i klartext via öppna nät till vård och behandling som riktar sig till patienter. En vårdgivare kan i Glooko skicka en inbjudan och delningskod till patienter via e-post. En

inbjudan i klartext om att ta del av eller dela glukosdata med en vårdgivare utgör inte en ”kallelse eller påminnelse till vård- och behandling” enligt Socialstyrelsens föreskrifter och allmänna råd. Att dessutom skicka en delningskod via e-post i ett öppet nät innebär stora risker för obehörigt röjande av delningskoden, och därmed hälsorelaterade uppgifter, med en tredje part. Användning av e-post för att skicka en delningskod med en patient är i strid med Socialstyrelsens föreskrifter och en otillåten behandling av personuppgifter. Det är förvisso vårdgivaren i rollen som personuppgiftsansvarig som gör sig skyldig till den otillåtna behandlingen av personuppgifter. Å andra sidan bär Glooko i rollen som personuppgiftsbiträde och tjänsteleverantör ett ansvar för att ge ”tillräckliga garantier” för skyddet av personuppgifter och registrerades fri- och rättigheter i sina tjänster och produkter (artikel 28.1 i dataskyddsförordningen). Att funktionen är frivillig för vårdgivaren att använda ”släcker” inte de krav på skydd och säkerhet som ställs på personuppgiftsbiträden i dataskyddsförordningen. Glooko rekommenderas att åtminstone informera vårdgivare om riskerna med att använda funktionen eller att lämna delningskoden till patienten vid ett personligt besök på kliniken i avvaktan på en säkrar lösning för delning, t.ex. sms eller push-notis i mobilen om att det finns ett meddelande från en vårdgivare som användaren tar del av i inloggat läge i appen.

15.73 Glooko har ifrågasatt bedömningen och uppgivit i huvudsak följande: En inbjudan som en vårdgivare själv kan skicka sina patienter innehåller inga personuppgifter förutom användarens namn. Om ett e-postmeddelande skickas av en vårdgivare, skickas detta e-postmeddelande bara en gång till patienten. E-postmeddelanden används inte för någon regelbunden, pågående kommunikation av något slag av Glooko systemet. Ingen av mottagarens faktiska hälsodata ingår i dessa e-postmeddelanden, annat än det faktum att användaren är en patient hos kliniken som skickar själva e-postmeddelandet. Utgående e-postmeddelanden som skickas från Glooko systemet skickas för närvarande genom ”Transport Layer Security”-kryptering. E-postkonton är för föremål för autentiseringsskyddade inloggningar, och olika e-postsystem för konsumenter kräver redan tvåfaktorsautentisering för att få tillgång till dem. I e-postmeddelandet finns en länk att klicka på för att "aktivera" användarens konto. Länken tar användaren till en inloggningssida på Glookos webbplats. På denna inloggningssida måste användaren ha kännedom om och ange sitt födelsedatum för att aktivera sitt konto i Glooko. Användaren måste således ha två faktorer i sin kontroll för att autentisera på denna inloggningssida: 1. tillgång till e- postkontot och 2. den mottagande användarens födelsedatum. Om mottagarens e-postprogram använder tvåfaktorsautentisering för att logga in är hela processen föremål för trefaktorsautentisering. Slutligen framhåller Glooko att den begränsade användningen av e-postkommunikation i tjänsten inte är det enda sättet på vilket en aktiveringslänk kan delas med en patient. Systemet gör det möjligt enligt Glooko för vårdgivaren att skriva ut och dela aktiveringslänken direkt med patienten personligen. Och inga vårdgivare är skyldiga att använda denna utgående e-postfunktionalitet. Glooko anser således att alla relevanta faktorer som identifierats ovan kraftigt begränsar risken för att något av innehållet i e-postmeddelandena nås av obehöriga tredje parter och för rättigheterna och friheterna för mottagarna av sådana e-postmeddelanden.

15.74 En inbjudan via e-post i klartext om att låta vårdgivaren få ta del av en patients glukosdata i hens Glooko-konto utgör dock inte en påminnelse eller en kallelse till vård och behandling enligt Socialstyrelsens föreskrifter. Uppgift om födelsedatum om invånare är i ett land som Sverige en publik uppgift. Bedömning och rekommendation kvarstår. Glooko har låtit meddela att man utvärderar potentiell användning av 1177 och andra meddelandetjänster för att göra andra lösningar tillgängliga för svenska vårdgivare i syfte att bjuda in patienter att aktivera sina konton.

Forskning

15.75 Enligt Glookos integritetspolicy för enskilda användare[55] används registrerades uppgifter för framtida forskning: ”*När vi får personuppgifter från dig kan vi komma att avidentifiera dessa uppgifter permanent och använda dem för statistisk analys, klinisk forskning, demografisk analys, profilering av användarbeteenden inom appen och it-egenskaper samt mäta intresset för och hanteringen av fysiska tillstånd och liknande behandling. Permanent avidentifierade uppgifter innehåller inga personuppgifter och kan därför inte spåras tillbaka till dig. Permanent avidentifierade uppgifter kan komma att exporteras till länder i eller utanför EU, USA eller andra områden. Inom USA kan både anonymisering med HIPAA ’Safe Harbor’ och tokenisering med hjälp av en expertbestämningsmetod användas för att anonymisera data. För personuppgifter som samlats in inom EES används GDPR-kompatibla anonymiseringsmetoder.”*

15.76 Såvitt förstås används den registrerades personuppgifter för ändamålet framtida forskning med stöd av ett samtycke när denne tecknar ett Glooko användarkonto. Det är ett frivilligt samtycke och inte ett villkor för att använda tjänsten.

15.77 Glookos integritetspolicy för enskilda användare specificerar dock inte vad för slags forskning det rör sig om eller vilka som ska bedriva forskningen. Vad som framgår är att Glooko hävdar att bolaget enbart kommer att använda sig anonymiserade data men inte vilka data. Någon ytterligare information om ”forskningen” finns inte att tillgå.

15.78 Varför Glooko inhämtar ett samtycke som rättslig grund när bolaget i själva fallet använder sig av anonymiserade uppgifter om användare för framtida forskning beror på att personuppgifter, dvs. individuppgifter, behöver tekniskt bearbetas för att skapa anonyma uppgifter. Avidentifieringen i sig för ändamålet forskning kräver alltså en bearbetning av personuppgifter om användare. Behandlingen ska dock vara tillåten enligt dataskyddsförordningen.

15.79 Av principen om ändamålsbegränsning i dataskyddsförordningen (artikel 5.1 b) framgår emellertid att all behandling av personuppgifter ska ha ett ändamål. Ändamål ska vara ”särskilda, uttryckligt angivna och berättigade”. Det kravet på ändamål gäller även behandling av personuppgifter för forskning. Det finns alltså inte utrymme i dataskyddsregelverket att skapa uppgiftssamlingar för framtida forskningsbehov eller framtida forskningsfrågor, inte ens med stöd av en enskilds samtycke eftersom samtycket

[55] Glookos integritetspolicy den 26 mars 2021.

inte kan ”släcka” de grundläggande dataskyddsprinciperna. Samma begränsningar råder för den som behandlar personuppgifter i syfte att skapa anonymiserade uppgifter för samma ändamål.

15.80 Av skäl 33 i dataskyddsförordningen framgår emellertid en inskränkning vad gäller kravet på samtycke för forskning. Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för forskning, när vedertagna etiska standarder för forskning iakttas. Några sådana områden eller beskrivna forskningsområden framgår inte av Glookos integritetspolicy för enskilda användare eller av annan dokumentation tillgänglig för allmänheten.

15.81 Glooko har låtit meddela att begreppet ”forskning” egentligen avser aggregerad statistisk analys och andra analyser, t.ex. användarbeteende och ”fysiska tillstånd”, som är nödvändiga för bolagets affärsverksamhet. Glooko har presenterat ett utkast till en ny integritetspolicy för enskilda användare som ska ersätta integritetspolicyn av den 26 mars 2021 och där alla hänvisningar till ordet "forskning" har tagits bort. Den rättsliga grunden är alltjämt ett frivilligt samtycke. Ändamålen får anses tillräckligt specificerade. Behandlingen bedöms därför utgöra en tillåten behandling.

Kakor och tredjepartsaktörer

Glooko använder Twilio Segment samt inloggnings-, funktions- och säkerhetsprogramvaror i sina appar och på www.glooko.com, vilka kräver kakor. Enligt Twilios integritetspolicy för Segment samlas bl.a. följande information om användarna: klient, t.ex. PC eller mobil enhet, operativsystem, tillverkare och modell, webbläsare, IP-adress, ”unika identifierare”, och geografisk information såsom geografisk plats. Vidare användardata, såsom besökt webbsida före besök av aktuell webbsida, sidor som användaren tittat på, hur lång tid som spenderades på en särskild sida, navigationslänkar, inloggningstid och tid tagen i anspråk på webbplatsen. Twilio Segment är en konkurrent till Google Analytics-sviten, men till skillnad från Google tillhandahåller inte Twilio konsumenttjänster och personliga konton på motsvarande sätt som Google. Twilio använder vidare egna utvecklade kakor för analys och användarregistrering. Twilio kan således inte på motsvarande sätt som Google spåra fysiska personer genom IP-nummer.

15.82 Enligt integritetspolicyn för enskilda användare används kakor enligt Glooko för följande syften:

- autentisering – kakor för att identifiera användare vid besök på Glookos webbplats, vid navigering på webbplats och vid användning av Glookos tjänster
- status – för att avgöra huruvida användaren är inloggad på Glookos tjänster
- personlig anpassning – för att lagra information om preferenser och för att kunna anpassa webbplats och tjänster (t.ex. språkval)
- säkerhet – kakor som en del av säkerhetsåtgärder som används för att skydda användarkonton.

- analys – kakor som kan hjälpa Glooko att analysera användandet av webbplats och tjänster samt att de fungera som de ska
- samtycke till användning av kakor – kakor för att lagra användarens mer allmänna preferenser när det gäller användning av kakor.

15.83 Såvitt kunnat utrönas ansvarar Glooko ensam för inloggnings-, funktions- och säkerhetskakorna. Twilio Segment-kakor används för att föra statistik över och göra analyser av användningen av tjänsten. Den typ av information som samlas in är aggregerad. Prestandaövervakningsdata kan inkludera appversion, land, IP-adress, OS-nivå, enhet, radio- och operatörsinformation. Det är oklart om informationen innehåller använda diabetesprodukters serienummer eller några andra personuppgifter, däribland hälsorelaterad information. Överföringen har stöd i kommissionens standardavtalsklausuler.

15.84 Det finns ingen information i Glookos kundavtal med vårdgivare inklusive personuppgiftsbiträdesavtal huruvida kakor används vid vårdgivares och deras medarbetares användning av Glookos tjänster. Det är en brist.

15.85 Överföring av personuppgifter till USA eller till annat tredjeland via Glookos underleverantör Twilio kan inte uteslutas. Twilio Segment registrerar IP-adress hos användare av appar och Glooko-molnet. Sannolikt kan inte Twilio hänföra IP-nummer från en enskild privat användares app eller dator vid inloggning i Glooko-konto i www.glooko.com till en fysisk levande person. Tredjepartstjänsten Twilio Segment bedöms därmed inte innebära en sannolik risk för otillåten behandling av personuppgifter via kakorna..

På uppdrag av SKR

Manólis Nymark

Bilaga 1

Glooko AB

Nellickevägen 20
412 63 Gothenburg
Sweden
031-762 88 88

Den 3 juni 2022

Promemoria

Glooko lämnar respektfullt in denna promemoria beträffande vissa frågor som tas upp i PM Laglighetsprövningen molntjänsten Glooko® avseende på dataskydd och annat integritetsskydd ("**Granskningen**"), på uppdrag av Sveriges Kommuner och Regioner.

Ämne: Användning av utgående e-postmeddelanden

Granskningen ifrågasätter Glooko systemets tillhandahållande av en utgående e-postmeddelande funktion som kan initieras av vårdgivare vilken skickar patienter ett e-postmeddelande som innehåller en aktiveringslänk ("**E-postmeddelanden**"). Ett exempel på ett av e-postmeddelandena bifogas denna promemoria som bilaga 2. Vårdgivaren kan (men det krävs inte) använda e-postmeddelandet för att skicka aktiveringslänken (vad författaren till Granskningen kallar en "delningskod") till mottagaren. Denna länk leder mottagaren till en landningssida på Glooko webbplatsen där mottagaren sedan uppmanas att ange sitt eget födelsedatum. Vid inmatning av rätt födelsedatum aktiverar mottagaren framgångsrikt sitt eget konto i Glooko programvaran som också automatiskt är ansluten till vårdgivarens konto i programvaran. Detta möjliggör uppladdning av data från diabetesenheter hemifrån, vilket gör det möjligt för vårdgivaren att på avstånd se data från diabetesenheten för patienten.

Granskningen anger "att skicka en delningskod via e-post i ett öppet nät innebär stora risker för obehörigt röjande av delningskoden, och därmed hälsorelaterade uppgifter, med en tredje part".

Även om inga elektroniska överföringar (inklusive textmeddelanden) som använder öppna nätverk är helt säkra, finns det ett antal faktorer som både skyddar de begränsade personuppgifterna i dessa e-postmeddelanden och användandet av själva aktiveringslänken. Dessa inkluderar följande:

1. Mottagarnas e-postkonton är själva redan föremål för autentiseringsskyddade inloggningar, och olika e-postsystem för konsumenter kräver för närvarande tvåfaktorsautentisering för att få tillgång till dem;

2. Utgående e-postmeddelanden från Glooko programvaran skickas via Transport Layer Security-kryptering som skyddar deras innehåll under transport;

3. Om ett e-postmeddelande skickas av en vårdgivare skickas e-postmeddelandet bara en gång till patienten. E-postmeddelanden används inte för någon regelbunden, pågående kommunikation av något slag av Glooko systemet;

4. Det finns inga specifika, känsliga hälsouppgifter i själva e-postmeddelandena. E-postmeddelandena innehåller inte: en indikation på att mottagarna är föremål för någon formell diagnos; mottagarens typ av diabetes, om någon; eventuella avläsningar från någon diabetesenhet; eller någon specifik biometrisk information om mottagaren (längd, vikt, blodtryck etc);

5. Aktiveringslänken tillåter inte någon som har tillgång till den att se mottagarens hälsodata. När du väl har klickat på aktiveringslänken från e-postmeddelandet och dirigerats till landningssidan hos Glooko måste användaren också ha födelsedatum för att verifiera sin åtkomst till Glooko-kontot. Detta andra verifieringssteg för att aktivera kontot i Glooko-programvaran (det första är att ha tillgång till e-postkontot via inloggningsuppgifter och potentiell tvåfaktorsautentisering), gör denna process för aktivering av kontot till minst tvåfaktorautentisering. Om mottagarens e-postprogram använder tvåfaktorsautentisering för att logga in är hela processen föremål för trefaktorsautentisering.

Slutligen notera att Glookos begränsade användning av e-postkommunikation inte är det enda sättet på vilket en aktiveringslänk kan delas med en patient. Systemet gör det möjligt för vårdgivaren att skriva ut och dela aktiveringslänken direkt med patienten personligen. Och inga vårdgivare är skyldiga att använda denna utgående e-postfunktionalitet.

Glooko anser att alla relevanta faktorer som identifierats ovan kraftigt begränsar risken för att något av innehållet i e-postmeddelandena nås av obehöriga tredje parter och för rättigheterna och friheterna för mottagarna av sådana e-postmeddelanden.

Bilaga 2

glooko

Hi [redacted]

Your care team at Florence Medical Group uses Glooko to view diabetes data so they can support your healthcare needs. Glooko is a secure, privacy-protected solution enabling health care teams to remotely visualize diabetes information for 2.8 million patients globally.

You can now use Glooko to sync your devices through your smart phone or home computer without the need to visit your doctor's office. Whether you want to share your device data before a phone or video appointment or simply save time by downloading your devices before you go into the clinic, your free Glooko account allows you and your care team to securely and conveniently manage your health together.

Florence Medical Group has invited you to activate your free Glooko account for use at home. Get started today.

ACTIVATE

If you have questions, please visit support.glooko.com.