PROMEMORIA

2022-07-03

Laglighetsprövning av Dexcom CGM-system 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.

1 Dexcom Real Time CGM-system (rtCGM) består av ett flertal CE-märkta medicintekniska produkter, både hårdvaror och mjukvaror, som utvecklas och tillhandahålls av det amerikanska företaget Dexcom, Inc. (fortsättningsvis Dexcom om inte annat anges). Hårdvarorna (sensor, sändare och mottagare) är kärnan i rtCGM-systemet och utgör de nödvändiga delarna för glukosmonitorering. Enskilda användare kan därutöver välja att komplettera hårdvaran med molnbaserade tjänster antingen från Dexcom eller tredje part, t.ex. Diasend/Glooko. Dexcom har ett flertal dotterbolag i Europa. I Sverige distribueras Dexcoms produkter av Nordic Infucare AB, vilket bolag är en tredje part i förhållande till Dexcom.

2 Dexcoms G6-system är ett sensorbaserat, CE-märkt system för glukosmätning. Dexcom G6 består av en sensor, sändare och mottagare. I stället för Dexcom-mottagaren kan en enskild användare välja appen Dexcom G6. En användare kan även ladda ner Dexcom Clarity-appen som sammanställer rapporter, kurvor, diagram och grafer i Dexcoms molntjänst Clarity och kan på så sätt hjälpa användaren att förstå effekterna av insulindosering, matvanor, träning, och eventuella läkemedel. Dexcom Clarity-appen överför glukosvärden till molntjänsten Clarity. Även G6-mottaragen kan överföra glukosdata till Clarity-molnet. Användaren kan välja att deaktivera sådana överföringar i appen genom att stänga av synkronisering till Dexcom Clarity. Mätvärden som överförs till Dexcoms molnbaserade tjänst Clarity sparas tills vidare så länge användaren inte säger upp sitt konto. En enskild användare är helt fri att bestämma om han eller hon vill använda den valfria molnbaserade funktionen i Clarity eller att avstå från användningen av Clarity helt

3 G6-appen och Clarity-appen kräver att användaren skapar ett Dexcom-konto i Dexcoms molnbaserade tjänst Clarity. En användare kan dela sina glukosvärden med en tredje part, t.ex. en vårdnadshavare eller en anhörig. I sådant fall krävs att den tredje parten använder Dexcoms Follow-app. Användare av Clarity-appen kan dela sina glukosmätningar och andra data med tio andra personer. Dexcoms rtCGM-system kan dessutom kombineras med

insulinpumpar från ett flertal andra tillverkare. Dexcom erbjuder även användare av sina produkter möjligheten att överföra uppgifter till molntjänsten Diasend/Glooko. Diasend/Glooko används i stor utsträckning av svenska vårdgivare för monitorering och uppföljning av diabetespatienter som bl.a. använder Dexcoms produkter.

4 Molntjänsten Dexcom Clarity kan också användas av vårdgivare. Clarity är en CE-märkt produkt. För detta syfte krävs att vårdgivaren använder programvaran Dexcom Uploader som laddas ner till aktuell klient. Gränssnittet är en webbläsare. Varje vårdgivare skapar ett klinik-konto som hanteras av en administratör hos denne. Administratören tilldelar sedan behörigheter till medarbetare hos vårdgivaren (”standardanvändare”). Patientsidan anger patientprofiler som registrerats på vårdgivar-kontot. Alla Dexcom Clarity-klinikanvändare har åtkomst till denna sida. För varje patient kan vårdgivaren ladda upp eller exportera rtCGM-data under besök, spara eller skriva ut rapporter, visa interaktiva rapporter, redigera eller radera information samt bjuda in patienter till att dela sina rtCGM-data. En enskild användare kan således välja att dela data med en vårdgivare antingen genom Clarity (med hjälp av den valfria molnbaserade funktionen), genom att använda tredjepartslösningar eller genom att använda Dexcom Uploader i samband med vårdbesök.

5 När en patient läggs till i klinikens Dexcom Clarity patientlista skapas inte ett Dexcom-konto automatiskt för denna patient. Patienter måste i stället skapa sitt eget konto i Dexcom Clarity om de vill visa eller ta del av CGM-data som har laddats upp på kliniken. En inbjudan innehåller en delningskod som patienterna anger i sitt personliga Dexcom-konto eller i Clarity-appen. När patienten har angett koden börjar kontona automatiskt att dela information sinsemellan. Via Dexcom Clarity kan en vårdgivare således ta del av data om en enskild person genom direktåtkomst till ett Dexcom-konto. Delningskoden och inbjudan till att dela data skickas via e-post till den enskilde användaren eller skrivs ut och ges till denne. Även glukosvärden från en Dexcom-mottagare kan laddas upp till vårdgivarens konto i Clarity-molnet. För enskilda användare som inte använder en app och istället använder en mottagare, måste mottagardata antingen laddas upp till användarens Dexcom-konto och delas med vårdgivaren eller laddas upp direkt till användarens journal i vårdgivarens Clarity-konto.

6 Dexcoms CGM-hårdvara kan inte i dagsläget införskaffas av enskilda individer för att monitorera glukosvärden i blodet på egen hand. Det är inga konsumentprodukter som kan köpas fritt av enskilda konsumenter utan kan endast erhållas efter förskrivning av en läkare.

7 Dexcom har uppgivit att dotterbolaget Dexcom (UK) Ltd. är personuppgiftsansvarig för enskilda privata användares personuppgifter i Clarity-molnet. Det framgår emellertid inte med all önskvärd tydlighet av Dexcoms integritetspolicy för enskilda användare vem som är personuppgiftsansvarig för behandlingen av personuppgifter i Dexcom-apparna och Clarity-molnet. Informationen når inte upp till kravet på koncis, klar, tydlig och begriplig information enligt artikel 12.1 och 13.1 a i dataskyddsförordningen. Informationen bryter därmed också mot principen om öppenhet i artikel 5.1 i samma förordning. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av

personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen. Dexcom har låtit meddela att integritetspolicyn ska justeras enligt följande: Dexcom (UK) Ltd. är personuppgiftsansvarig för de personuppgifter som behandlas i Clarity, Share och Dexcom-apparna när användarna finns i EU/EES, Schweiz eller Storbritannien.

8 Dexcom brister vidare i sina skyldigheter enligt dataskyddsförordningen genom att inte tillhandahålla i sin integritetspolicy för enskilda användare[1] en koncis, klar, tydlig och begriplig information enligt artikel 12.1 och 13.1 i dataskyddsförordningen om dels vilka specifika personuppgifter bolaget samlar in och lämnar ut till myndigheter för ändamålet kvalitets- och säkerhetsövervakning av medicintekniska produkter, dels med vilket undantag i artikel 9.2 i dataskyddsförordningen som bolaget behandlar enskilda personers hälsorelaterade personuppgifter i appar och i molntjänsten Dexcom Clarity. Informationen bryter därmed också mot principen om öppenhet i artikel 5.1 i samma förordning. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen. Dexcom har låtit meddela att den påstådda bristen kommer att beaktas i en framtida översyn av integritetspolicyn”

9 Det framgår inte heller av integritetspolicyn för enskilda användare[2] i vilken utsträckning Dexcom (UK) Ltd. i rollen som personuppgiftsansvarig tillämpar eller beaktar principerna om uppgiftsminimering eller lagringsminimering enligt artikel 5.1 i dataskyddsförordningen. Det finns inga beskrivningar av vilka personuppgifter och för vilka ändamål som uppgifter pseudonymiseras eller anonymiseras, bara att så sker. Det finns en påtaglig osäkerhet om Dexcom i rollen som personuppgiftsansvarig alls anonymiserar eller pseudonymiserar registrerades personuppgifter vid egen användning eller vid delning med partners och myndigheter. Dexcom har låtit meddela att den påstådda bristen kommer att beaktas i en framtida översyn av integritetspolicyn.

10 Dexcom (UK) Ltd. i Storbritannien baserar all sin personuppgiftsbehandling i rollen som personuppgiftsansvariga för enskilda privatpersoners personuppgifter på den rättsliga grunden ”avtal” (artikel 6.1 b i dataskyddsförordningen). Överföringsmekanismen till Storbritannien som är ett tredjeland är kommissionens beslut om att landet har en adekvat skyddsnivå. Dexcom har däremot inte tydligt angivit med vilken rättslig mekanism privatpersoners personuppgifter överförs från Storbritannien till USA eller andra tredjeländer. I Dexcoms integritetspolicy för enskilda användare anges att kommissionens standardavtalsklausuler (SCC) ligger till grund för all tredjelandsöverföring för exempelvis sms, e-post, support och framtida forskning. Å andra sidan inhämtas ett uttryckligt samtycke i appen och i Clarity-molnet för tredjelandsöverföring för ändamålet support.

11 Utgångspunkten i denna rättsutredning är att Dexcom lägger användarens uttryckliga samtycke till grund för överföringen av personuppgifter till tredjeländer för ändamålet

[1] Integritetspolicy för Dexcom den 25 februari 2021.
[2] Integritetspolicy för Dexcom den 25 februari 2021.

support med stöd av det specifika undantaget ”samtycke” i dataskyddsförordningen för tredjelandsöverföringar, artikel 49.1 a. Av den bestämmelsen framgår att den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder. Det har inte föreskrivits i dataskyddsförordningen något visst innehåll i informationen till den registrerade om riskerna med tredjelandsöverföring baserad på ett uttryckligt samtycke, 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. Dexcom uppfyller inte det kravet. Dexcom måste vara mer specifik med till vilka tredjeländer man överför användarens uppgifter och på vilket sätt dessa länder brister i sitt dataskydd. Denna brist på information om eventuella risker med sådana överföringar för ändamålen support och kundservice för de registrerade bedöms därmed innebära en hög risk för deras fri- och rättigheter. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen.

12 Artikel 49.1 är vidare bara tillämplig om det saknas ett beslut om adekvat skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46). Av Dexcoms integritetspolicy för enskilda användare av tjänsterna anför Dexcom att det använder sig av kommissionens standardavtalsklausuler vid överföring av personuppgifter från EU till tredjeland, t.ex. Filippinerna. Standardavtalsklausulerna är en skyddsåtgärd som är uttryckligen angiven i artikel 46 i dataskyddsförordningen. Dexcom kan således inte stödja sig på någon av bestämmelserna i artikel 49.1 eftersom artikel 46 är ”aktiverad”. Dexcom rekommenderas att justera sitt samtycke för tredjelandsöverföring (se ovan) så att det reflekterar de korrekta mekanismerna för tredjelandsöverföring för svenska invånares personuppgifter, dvs. kommissionens standardavtalsklausuler alternativt att tydligt ange att vilka uppgifter och ändamål för tredjelandsöverföring som omfattas av standardavtalsklausulerna och vilka andra uppgifter och ändamål som är undantagna dessa och som i stället baseras på de särskilda undantagen i artikel 49.1 i dataskyddsförordningen. Dexcom har låtit meddela att de påstådda bristerna i denna punkt och i punkt 11 kommer att beaktas i en framtida översyn av integritetspolicyn för Clarity.

13 Dexcom anlitar en flertal underleverantörer och dotterbolag för att behandla enskilda användares personuppgifter (18 stycken). Granskningen har därför begränsats till ett urval underleverantörer. Dexcom anlitar det amerikanska bolaget Google i Tyskland för drift och support av sina tjänster. Drift av Dexcoms data sker inom EU. Dexcom anlitar även, såvitt kan bedömas, det amerikanska bolaget Twilio, Inc. i USA för sms- och e-postmeddelanden. Dexcom samt leverantörerna Google och Twilio är amerikanska företag som, såvitt kan bedömas, enligt egna källor, policys och avtalsvillkor, inte utesluter att de kan behöva överföra personuppgifter tillhörande både patienters och anställd personal hos vårdgivare till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa

länder. Både Dexcoms och underleverantörerna Googles och Twilios avtal innehåller bl.a. ansvarsfriskrivningar för det fallet att de skulle tvingas av domstol att lämna ut uppgifter enligt bl.a. FISA 702 eller Cloud Act.

14 Det finns således en risk, trots vidtagna organisatoriska och tekniska åtgärder från Dexcoms sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Dexcom får dock betraktas som mycket låg. Dexcom har låtit meddela att man aldrig har mottagit en begäran om att lämna ut uppgifter med stöd av FISA. Det finns andra risker, t.ex. cyberattacker mot molntjänster generellt, som får betraktas som högre och mer allvarliga. Det erinras också att själva rtCGM-systemet inte är molnbaserat och att G6-produkterna kan användas utan molnfunktionalitet. Däremot är risken högre för att Twilio – leverantör av sms- och e-postmeddelanden i Dexcoms tjänster– omfattas av ett övervakningsprogram enligt Sektion 702 FISA. Motsvarande bedömning görs för de amerikanska leverantörerna Sumo Logic, Inc (logguppföljning), Zendesk, Inc (incidenthantering), Datadog, Inc. (logguppföljning), Snaplogic, Inc (plattforsmadministration), Cloudflare, Inc. (filtering oönskad kod) och Veeva, Inc (behandling av personuppgifter om hälso- och sjukvårdspersonal för marknadsföring).

15 Dexcoms avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver dessutom kompletteras med tydliga skriftliga instruktion från vårdgivare till Dexcom (UK) Ltd. om en rätt att tredjelandsöverföra personuppgifter till exempelvis Dexcom, Inc. i USA för nödvändig support och underhåll. Dexcom har låtit meddela att den påtalade bristen kommer att beaktas vid en framtida revision av avtalsvillkoren med svenska vårdgivare och personuppgiftsbiträdesavtal.

16 Dexcoms 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 Dexcom Clarity när denne efterfrågar uppgifterna. Dexcom är personuppgiftsansvarig för den enskildes Dexcom-konto 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 Dexcoms produkter, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att Dexcoms produkter kopplas direkt till vårdgivarens klinik-konto i Dexcom Clarity eller att vårdgivaren skapar egna hälsokonton och tillhandahåller användaruppgifter åt patienter i Dexcom Clarity. Så är inte fallet nu.

17 Den av Dexcom valda juridiska lösningen för Dexcom Clarity 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. En osäkerhetsfaktor i sammanhanget är om PDL förbjuder en vårdgivare att bereda sig

direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Dexcom) eller om lagen tillåter direktåtkomst eftersom den ligger utanför PDL:s tillämpningsområde. Rättsläget är alltså oklart. Genom tydligare information i personuppgiftspolicy för enskilda användare respektive avtalsvillkor för vårdgivare torde Dexcom 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 Dexcom och vårdgivare att tydligare reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke och att använda sig av direktåtkomst. Andra alternativ, som ska betraktas som rekommendationer, är att avtalsmässigt avgränsa vårdgivares användning av Dexcom-konto till egenvård inom ramen för ett egenvårdsbeslut, eller självhjälp, varvid användaren kan dela sina egenhändigt insamlade glukosvärden med en vårdgivare i Clarity för egenvårdsuppföljning genom s.k. ADB-utlämnande, inte genom direktåtkomst. Patienter däremot får enligt PDL ha direktåtkomst till en vårdgivares vårddokumentation, om vårdgivaren så tillåter, dvs. en direktåtkomst från sitt hälsokonto i Clarity-molnet till vårdgivarens klinikkonto i samma moln.

18 Beträffande vårdgivares inloggning till sitt klinik-konto i Dexcom Clarity lever bolaget (Dexcom (UK) Ltd.) i rollen som leverantör, tillika personuppgiftsbiträde, inte upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Beträffande sedan en enskild persons inloggning till sitt konto i Clarity lever Dexcom inte heller upp till kraven på stark autentisering. Beträffande slutligen apparna G6, Clarity och Follow 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 Dexcom Clarity ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter. Dexcom har låtit meddela att implementering av stark autentisering kommer att finnas i de relevanta Dexcom produkterna inom nästa år.

19 En vårdgivare kan 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 i Dexcom Clarity 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 som nyttjar Clarity som gör sig skyldig till den otillåtna behandlingen av personuppgifter. Dexcom rekommenderas att stänga funktionaliteten och uppmana vårdgivare att lämna delningskoden till patienten vid ett personligt besök på kliniken eller i inloggat läge i avvaktan på en säkrar lösning för delning.

20 På flera ställen i Dexcoms integritetspolicy för enskilda användare nämns ”forskning” som ett ändamål för bolagets vidareanvändning av registrerades personuppgifter. Integritetspolicyn har stora brister vad gäller Dexcoms användning av enskilda användares glukosdata för ändamålet ”forskning”. Den rättsliga grunden som Dexcom stödjer sig på är avtal (artikel 6.1 b i dataskyddsförordningen), men avser forskningen behandling av känsliga personuppgifter, dvs. hälsorelaterade uppgifter, krävs därutöver att behandlingen sker med ett uttryckligt samtycke av den registrerade enligt artikel 9.2 a eller med stöd av artikel 9.2 j och 89.1 såvida stöd finns i nationell rätt i det medlemsland inom EU där forskningen ska bedrivas. Om så är fallet bedöms Dexcom Clarity innefatta en otillåten personuppgiftsbehandling såvida användaren väljer att samtycka till framtida forskning. Det saknar betydelse att det rör sig om i huvudsak oidentifierbara uppgifter eftersom framtagandet av anonymiserade uppgifter kräver en behandling av personuppgifter för det specifika ändamålet. Erbjudandet till enskilda användare om att dela sina data för framtida forskning bör avskaffas. Ett alternativ är att Dexcom inhämtar samtycke till delning av data för redan etikgodkända forskningsstudier (inte framtida studier) i antingen Sverige eller andra länder. Dexcom har låtit meddela att den påstådda bristen kommer att beaktas i en framtida översyn av integritetspolicyn.

21 Den stora mängden kakor (ca 145 stycken) samt annan inbäddad spårningsteknik i Clarity-appen och i Clarity-molnet öppnar för risker för registreras fri- och rättigheter. Dexcom är emellertid tydlig med vilka specifika kakor som används, vilka finns publicerade i en cookiepolicy, och tillhandahåller verktyg för kontroll över dessa. Risken för otillåten behandling av personuppgifter får därför betraktas som låg.

Innehållsförteckning

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.

1.4 När en insulinpump kombineras med en CGM som skickar glukosvärden 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 nått önskvärd nivå. 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.[3] 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 datahanteringssystem
- Dexcom Clarity/Personal och appar
- Carelink System/Personal och appar

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

- Glooko

1.9 I denna promemoria utreds produkterna Dexcom G6-appen, Clarity-appen och Follow-appen och molntjänsten Dexcom Clarity.

1.10 Dexcom Real-Time CGM-system (rtCGM) består av ett flertal CE-märkta medicintekniska produkter, både hårdvaror och mjukvaror, som utvecklas och tillhandahålls av det amerikanska företaget Dexcom, Inc., fortsättningsvis benämnd Dexcom såvida inte annat anges. I Sverige distribueras Dexcoms produkter av Nordic Infucare AB, vilket bolag är en tredje part i förhållande till Dexcom.

1.11 Dexcom har en centraliserad organisationsstruktur. Dexcom Inc. i USA ansvarar för tillverkningen av mätanordningar (mottagare, sändare och applikatorer med integrerad sensor) och av den molnbaserade mjukvaran Clarity samt Dexcom-apparna. Dexcom International Ltd. (registrerat på Cypern, Nicosia) är exklusiv distributör för alla hårdvaruprodukter (mottagare, sändare och applikatorer med integrerad sensor) inom hela EU utanför Tyskland. Dexcom (UK) Ltd. baserat i Storbritannien ansvarar bl.a. för marknadsföring och distribution av Clarity och för tillhandahållande, support och drift av Clarity-tjänsten och Dexcom-apparna i Europa. Dexcom (UK) Ltd. är vidare dels personuppgiftsansvarig för enskilda privata användares personuppgifter i Clarity-molnet (se avsnitt 5), dels personuppgiftsbiträde åt svenska vårdgivare som skapar ett klinikkonto i Clarity.

1.12 Ansvarsområdena för kontinentaleuropeiska dotterbolag till Dexcom, Inc. är begränsade till distribution och marknadsföring av hårdvara (rtCGM-system), inklusive att säkerställa att hårdvaran innefattas i upphandlingar alternativt ingår som en förmån enligt medlemsländernas nationella socialförsäkringslagstiftning samt tillhandahållande av teknisk support, distributionshjälp och kundservice för slutanvändare inom EU.

1.13 Dexcom-hårdvaran utgör grunden för Dexcom rtCGM-systemet. Hårdvarorna består av en sensor, en sändare och en mottagare. Inga molnbaserade programvaror eller appar behövs för att använda rtCGM-systemet. Systemet fungerar som en fristående produkt och behöver inte anslutning till internet eller att den enskilda användaren ger åtkomst till andra. Enskilda användare kan emellertid komplettera hårdvaran med molnbaserade tjänster antingen från Dexcom eller tredje part, t.ex. Diasend/Glooko (se nedan). Det är således frivilligt. Endast rtCGM-hårdvaran säljs av Dexcom och är föremål för upphandlingar.

1.14 Dexcom har framhållit[4] att det inte finns några skillnader i användningen av Dexcoms molnbaserade mjukvara Clarity (tillhandahålls som ett frivilligt tillägg och gratis direkt till patienter som önskar använda den) eller molnlösningar från tredje part. Enskilda användare kan enligt Dexcom bekvämt använda mjukvarulösningar från tredje part, med eller utan moln, tillsammans med Dexcom rtCGM-systemet, eftersom Dexcoms produkter är interoperabla i enlighet med rådande branschstandard.

[4] Mejl från Dexcom inklusive synpunkter på laglighetsprövningen den 3 juni 2022.

Tredjepartsmjukvaran Diasend/Glooko är för närvarande den mest använda tjänsten i Sverige tillsammans med Dexcoms hårdvaror för glukosmonitorering och analys. Dexcom förklarar att deras egna mjukvaror är bara en av många lösningar som för närvarande finns på marknaden och används av patienter.

1.15 Dexcom G6-systemet är ett sensorbaserat, CE-märkt system för glukosmätning.[5] Dexcom G6 består av en sensor, sändare och mottagare. Data kan endast läsas från G6-mottagaren via ett USB-gränssnitt. Åtkomst till data lagrad i G6-mottagaren kräver fysisk åtkomst till enheten. I stället för G6-mottagaren kan en enskild användare välja att ladda ner appen Dexcom G6. G6-appen kan förutom att redovisa aktuell glukosnivå varna för höga eller låga nivåer. En användare kan även ladda ner Dexcom Clarity-appen som sammanställer rapporter, kurvor, diagram och grafer i Dexcoms molntjänst Clarity och kan på så sätt hjälpa användaren att förstå effekterna av insulindosering, matvanor, träning, och eventuella läkemedel. Dexcom Clarity-appen överför glukosvärden till molntjänsten Clarity. Även G6-mottaragen kan överföra glukosdata till molntjänsten Clarity. Dexcom-sensorn bärs på armen eller magen. Dexcom G6 är godkänd för patienter i åldrarna 2 och äldre. Glukosvärden från sändaren till appen överförs var femte minut om sändaren befinner sig inom räckhåll för den mobila enheten. Användaren kan välja att deaktivera sådana överföringar i appen genom att stänga av synkronisering till Dexcom Clarity. . Tre timmar efter överföring till Dexcoms servrar är glukosdata tillgänglig för rapporter. Mätvärden som överförs till Dexcoms molnbaserade tjänst Clarity sparas tills vidare så länge användaren inte säger upp sitt konto.[6] Dexcom har låtit meddela att en enskild användare är helt fri att bestämma om han eller hon vill använda den valfria molnbaserade funktionen i Clarity eller att avstå från användningen av Clarity helt.[7] Det framgår enligt Dexcom av användarmanualen för Dexcom Clarity som anger uttryckligen att den webbaserade lösningen är en stödfunktion för granskning, analys och utvärdering av rtCGM-jämförande data och dess status som ett "tillbehör" för Dexcom rtCGM-enheter.

1.16 G6-appen och Clarity-appen kräver att användaren skapar ett Dexcom-konto i Dexcoms molnbaserade tjänst Clarity. Användaren kan dela sina glukosvärden med en tredje part, t.ex. en vårdnadshavare eller en anhörig. I sådant fall krävs att den tredje parten använder Dexcom Follow-appen. Dexcoms rtCGM-system kan kombineras med insulinpumpar från flertal andra tillverkare, t.ex. t:slim X2insulinpump från Tandem Diabetes Care eller Ypsomed.

---

[5] Dexcom tillhandahåller även rtCGM-systemet G5. G6 är den senaste generationen rtCGM-system och vars nya funktioner inkluderar fabrikskalibrering, en 10-dagars användningsperiod för sensor, en snabbkopplingsapplikator, en ny varning för ”Akut lågt värde inom kort”, anpassningsbara dag- och nattvarningar (Notis-schema), ingen paracetamolinterferens och en diskret sändare med låg profil. G7 är en kommande generation.

[6] Dexcom har låtit meddela i ett mejl inklusive synpunkter på laglighetsprövningen den 3 juni 2022 att man raderar personuppgifter i enlighet med sina lagringspolicys för att säkerställa att Dexcom endast behandlar personuppgifter som är adekvata, korrekta, uppdaterade, relevanta och begränsade till vad som är nödvändigt i förhållande till ändamålen med behandlingen. Alla anställda på Dexcom är informerade om Dexcoms lagringspolicys och får lämplig utbildning i hur man följer policyerna. Dexcoms legal-avdelning ansvarar för tillsyn över och efterlevnad av Dexcoms lagringspolicyer och utför tillsyn på regelbunden basis.

[7] Mejl från Dexcom inklusive synpunkter på laglighetsprövningen den 3 juni 2022.

1.17 Dexcom erbjuder även användare av sina produkter möjligheten att överföra uppgifter till molntjänsten Glooko, tidigare Diasend. Glooko-molnet tillhandahålls av leverantören Glooko AB, dotterbolag till Glooko, Inc. i USA. I skrivande stund sker en migrering av användare i Diasend-molnet till Glooko-molnet. Diasend används i stor utsträckning av svenska vårdgivare för monitorering och uppföljning av diabetespatienter som bl.a. använder Dexcoms produkter. Diasend och Glooko kan lagra och analysera data från mer än 190 olika glukosmätare, insulinpumpar och CGM-system. Diasend, liksom Glooko, är CE-märkta produkter och används i ett flertal länder. Överföring till Diasend/Glooko förutsätter dock att en användare av Dexcoms produkter har ett Dexcom-konto. Diasends efterträdare, Glooko-molnet, analyseras i en separat laglighetsprövning.

1.18 Användare av Clarity-appen kan dela sina glukosmätningar och andra data med tio andra personer. Mottagaren behöver inte ha en särskild app, även om det finns en sådan tillgänglig, appen Dexcom Follow. Delning av data sker i tjänsten Clarity på clarity.dexcom.eu. Delning kan ske med hjälp av appen Clarity eller direkt på webben.

1.19 Molntjänsten Dexcom Clarity kan också användas av vårdgivare på en stationär dator. Clarity är en CE-märkt produkt. För detta syfte krävs programvaran Dexcom Uploader som laddas ner till aktuell klient. Gränssnittet är dock en webbläsare. Webbadressen för europeiska vårdgivare är clarity.dexcom.eu/professional. Inloggning sker med namn och lösenord. Varje vårdgivare skapar ett klinik-konto som hanteras av en administratör hos kliniken.[8] Administratören tilldelar sedan behörigheter till medarbetare hos vårdgivaren (”standardanvändare”). Patientsidan anger patientprofiler som registrerats på vårdgivar-kontot. Alla Dexcom Clarity-klinikanvändare har åtkomst till denna sida.

1.20 För varje patient kan vårdgivaren ladda upp eller exportera CGM-data under besök, spara eller skriva ut rapporter, visa interaktiva rapporter, redigera eller radera information samt bjuda in patienter till att dela sina CGM-data. När en patient läggs till i klinikens Dexcom Clarity patientlista skapas inte ett Dexcom-konto automatiskt för denna patient. Patienter måste i stället skapa sitt eget konto i Dexcom Clarity om de vill visa eller dela CGM-data som har laddats upp på kliniken. En inbjudan innehåller en delningskod som patienterna anger i sitt personliga Dexcom-konto eller i Clarity-appen. När patienten har angett koden börjar kontona automatiskt att dela information sinsemellan. Delningskoden och inbjudan till att dela data skickas via e-post till patienten eller skrivs och ges till patienten. Även glukosvärden från en Dexcom-mottagare kan laddas upp till vårdgivarens konto i Clarity-molnet. En enskild användare kan således välja att dela data med en vårdgivare antingen genom Clarity (med hjälp av den valfria molnbaserade funktionen), genom att använda tredjepartslösningar, t.ex. molntjänsten Diasend/Glooko, eller genom att använda Dexcom Uploader i samband med vårdbesök. För enskilda användare som inte använder en app och istället använder en mottagare, måste mottagardata antingen laddas upp till användarens Dexcom-konto och delas med vårdgivaren eller laddas upp direkt till användarens journal i vårdgivarens Clarity-konto.

[8] Dexcom Clarity. Användarhandbok för kliniker.

1.21 Det finns en möjlighet för vårdgivare att ladda upp en patients glukosdata anonymt till Clarity-molnet.. Om en vårdgivare som använder programvaran Clarity överför mottagardata från patientens mottagare till programvaran Clarity via en fysisk USB-anslutning, har vårdgivaren möjlighet att anonymt ladda upp patientdata så att den endast kan läsas och analyseras för respektive session. Data kommer inte att sparas vid denna anslutning. När vårdgivaren återgår till patientens lista kommer de inte att kunna komma åt patientens data. Det finns en möjlighet för medarbetare hos en vårdgivare att inkludera en identifierare (ID) som visas överst i rapporterna (för utskrift), men denna rapport (och identifierare) är inte tillgänglig när de återvänder till patientens lista eller stänger webbläsaren. ID-informationen raderas även från Dexcoms servrar inom 24 timmar. Dexcom avråder uttryckligen från användningen av identifierbar information som patientens namn eller födelsedatum i detta fält. Det bör noteras att vid anonym användning, under uppladdningen, fångas endast klinikens IP-adress, men inte identifierare som hänför sig till patienten.

1.22 Dexcom Clarity kräver användning av kakor för en rad olika syften, som insamling av data om webbplatsanvändning, hantering av innehåll, anpassat innehåll och webbtrafikmätning och -analys. Mer information om användning av Dexcoms kakor finns i bolagets cookiepolicy på dexcom.com. Användning av kakor i tjänsten behandlas i avsnitt 15.

Uppdrag och frågeställningar

2.1 SKR har begärt en laglighetsprövning av Dexcom-apparna och molntjänsten Dexcom Clarity. Laglighetsprövningen är avgränsad till själva behandlingen och skyddet av personuppgifter i apparna respektive molntjänsten 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 produkter och 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.

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 §).

Vilka registerförfattningar är tillämpliga på Dexcoms appar och Clarity?

4.1 Dexcoms CGM-hårdvara är ett verktyg enbart för vårdgivare för att bedriva diabetesvård. Dexcoms produkter kan alltså inte inhandlas på konsumentmarknaden i Sverige utan måste förskrivas av en läkare. Dexcom tillhandahåller således en komplett systemlösning optimerad för att hälso- och sjukvården ska kunna utreda och erbjuda patienter möjligheten att kontinuerligt mäta glukoshalten i blodet. Patienter kan egenmonitorera glukosövervakning med hjälp av Dexcoms appar (G6 och Clarity) och ett Dexcom-konto. Mätvärden sparas automatiskt i Dexcoms molnbaserade tjänst Clarity så länge det finns ett aktivt konto, såvida inte patienten stänger av överföringen.

4.2 Patienter har vidare möjlighet att dela sina mätvärden med upp till tio andra personer via Dexcoms tjänst Clarity. Det kräver att mottagaren också tecknar ett Dexcom-konto. Mottagarens behörighet tilldelas av patienten. Vårdgivare förfogar även över en applikation för att ta emot mätvärden för ett flertal patienter. Applikation kräver lokal installation i vårdgivarens systemmiljö. Via webbläsare kan en vårdgivare skapa patientprofiler samt ladda ner data med patientens medgivande från dennes Dexcom-konto.

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 produkten för att bedriva kontinuerlig glukosmonitorering av en patient på distans (**distanssjukvård**) är PDL i huvudsak tillämplig på behandlingen av personuppgifter i produkten och stödjande digitala tjänster. 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 4.7.

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. För dessa produkter gäller 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.[9] 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. Dexcoms CGM-system utgör exempel på den typen av produkter.

4.9 Sammanfattningsvis är Dexcoms rtCGM-hårdvara inte konsumentprodukter. De är inte avsedda för konsumentbruk, dvs. självhjälp. Produkterna är avsedda att användas enbart i enlighet med en ordination av läkare inom ramen för antingen hälso- och sjukvård (distanssjukvård) eller egenvård enligt ett egenvårdsbeslut av en vårdgivare. Som utgångspunkt är PDL tillämplig på en vårdgivares behandling av enskilda individers personuppgifter i Dexcoms produkter, och dataskyddsförordningen är tillämplig på Dexcoms behandling av personuppgifter som sker inom ramen för den enskildes egenvård i hemmet.

Vem är personuppgiftsansvarig?

Bedömning: Dexcom har uppgivit att dotterbolaget Dexcom (UK) Ltd. är personuppgiftsansvarig för enskilda privata användares personuppgifter i Clarity-molnet. Det framgår emellertid inte med all önskvärd tydlighet av Dexcoms integritetspolicy för enskilda användare vem som är personuppgiftsansvarig för behandlingen av personuppgifter i Dexcom-apparna och Clarity-molnet. Informationen når inte upp till kravet på koncis, klar, tydlig och begriplig information enligt artikel 12.1 och 13.1 a i dataskyddsförordningen. Informationen bryter därmed också mot principen om öppenhet i artikel 5.1 i samma förordning. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen. Dexcom har låtit meddela att

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

integritetspolicyn ska justeras enligt följande: Dexcom (UK) Ltd. är personuppgiftsansvarig för de personuppgifter som behandlas i Clarity, Share och Dexcom-apparna när användarna finns i EU/EES, Schweiz eller Storbritannien".[10]

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 Follow-appen eller Dexcom Clarity via webbläsare för distanssjukvård samt för uppföljning av egenvård (egenmonitorering) är patientansvarig vårdgivare personuppgiftsansvarig. För all annan personuppgiftsbehandling i Clarity-molnet samt G6- respektive Clarity-appen är Dexcom personuppgiftsansvarig, dvs. för enskilda användares egna genererade data.

5.3 Av Dexcoms integritetspolicy för enskilda användare[11] avseende Dexcom Clarity och tillhörande appar framgår emellertid att med ”Dexcom” avses ”den Dexcom-enhet som tillhandahåller produkterna och tjänsterna till dig enligt villkoren för respektive produkter och tjänster och därmed fungerar som kontrollant med avseende på dina personuppgifter som samlas in eller behandlas i samband med sådana produkter och tjänster; eller det dotterbolag som din personinformation lagligen delades med i enlighet med denna sekretesspolicy.”

5.4 Av artikel 12.1 i dataskyddsförordningen framgår att den personuppgiftsansvarige ska tillhandahålla information till registrerade, bl.a. om personuppgiftsansvaret, i en koncis, klar, tydlig, begriplig och lätt tillgänglig form. Kravet på transparens i personuppgiftsbehandlingen är en grundläggande dataskyddsprincip (artikel 5.1 a). Se vidare avsnitt 7. Dexcoms information om personuppgiftsansvar, särskilt med tanke att apparna och Clarity-tjänsten riktar sig till barn, är inte alls tydlig med vem som är personuppgiftsansvarig för behandlingen av personuppgifter i appar och Clarity-molnet. Om flera av bolagen i Dexcom-koncernen är tillsammans personuppgiftsansvariga för en viss typ av personuppgiftsbehandling, ska det anges. Att räkna upp alla dotterbolag runt om i världen uppnår inte till kravet på en ”koncis, klar, tydlig och begriplig” information till registrerade. För övrigt noteras ”Dexcom Sweden AB” som nämns i Dexcoms integritetspolicy inte längre existerar.

5.5 Dexcoms representant i Sverige, Nordic Infucare, har på begäran låtit meddela att Dexcom (UK) Ltd. är personuppgiftsansvarig för enskilda användares personuppgifter i Clarity-molnet.[12] Dexcom har låtit meddela att integritetspolicyn beskriver tydligt att den Dexcom-enhet som den enskilda privata användaren ingår avtal med också kommer att vara personuppgiftsansvarig. Inom EU/EES är Dexcom (UK) Ltd. avtalspart gällande Clarity. Faktum kvarstår dock att den information som tillhandahålls registrerade vidlåder brister i fråga om vilket av bolagen som bär personuppgiftsansvaret.

[10] Dexcoms kommentarer på laglighetsprövningen den 23 juni 2022.
[11] Integritetspolicy för Dexcom den 25 februari 2021.
[12] Mejlkonversation den 22 mars 2022.

Användarvillkoren för bl.a. Clarity-tjänsten från den 21 februari 2021 är lika oklar med vem den enskilda användaren ingår avtal med. Kravet på en ”koncis, klar, tydlig och begriplig” information i denna del är inte uppfyllt. Fortsättningsvis används ”Dexcom” som beteckning för detta personuppgiftsansvar, om inte annat anges. Dexcom har låtit meddela att integritetspolicyn ska justeras enligt följande: ”Dexcom (UK) Ltd. är personuppgiftsansvarig för de personuppgifter som behandlas i Clarity, Share och Dexcom-apparna när användarna finns i EU/EES, Schweiz eller Storbritannien".[13]

5.6 Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda sanktionsavgifter (artikel 83.5 a i dataskyddsförordningen).

5.7 Privatundantaget i dataskyddsförordningen är inte tillämplig på Dexcoms behandling av personuppgifter om en enskild användare eftersom företaget använder enskild individs personuppgifter för egna ändamål eller delar dessa med en vårdgivare på uppdrag av den enskilde (se avsnitt 4).

Rättslig grund och tillåtna ändamål för behandling av personuppgifter

Bedömning: Dexcom brister i sina skyldigheter enligt dataskyddsförordningen genom att inte tillhandahålla i sin integritetspolicy för enskilda användare[14] en koncis, klar, tydlig och begriplig information enligt artikel 12.1 och 13.1 i dataskyddsförordningen om bl.a. dels vilka specifika personuppgifter bolaget samlar in och lämnar ut till myndigheter för ändamålet kvalitets- och säkerhetsövervakning av medicintekniska produkter, dels med vilket undantag i artikel 9.2 i dataskyddsförordningen som bolaget behandlar enskilda personers hälsorelaterade personuppgifter i appar och i molntjänsten Dexcom Clarity. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen. Dexcom har låtit meddela att den påstådda bristen kommer att beaktas i en framtida översyn av integritetspolicyn.

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.[15]

6.2 Vårdgivares distanssjukvård av patient med stöd av ett Clarity-klinikkonto eller Follow-appen är således en tillåten behandling enligt PDL, såvida behandlingen är nödvändig för ändamålet och de grundläggande dataskyddsprinciperna i dataskyddsförordningen

[13] Dexcoms kommentarer på laglighetsprövningen den 23 juni 2022.
[14] Integritetspolicy för Dexcom den 25 februari 2021.
[15] SOU 2017:66 s. 227.

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 G6-sensor åt en invånare för egenvård konstituerar inte automatiskt ett personuppgiftsansvar för vårdgivaren för all behandling av personuppgifter i Follow-appen eller i molntjänsten Dexcom Clarity. Däremot torde en vårdgivare anses som personuppgiftsansvarig för hälsokonton som vårdgivaren skapar åt en invånare; det får presumeras att i dessa fall avser vårdgivaren att bedriva hälso- och sjukvård (distanssjukvård) med hjälp av tjänsten och ingenting annat. En vårdgivare kan emellertid inte skapa konton åt en patient i Dexcom Clarity, varför övervägande skäl talar för att Dexcoms produkter i kombination med G6- eller Clarity-appen bara kan användas inom ramen för egenvård enligt Socialstyrelsens egenvårdsföreskrifter (se avsnitt 4).

6.3 Vid egenvård (egenmonitorering) genom hälsoappar m.m. enligt ett egenvårdsbeslut 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 Dexcoms *insamling* av enskilda användares personuppgifter för deras nyttjande av bolagets tjänster för glukosövervakning är inte tillämplig. Här bortses från rättsliga grunder för andra ändamål, såsom marknadsföring, kvalitets- och säkerhetsövervakning av medicintekniska produkter och forskning.

6.4 Av Dexcoms integritetspolicy för enskilda användare[16] framgår att bolaget behandlar enskilda användares personuppgifter i ”*Överensstämmelse med tillämpliga lagar och skydd av våra legitima affärsintressen, juridiska rättigheter och skyldigheter*.” Med detta torde menas att Dexcom (UK) Ltd. behandlar personuppgifter i rollen som personuppgiftsansvarig med stöd av den rättsliga grunden ”rättslig förpliktelse” enligt artikel 6.1 i dataskyddsförordningen.

6.5 Till stöd för den rättsliga grunden rättslig förpliktelse åberopar Dexcom i den nämnda handlingen skyldighet ”*att avslöja dina personuppgifter som svar på en laglig begäran från offentliga myndigheter, inklusive för att uppfylla nationella säkerhets-[…] krav och i enlighet med krav som ställs från myndigheter som reglerar medicinsk utrustning i det land där du befinner dig*”. Med detta menas reglering av 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.

[16] Integritetspolicy för Dexcom den 25 februari 2021.

6.6 Det framgår dock inte helt klart vilka specifika personuppgifter Dexcom samlar in och lämnar ut till myndigheter för ändamålet kvalitets- och säkerhetsövervakning av medicintekniska produkter. Det är en brist i integritetspolicyn för enskilda användare, och därmed mot kraven på koncis, klar, tydlig och begriplig information enligt artikel 12.1 i dataskyddsförordningen (se avsnitt 5 och 7).

6.7 Dexcom samlar i huvudsak in personuppgifter för ändamålet att tillhandahålla tjänsten genom en frivillig överenskommelse (avtal) mellan parterna i syfte att låta invånare primärt komma i åtnjutande av bolagets Clarity-tjänster. Det innebär att om en invånare säger upp sitt Dexcom-konto, och därmed den rättsliga grunden för Dexcoms 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”.

6.8 Utöver den rättsliga grunden ”avtal” behöver leverantören ytterligare rättsligt stöd för att få behandla känsliga personuppgifter, såsom uppgifter om hälsa (artikel 9.2 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). Övriga undantag från förbudet kan inte åberopas av leverantören i rollen som personuppgiftsansvarig och berörs därför inte här.

6.9 I G6 och Clarity-appen och Dexcom Clarity behandlar Dexcom i rollen som personuppgiftsansvarig enskilda användares, dvs. enskilda privatpersoners användning av produkten, personuppgifter med stöd av det avtal (Allmänna villkor) som användaren tecknar i samband med öppnande av ett Dexcom-konto, vilket är korrekt. Det framgår av Dexcoms integritetspolicy för enskilda användare.[17]

6.10 Däremot framgår inte med all önskvärd tydlighet av integritetspolicyn under rubriken *Vad är den rättsliga grunden för behandlingen av mina personuppgifter*? att Dexcom behandlar en användares hälsorelaterade uppgifter, som ju utgör känsliga personuppgifter, med stöd av ett uttryckligt samtycke. I stället används benämningar såsom ”*där du har givit ditt samtycke*” eller ”*specifikt har identifierats i samtycke som du ger oss*” osv. Det erinras att det ska röra sig om ett ”uttryckligt” samtycke genom någon form av aktiv handling, t.ex. en kryssruta, för att vara giltig.

6.11 Det ska alltså framgå med all önskvärd tydlighet av integritetspolicyn med vilket villkor från förbudet i artikel 9.2 i dataskyddsförordningen som Dexcom samlar in och vidareanvänder hälsorelaterade uppgifter. Det är en självklar förutsättning för en användare att få en överblick över Dexcoms rättsliga grunder innan denne tecknar ett konto (se avsnitt 7 om informationsskyldigheten för personuppgiftsansvariga enligt dataskyddsförordningen).

[17] Integritetspolicy för Dexcom den 25 februari 2021.

6.12 För Dexcoms insamling av hälsorelaterade personuppgifter i samband med tillhandahållande av tjänsterna är ett uttryckligt samtycke (artikel 9.2 a) det enda rimliga alternativet eller undantaget för behandlingen av personuppgifter om hälsa eftersom bolaget varken är en myndighet eller vårdgivare. För fortsatt behandling för andra ändamål, t.ex. säkerhets- och kvalitetskrav avseende medicintekniska produkter, om personuppgifter om hälsa över huvud taget är nödvändiga, aktualiseras artikel 9.2 f (behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk). Dexcom brister således i den skyldighet bolaget har att i en koncis, klar, tydlig och begriplig information enligt artikel 12.1 i dataskyddsförordningen beskriva med vilket eller vilka undantag i artikel 9.2 i dataskyddsförordningen som bolaget behandlar enskilda personers hälsorelaterade personuppgifter i appar och i molntjänsten Dexcom Clarity.

6.13 Dexcom har förklarat att man avser att förtydliga sin integritetspolicy och att uttryckligen ange vilka tillsynsmyndigheter Dexcom delar personuppgifter med (särskilt avseende tillsyn av medicintekniska produkter). Den påstådda bristen kommer enligt Dexcom att beaktas i en framtida översyn av integritetspolicyn.

6.14 Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda sanktionsavgifter (artikel 83.5 a i dataskyddsförordningen).

6.15 Dexcom inhämtar vidare ett uttryckligt samtycke för framtida forskning på en användares personuppgifter när denne tecknar ett Dexcom-konto. Framställningen återkommer till denna fråga i avsnitt 15.

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 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 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).

7.5 I avsnitt 5 och 6 noteras brister i Dexcoms information till registrerade om bl.a. vem som är personuppgiftsansvarig för behandlingen av personuppgifter i appar och Clarity-molnet samt villkor för behandlingen av registrerades hälsorelaterade personuppgifter och vilka specifika personuppgifter bolaget samlar in och lämnar ut till myndigheter för ändamålet kvalitets- och säkerhetsövervakning av medicintekniska produkter.

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).

8.10 Vid vårdgivares nyttjande av Clarity-klinikkonton är Dexcom (UK) Ltd. personuppgiftsbiträde.

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.

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.[18] EDPB har vidare publicerat ett utkast till riktlinjer som klargör vad som utgör, och inte utgör, en överföring av personuppgifter till tredjeland.[19] Riktlinjerna är i skrivande stund föremål för synpunkter.

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.

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

Applikationerna G6 och Clarity samt molntjänsten Dexcom Clarity

Bedömning:
Det framgår inte heller av integritetspolicyn för enskilda användare i vilken utsträckning Dexcom i rollen som personuppgiftsansvarig tillämpar eller beaktar principerna om uppgiftsminimering eller lagringsminimering enligt artikel 5.1 i dataskyddsförordningen. Det finns en påtaglig osäkerhet om Dexcom i rollen som personuppgiftsansvarig alls anonymiserar eller pseudonymiserar registrerades personuppgifter vid egen användning eller vid delning med partners och myndigheter. Dexcom har låtit meddelat att den påstådda bristen kommer att beaktas i en framtida översyn av integritetspolicyn.

12.1 Dexcom är leverantör av rtCGM-systemet G6 bestående av sensor, sändare och mottagare och därutöver apparna G6 och Clarity samt Dexcoms Clarity-moln för glukosövervakning. rtCGM-systemet G6 är FDA-godkända och CE-märkta produkter.

[18] 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.
[19] Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

12.2 G6-appen tillsammans med G6-sensorn tillåter användare att mäta och registrera glukosvärden när som helst och var som helst. Analys av föregående CGM, händelser och mönster sker i Dexcoms mjukvara Clarity. Bärbara insulinpumpar från flertal andra tillverkare, t.ex. t:slim X2insulinpump från Tandem Diabetes Care eller Ypsomed kan kopplas till Dexcoms sensor. Managering av pumpen och glukosövervakning kan ske i molntjänsten Dexcom Clarity eller i pumpleverantörens molntjänst. Dexcom-hårdvaran kan även kommunicera med andra tredjepartsmolntjänster, såsom Diasend/Glooko som en användare frivilligt kan välja i stället för Dexcoms Clarity-moln. Användaren kan dela sina glukosdata med t.ex. vårdnadshavare eller anhöriga. Det förutsätter att anhöriga respektive vårdnadshavare laddar ner Dexcom Follow-appen. Appen kräver att användaren tecknar ett konto i Dexcom Clarity. Vårdgivare kan skapa ett klinikkonto i molntjänsten Dexcom Clarity. Ett klinikkonto kräver att särskild programvara (Upload) installeras lokalt hos vårdgivaren. En vårdgivare kan via Dexcom Clarity lagra uppgifter som samlats in från en enskild användares mottagare, från enskilda användares Dexcom-konton eller från en tredjepartsmolntjänst, såsom Diasend/Glooko. Uppgifter från insulinpumpar, monitorer och blodsockermätare kan skickas till systemet, sparas och sedan användas för att generera olika rapporter och översikter, t.ex. behandlingsrekommendationer.

12.3 Enligt Dexcom har hela Clarity CGM-systemet byggts med säkerhet i åtanke.[20] Lämpliga skyddsåtgärder inkluderar individuella användarkonton till vilka åtkomst endast ges med ett giltigt användarnamn och lösenord. Personuppgifter krypteras när de överförs från sändare eller pump till avläsare eller app, och sedan krypteras personuppgifterna igen när de överförs från patientens app till servern för Dexcom Clarity. Servern för Dexcom Clarity övervakas kontinuerligt för skydd mot eventuella attacker och intrång. Dexcom granskar regelbundet sina policyer och rutiner och den fysiska miljön för dess utrustning för att förbättra de tekniska och organisatoriska åtgärder som vidtas med avseende på säkerhetsåtgärder i syfte att skydda användares personuppgifter (inklusive patienters hälsouppgifter) mot oavsiktlig, olaglig eller obehörig spridning, förändring eller förstörelse.

12.4 Dexcom använder Google Cloud i Tyskland för drift och underhåll av servrar för Dexcom Clarity vilkas användare finns i Europa (se vidare avsnitt 13). All data i Clarity är krypterad, både i vila och vid transport. Dexcom använder inte ett distribuerat molnlagringssystem för att skydda mot dataförlust i händelse av en naturlig eller annan katastrofal händelse. Glukosdata förvaras inte separerad från privata användares kontouppgifter. Européers kundinformation lagras inom EU (Tyskland) för bättre integritetsskydd.

12.5 Dexcom-sensorer överför personliga glukosvärden och annan data på ett säkert sätt till appar och avläsare med krypterad Bluetooth-teknik. Dexcom framhåller att hela Clarity-plattformen har byggts med integritet i åtanke. EU-medborgare och medborgare inom ESS garanteras av Dexcom en rätt att få utöva sina rättigheter enligt dataskyddsförordningen. Google i Tyskland betraktas av Dexcom som en betrodd

[20] Dexcom Clarity Data Security and Privacy rev. 002

molntjänstleverantörer som är certifierad enligt ISO 27001 Ledningssystem för informationssäkerhet. Även Dexcom är certifierad enligt ISO 27001 och andra standarder inom det medicintekniska området.

12.6 Av Dexcoms integritetspolicy för enskilda användare[21] framgår att bolaget delar ”personuppgifter” med ”dotterbolag”, ”tjänsteleverantörer”, ”myndigheter”, ”distributörer” för en mängd olika ändamål som är desamma oavsett mottagare, såsom för att tillhandahålla tjänsterna (inklusive utveckling, underhåll och support av produkter och tjänster), för att leverera produkter och tjänster till användare, upprätta, utföra och upprätthålla ett kontrakt med användare, marknadskommunikation, utskick av enkäter, för att efterleva tillämplig lagstiftning, forskning och för att framställa, utöva eller försvara juridiska krav och lagliga rättigheter”. Det är emellertid oklart, bortsett från dotterbolagen, vilka andra aktörer Dexcom delar registrerades ”personuppgifter” med och vilka slag av personuppgifter som används för de olika ändamålen. Enligt dataskyddsförordningen är detta särskilt relevant i informationen till registrerade i situationer ”där mängden olika aktörer och den tekniska komplexiteten gör det svårt för den registrerade att veta och förstå om personuppgifter som rör honom eller henne samlas in, vem som gör det och för vilket syfte […] (skäl 58 i dataskyddsförordningen). Av artikel 13.1 e i dataskyddsförordningen framgår dock att den registrerade ska få information om mottagarna eller kategorier av mottagare som ska få ta del av den registrerades personuppgifter. Det kravet får anses uppfyllt av Dexcom.

12.7 Det framgår dock inte i vilken utsträckning Dexcom tillämpar principerna om uppgiftsminimering eller lagringsminimering enligt artikel 5.1 i dataskyddsförordningen vid delning av personuppgifter med andra aktörer och myndigheter. Av Dexcoms integritetspolicy för enskilda användare[22] framgår förvisso att bolaget kan samla in och använda icke identifierbar information för alla ändamål i den utsträckning som detta tillåts i tillämplig lagstiftning när den registrerade interagerar med bolaget på något sätt. Dexcom anger i integritetspolicyn för enskilda användare att bolaget samlar in och behandlar icke identifierbar information för affärsändamål och för att bedriva och hantera verksamheten, inklusive utveckling, underhåll och support av produkter och tjänster. Dexcom anonymiserar och pseudonymiserar registrerades personuppgifter vid egen användning, men det är oklart i vilken utsträckning det sker vid delning med partners och myndigheter.

12.8 Informationen i integritetspolicyn för enskilda användare[23] eller av annan dokumentation når inte helt upp till kravet på koncis, klar, tydlig och begriplig information enligt artikel 12.1 i dataskyddsförordningen. Informationen bryter därmed också mot principen om öppenhet i artikel 5.1 i samma förordning. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen.

[21] Integritetspolicy för Dexcom den 25 februari 2021.
[22] Integritetspolicy för Dexcom den 25 februari 2021.
[23] Integritetspolicy för Dexcom den 25 februari 2021.

12.9 Dexcom förklarar att man avser att uppdatera sin integritetspolicy och förtydliga vilka riskreducerande åtgärder man vidtar avseende personuppgiftsbehandlingen.[24] Den påstådda bristen kommer enligt Dexcom att beaktas i en framtida översyn av integritetspolicyn.

12.10 Det noteras dock att Dexcom i sitt *personuppgiftsbiträdesavtal* som tecknas med svenska vårdgivare på ett föredömligt sätt uttömmande beskrivit anlitade underleverantör, vilka agerar som underbiträden åt de personuppgiftsansvariga vårdgivarna. En motsvarande uttömmande beskrivning i integritetspolicyn för enskilda användare skulle skapa större transparens för registrerade vad gäller spridningen av den registrerades personuppgifter till andra aktörer. Dexcom har dock framhållit[25] att detaljerad information om varje mottagare på grund av att sådan information är värdefull för hackare och andra som är intresserade av att göra dataintrång. Därför prioriterar Dexcom patienters säkerhet samtidigt som de tillhandahåller den information som krävs enligt dataskyddsförordningen.

12.11 Dexcom sparar användares glukosvärden och annan data i molnet, dvs. i Dexcom Clarity, så länge det finns ett aktivt konto, såvida inte patienten stänger av överföringen. Ett Dexcom-konto krävs alltid för att använda Dexcoms produkter, men användaren kan stänga dataöverföring från Dexcoms produkter till molnet. En användare kan således begränsa överföring av data från appen till molnet. Dexcoms mätare sparar däremot inte glukosvärden i molnet utan enbart i mätaren. Data kan delas med en vårdgivare genom antingen att denne tankar av data i mätaren till egen dator eller till Dexcoms molntjänst för vårdgivare, Dexcom Clarity eller en extern molnbaserad tredjepartstjänst såsom Diasend/Glooko..

12.12 Inloggning i Dexcoms appar sker utan någon stark autentisering. Användares åtkomst till egen data i Dexcom Clarity (clarity.dexcom.eu) sker med enfaktorsautentisering (användarnamn och lösenord). Åtkomst kan än så länge inte ske med Bank-ID eller annat elektroniskt ID. Såvitt förstås loggar vårdgivare in på sitt klinik-konto i Dexcom Clarity med användarnamn och lösenord. De kan inte nyttja SITHS-kort eller annat slag av e-legitimation. I Dexcom-kontot, liksom i apparna, kan en användare ta del av glukosvärden och annan data över tid såsom dagliga mönster, tid i målvärdesområde, medelvärde för glukos.

12.13 Användare av Dexcoms produkter kan dela sina elektroniska glukosvärden med en vårdgivare som har ett klinik-konto i Dexcoms molntjänst Clarity och där skapat en patientprofil för användaren. Av Dexcoms integritetspolicy för enskilda användare[26] finns ett avsnitt med rubriken ”*Organisatoriska slutanvändare*”. Där framgår att “organisatoriska slutanvändare” är “underlagda organisationens sekretesspolicy och informationspraxis”. Av Dexcoms standardiserade personuppgiftsbiträdesavtal[27] som används när bl.a. svenska vårdgivare i rollen som personuppgiftsansvariga nyttjar

[24] Dexcoms kommentarer på laglighetsprövningen den 23 juni 2022.
[25] Mejl från Dexcom inklusive synpunkter på laglighetsprövningen den 3 juni 2022.
[26] Integritetspolicy för Dexcom den 25 februari 2021.
[27] Dexcoms personuppgiftsbiträdesavtal

Dexcom Clarity-molnet framgår att "*For the avoidance of doubt, the DPA does not apply to the data processing operations based on the Dexcom's or its affiliates agreements with patients in connection with their use of Dexcom CLARITY*." Personuppgiftsbiträdesavtalet är således tydligt med att vårdgivaren är personuppgiftsansvarig för sina egna medarbetares och patienters personuppgiftsbehandling i ett Clarity klinikkonto, inte Dexcom.

12.14 Av Dexcoms standardiserade personuppgiftsbiträdesavtal framgår vidare att ett dotterbolag i Storbrittanden agerar i rollen som personuppgiftsbiträde åt svenska vårdgivare, Dexcom (UK) Ltd. Storbritannien är godkänd av kommissionen som ett tredjeland med en adekvat skyddsnivå enligt dataskyddsförordningen. I personuppgiftsbiträdesavtalet saknas dock kommissionens nya standardiserade avtalsklausuler (SCC) för tredjelandsöverföring.

12.15 Av integritetspolicyn för enskilda användare berörs även utsedda mottagare som den registrerade utser eller instruerar Dexcom om att dela dennes personuppgifter med. Utsedda mottagare är bl.a. "vårdgivare".

12.16 Dexcom nämner i sin integritetspolicy för enskilda användare[28] att bolaget använder sig av kommissionens standardavtalsklausuler vid överföring av personuppgifter från EU till tredjeland, t.ex. Filippinerna. I integritetspolicyn nämns som exempel på syften kundservice eller support. Dexcom anför i sin integritetspolicy följande: "*Dessa länder kanske inte har lagar gällande datasekretess eller skydd som motsvarar lagarna i ditt eget land. I sådant fall kan vi förlita oss på mekanismer som är tillåtna enligt lagarna i det land där du befinner dig för att påverka överföringen så att den omfattas av lämpliga skyddsåtgärder*."

12.17 När en privat användare skapar för första gången sitt konto i Dexcom Clarity, efterfrågar tjänsten samtycke av användaren för att låta Dexcom (UK) Ltd. överföra personuppgifter, inklusive hälsorelaterade uppgifter, till Dexcom, Inc. i USA för support. Enligt information i appen Clarity sker överföringen med beaktande av lämpliga skyddsåtgärder för att möjliggöra teknisk support. Dexcom synes lägga användarens uttryckliga samtycke till grund för överföringen av personuppgifter mellan Sverige och USA med stöd av det specifika undantaget "samtycke" i dataskyddsförordningen för tredjelandsöverföringar, artikel 49.1 a. Av den bestämmelsen framgår att den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder. Någon information i appen om vilka risker som överföringen medför för en svensk användare finns inte.

12.18 Av integritetspolicyn för enskilda användare[29] framgår inte vilka underleverantörer Dexcom anlitar. I integritetspolicyn nämns bl.a. företaget Twilio för användare i Japan

[28] Integritetspolicy för Dexcom den 25 februari 2021
[29] Integritetspolicy för Dexcom den 25 februari 2021

och Sydkorea beträffande sms och e-post. Varför Dexcom i övrigt inte förmedlar information om underleverantörer beträffande användare i andra länder inom EU är oklart.

12.19 Av Dexcoms integritetspolicy för enskilda användare[30] framgår att bolaget kan röja den information som samlas in från användare, inklusive hälsouppgifter, för att uppfylla ”*en laglig begäran från offentliga myndigheter, inklusive för att uppfylla nationella säkerhets- eller brottsbekämpningskrav i det land där du befinner dig*.” Och vidare: ”*Vi kan bli skyldiga att lämna ut dina personuppgifter vid en domstol eller vid ett administrativt förfarande för att efterleva tillämplig lagstiftning, och för att framställa, utöva eller försvara juridiska krav och lagliga rättigheter*”. Av policyn framgår inte om Dexcom informerar användare om rättsliga processer som söker tillgång till dennes information, såsom domstolsbeslut eller stämningar.

12.20 Av Dexcoms personuppgiftsbiträdesavtal med svenska vårdgivare[31] framgår bl.a., att Dexcom “*shall not use the Controller’s Personal Data for any purpose other than described in the Contract and to fulfill its obligations under the Contract, unless required by applicable law*.” Och vidare: ”*The Processor shall notify the Controller of the Processor’s point of contact for all issues related to data protection within the scope of the Contract.*”

12.21 Som framhållits finns inte kommissionens standardavtalsklausuler bilagt eller inbäddat i varken Dexcoms användarvillkor för enskilda användare eller i Dexcoms personuppgiftsbiträdesavtal. I det senare fallet är ett standardavtalsvillkor inte nödvändigt för överföringen av svenska vårdgivares medarbetares och patienters personuppgifter till Storbritannien. Kommissionen har godkänt Storbritannien som ett land med en adekvat skyddsnivå. Däremot sker en tredjelandsöverföring när dotterbolaget Dexcom (UK) Ltd. överför personuppgifter till bl.a. Dexcom, Inc. i USA Modul 3 i kommissionens standardavtalsklausuler ska appliceras i en sådan tredjelandsöverföring (personuppgiftsbiträde till personuppgiftsbiträde).

12.22 Enligt integritetspolicyn för enskilda användare[32] samt cookie-policy[33] för Dexcom Clarity och tillhörande appar använder Dexcom kakor. Dessa används för att hjälpa bolaget att förbättra sin service, prestanda, förhindra robotar och främja användarupplevelser. Enligt Dexcom kan kakorna även komma att samla in information om användning av andra webbplatser, appar och onlinetjänster som den registrerade använder. Av cookiepolicyn framgår inte specifikt vilka personuppgifter som samlas in av Dexcom eller tredjepartsaktörer som tillhandahåller kakorna. Dexcom nämner dock i integritetspolicyn att IP-nummer och platsinformation kan samlas in. Däremot listas alla kakor. Förutom nödvändiga kakor använder Dexcom funktionella kakor (ca 13 stycken), prestandakakor (ca 22 stycken) och riktade kakor för främst marknadsföring (ca 110 stycken). Tredjepartskakor, dvs. kakor som placeras i användarens dator av en annan

[30] Integritetspolicy för Dexcom den 25 februari 2021.
[31] Dexcoms personuppgiftsbiträdesavtal.
[32] Integritetspolicy för Dexcom den 25 februari 2021.
[33] Cookiepolicy för Dexcom januari 2022

aktör än Dexcom, förekommer inom alla kategorierna av kakor, men mest inom kategorin riktade kakor.

12.23 Dexcom tillhandahåller allmän information i integritetspolicyn hur man kan ta bort kakor eller begränsa dem.

Tredjepartsapplikationer och tredjepartsaktörer avseende Dexcom Clarity

13.1 Som redovisas i avsnitt 12 driftas Dexcoms back-end för Dexcom Clarity samt apparna av det amerikanska företaget Google LLC (Google) i USA. Google agerar här i rollen som personuppgiftsbiträde åt Dexcom och underbiträde till personuppgiftsbiträdet Dexcom (UK) Ltd som är det bolag som agerar i rollen som personuppgiftsbiträde åt svenska vårdgivare.

13.2 Som framgår av avsnitt 12 informerar inte Dexcom i sin integritetspolicy för enskilda användare[34] vilka tredjepartsaktörer som bolaget delar svenska användares personuppgifter med för olika ändamål. Det framgår bara olika kategorier av mottagare. Det går därför inte att bedöma omfattningen av spridningen av registrerades personuppgifter, t.ex. till antalet leverantörer eller till mottagare i tredjeland. Inte heller om spridningen sker anonymiserat eller pseudonymiserat. Det finns en påtaglig osäkerhet om Dexcom i rollen som personuppgiftsansvarig alls anonymiserar eller pseudonymiserar registrerades personuppgifter vid egen användning eller vid delning med partners och myndigheter.

13.3 Som också redovisas i avsnitt 12 överför Dexcom både användares och svensk hälso- och sjukvårdspersonals personuppgifter till bl.a. USA för ändamålet kundsupport. Sannolikt överför Dexcom, såvitt kan bedömas genom nyttjandet av Twilio, Inc, och i brist på annan information, sms- och e-postmeddelanden till USA. Några absoluta garantier för att européers personuppgifter stannar i Europa ges alltså inte av Dexcom.

13.4 Dexcom stödjer sin tredjelandsöverföring av vårdgivares patientuppgifter och medarbetares uppgifter till Storbritannien på ett standardiserat personuppgiftsbiträdesavtal och ett beslut om adekvat skyddsnivå (artikel 46 i dataskyddsförordningen). För överföringen av vårdgivares uppgifter om patienter vidare till USA och andra tredjeländer för vissa ändamål, såsom teknisk support, saknas uppgift om adekvata skyddsåtgärder, såsom kommissionens standardavtalsklausuler (SCC). Beträffande tredjelandsöverföring av invånares personuppgifter till USA verkar Dexcom stödja sig på både SCC och bestämmelserna om undantagssituationer i särskilda situationer i dataskyddsförordningen, artikel 49. Framställningen återkommer till frågorna i avsnitt 15.

13.5 Dexcom använder en mängd olika kakor på clarity.dexcom.eu. Kakorna används för ett flertal olika ändamål. Flertalet av kakorna tillhandahålls av amerikanska leverantörer

[34] Integritetspolicy för Dexcom den 25 februari 2021.

(Salesforce, Snapchat m.fl.). Överföring av personuppgifter till USA eller till annat tredjeland via Dexcoms underleverantörer m.fl. kan inte uteslutas.

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 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 (Dexcom 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[35]).
    - 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

[35] 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.

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.

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 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 är inte inbäddade i vare sig Dexcoms användarvillkor för enskilda användare eller personuppgiftsbiträdesavtal med vårdgivare. 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.

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

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

leverantörens lagstiftning är straffbart. Det är omständigheter som en myndighet måste väga in i sin skadeprövning när utländska molntjänstleverantörer övervägs i verksamheten.

Har personuppgifter i Dexcoms appar samt i tjänsten Dexcom Clarity ett godtagbart skydd?

Bedömning: Dexcoms rtCGM-hårdvara kan inte i dagsläget införskaffas av enskilda individer för att monitorera glukosvärden i blodet på egen hand. Det är således inga konsumentprodukter som kan köpas fritt av enskilda konsumenter utan kan endast erhållas efter förskrivning av en läkare. Dexcoms appar (G6, Clarity och Follow) kan däremot alltid införskaffas av enskilda privata användare gratis. Alternativt kan en användare även nyttja tredjepartsmolnbaserade tjänster, t.ex. Diasend/Glooko.

Dexcom (UK) Ltd. i Storbritannien (fortsättningsvis Dexcom om inte annat anges) baserar all sin personuppgiftsbehandling i rollen som personuppgiftsansvariga för enskilda privatpersoners personuppgifter på den rättsliga grunden ”avtal” (artikel 6.1 b i dataskyddsförordningen). Överföringsmekanismen till Storbritannien som är ett tredjeland är kommissionens beslut om att landet har en adekvat skyddsnivå. Dexcom har däremot inte tydligt angivit med vilken rättslig mekanism privatpersoners personuppgifter överförs från Storbritannien till USA eller andra tredjeländer. I Dexcoms integritetspolicy för enskilda användare anges att kommissionens standardavtalsklausuler (SCC) ligger till grund för all tredjelandsöverföring för exempelvis sms, e-post, support och framtida forskning. Å andra sidan inhämtas ett uttryckligt samtycke i appen och i Clarity-molnet för tredjelandsöverföring för ändamålet support.

Utgångspunkten i denna rättsutredning är att Dexcom lägger användarens uttryckliga samtycke till grund för överföringen av personuppgifter till tredjeländer för ändamålet support med stöd av det specifika undantaget ”samtycke” i dataskyddsförordningen för tredjelandsöverföringar, artikel 49.1 a. Av den bestämmelsen framgår att den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.

Dexcom är tydlig med i sin integritetspolicy för enskilda användare[37] av tjänsterna att överföring av personuppgifter, inklusive hälsorelaterade uppgifter, kan ske ”till exempel till Filippinerna för ändamålen kundsupport och teknisk support”. Dexcom uppger dock inte i sin integritetspolicy på vad sätt bolagets leverantörer av tredjepartstjänster i tredjeländer inte uppfyller dataskydds- och säkerhetsbestämmelser enligt dataskyddsförordningen. Dexcom har inte heller uttömmande beskrivit till vilka tredjeländer man överför användarens uppgifter, till vilka mottagare, på vilken rättslig

[37] Integritetspolicy för Dexcom den 25 februari 2021.

grund och på vilket sätt dessa länder brister i sitt dataskydd om samtycke enligt artikel 49.1 a utgör den rättsliga grunden för överföringen.

Det har inte föreskrivits i dataskyddsförordningen något visst innehåll i informationen till den registrerade om riskerna med tredjelandsöverföring baserad på ett uttryckligt samtycke, 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. Dexcom uppfyller inte det kravet. Dexcom måste vara mer specifik med till vilka tredjeländer man överför användarens uppgifter och på vilket sätt dessa länder brister i sitt dataskydd.

Denna brist på information om eventuella risker med sådana överföringar för ändamålen support och kundservice för de registrerade bedöms därmed innebära en hög risk för deras fri- och rättigheter. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen.

Artikel 49.1 är vidare bara tillämplig om det saknas ett beslut om adekvat skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46). Av Dexcoms integritetspolicy för enskilda användare av tjänsterna anför Dexcom att det använder sig av kommissionens standardavtalsklausuler vid överföring av personuppgifter från EU till tredjeland, t.ex. Filippinerna. Standardavtalsklausulerna är en skyddsåtgärd som är uttryckligen angiven i artikel 46 i dataskyddsförordningen. Dexcom kan således inte stödja sig på någon av bestämmelserna i artikel 49.1 eftersom artikel 46 är ”aktiverad”. Dexcom rekommenderas att justera sitt samtycke för tredjelandsöverföring (se ovan) så att det reflekterar de korrekta mekanismerna för tredjelandsöverföring, dvs. kommissionens standardavtalsklausuler alternativt att tydligt ange vilka uppgifter och ändamål för tredjelandsöverföring som omfattas av standardavtalsklausulerna och vilka andra uppgifter och ändamål som är undantagna dessa och som i stället baseras på de särskilda undantagen i artikel 49.1 i dataskyddsförordningen.

Dexcom anlitar en flertal underleverantörer och dotterbolag för att behandla enskilda användares personuppgifter (18 stycken). Granskningen har därför begränsats till ett urval underleverantörer. Dexcom anlitar det amerikanska bolaget Google i Tyskland för drift och support av sina tjänster. Drift av Dexcoms data sker inom EU. Dexcom anlitar även, såvitt kan bedömas, det amerikanska bolaget Twilio, Inc. i USA för sms- och e-postmeddelanden. Dexcom samt leverantörerna Google och Twilio är amerikanska företag som, såvitt kan bedömas, enligt egna källor, policys och avtalsvillkor, inte utesluter att de kan behöva överföra personuppgifter tillhörande både patienters och anställd personal hos vårdgivare till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Både Dexcoms och underleverantörerna

Googles och Twilios avtal innehåller bl.a. ansvarsfriskrivningar för det fallet att de skulle tvingas av domstol att lämna ut uppgifter enligt bl.a. FISA 702 eller Cloud Act.

Det finns således en risk, trots vidtagna organisatoriska och tekniska åtgärder från Dexcoms sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Dexcom får dock betraktas som mycket låg. Dexcom har låtit meddela att man aldrig har mottagit en begäran om att lämna ut uppgifter med stöd av FISA. Det finns andra risker, t.ex. cyberattacker mot molntjänster generellt, som får betraktas som högre och mer allvarliga. Det erinras också att själva rtCGM-systemet inte är molnbaserat och att G6-produkterna kan användas utan molnfunktionalitet. Däremot är risken högre för att Twilio – leverantör av sms- och e-postmeddelanden i Dexcoms tjänster– omfattas av ett övervakningsprogram enligt Sektion 702 FISA. Motsvarande bedömning görs för de amerikanska leverantörerna Sumo Logic, Inc (logguppföljning), Zendesk, Inc (incidenthantering), Datadog, Inc. (logguppföljning), Snaplogic, Inc (plattforsmadministration), Cloudflare, Inc. (filtering oönskad kod) och Veeva, Inc (behandling av personuppgifter om hälso- och sjukvårdspersonal för marknadsföring).

Dexcoms avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver dessutom kompletteras med tydliga skriftliga instruktion från vårdgivare till Dexcom (UK) Ltd. om en rätt att tredjelandsöverföra personuppgifter till exempelvis Dexcom, Inc. i USA för nödvändig support och underhåll. Dexcom har låtit meddela att den påtalade bristen kommer att beaktas vid en framtida revision av avtalsvillkoren med svenska vårdgivare och personuppgiftsbiträdesavtal.

Dexcoms 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 Dexcom Clarity när denne efterfrågar uppgifterna. Dexcom är personuppgiftsansvarig för den enskildes Dexcom-konto 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 Dexcoms produkter, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att Dexcoms produkter kopplas direkt till vårdgivarens klinik-konto i Dexcom Clarity eller att vårdgivaren skapar egna hälsokonton och tillhandahåller användaruppgifter åt patienter i Dexcom Clarity. Så är inte fallet nu.

Den av Dexcom valda juridiska lösningen för Dexcom Clarity 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. En osäkerhetsfaktor i sammanhanget är om PDL förbjuder en vårdgivare att bereda sig

direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Dexcom) eller om lagen tillåter direktåtkomst eftersom den ligger utanför PDL:s tillämpningsområde. Rättsläget är alltså oklart. Genom tydligare information i personuppgiftspolicy för enskilda användare respektive avtalsvillkor för vårdgivare torde Dexcom 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 Dexcom och vårdgivare att tydligare reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke och att använda sig av direktåtkomst. Andra alternativ, som ska betraktas som rekommendationer, är att avtalsmässigt avgränsa vårdgivares användning av Dexcom-konto till egenvård inom ramen för ett egenvårdsbeslut, eller självhjälp, varvid användaren kan dela sina egenhändigt insamlade glukosvärden med en vårdgivare i Clarity för egenvårdsuppföljning genom s.k. ADB-utlämnande, inte genom direktåtkomst. Patienter däremot får enligt PDL ha direktåtkomst till en vårdgivares vårddokumentation, om vårdgivaren så tillåter, dvs. en direktåtkomst från sitt hälsokonto i Clarity-molnet till vårdgivarens klinikkonto i samma moln.

Beträffande vårdgivares inloggning till sitt klinik-konto i Dexcom Clarity lever bolaget (Dexcom (UK) Ltd.) i rollen som leverantör, tillika personuppgiftsbiträde, inte upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Beträffande sedan en enskild persons inloggning till sitt konto i Clarity lever Dexcom inte heller upp till kraven på stark autentisering. Beträffande slutligen apparna G6, Clarity och Follow 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 Dexcom Clarity ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter. Dexcom har låtit meddela att implementering av stark autentisering kommer att finnas i de relevanta Dexcom produkterna inom nästa år.

En vårdgivare kan 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 i Dexcom Clarity 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 som nyttjar Clarity som gör sig skyldig till den otillåtna behandlingen av personuppgifter. Dexcom rekommenderas att stänga funktionaliteten och uppmana vårdgivare att lämna delningskoden till patienten vid ett personligt besök på kliniken eller i inloggat läge i avvaktan på en säkrar lösning för delning.

På flera ställen i Dexcoms integritetspolicy för enskilda användare nämns ”forskning” som ett ändamål för bolagets vidareanvändning av registrerades personuppgifter. Integritetspolicyn har stora brister vad gäller Dexcoms användning av enskilda användares glukosdata för ändamålet ”forskning”. Den rättsliga grunden som Dexcom stödjer sig på är avtal (artikel 6.1 b i dataskyddsförordningen), men avser forskningen behandling av känsliga personuppgifter, dvs. hälsorelaterade uppgifter, krävs därutöver att behandlingen sker med ett uttryckligt samtycke av den registrerade enligt artikel 9.2 a eller med stöd av artikel 9.2 j och 89.1 såvida stöd finns i nationell rätt i det medlemsland inom EU där forskningen ska bedrivas. Om så är fallet bedöms Dexcom Clarity innefatta en otillåten personuppgiftsbehandling såvida användaren väljer att samtycka till framtida forskning. Det saknar betydelse att det rör sig om i huvudsak oidentifierbara uppgifter eftersom framtagandet av anonymiserade uppgifter kräver en behandling av personuppgifter för det specifika ändamålet. Erbjudandet till enskilda användare om att dela sina data för framtida forskning bör avskaffas. Ett alternativ är att Dexcom inhämtar samtycke till delning av data för redan etikgodkända forskningsstudier (inte framtida studier) i antingen Sverige eller andra länder. Dexcom har låtit meddela att den påstådda bristen kommer att beaktas i en framtida översyn av integritetspolicyn.

Den stora mängden kakor (ca 145 stycken) samt annan inbäddad spårningsteknik i Clarity-appen och i Clarity-molnet öppnar för risker för registreras fri- och rättigheter. Dexcom är emellertid tydlig med vilka specifika kakor som används, vilka finns publicerade i en cookiepolicy, och tillhandahåller verktyg för kontroll över dessa . Risken får otillåten behandling av personuppgifter får därför betraktas som låg.

15.1 Föreliggande laglighetsprövningen av Dexcoms CGM-system är enligt uppdrag avgränsad till själva behandlingen och skyddet av personuppgifter i apparna och tredjepartsapplikationer. Uppdraget är att redovisa om personuppgiftsbehandlingen i produkterna 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 Dexcom, Inc. är ett amerikansk bolag. Bolaget representeras i Sverige av det svenska bolaget Nordic Infucare. Personuppgiftsansvarig för enskilda privata användares användning av appar och molntjänster är Dexcom (UK) Ltd. i Storbritannien. I rollen som personuppgiftsansvarig, vilken roll Dexcom (UK) Ltd. har beträffande behandling av personuppgifter vid egenvård, är dataskyddsförordningen tillämplig på personuppgiftsbehandlingen i Dexcoms tjänster och appar enligt artikel 3.2 a i dataskyddsförordningen eftersom bolaget utbjuder varor och tjänster till vårdgivare inom unionen, oavsett om moderbolaget inte är etablerat i unionen. Motsvarande gäller Dexcom (UK) Ltd. som agerar i rollen som personuppgiftsbiträde åt svenska vårdgivare.

15.5 Det s.k. privatundantaget i artikel 2.2 c i dataskyddsförordningen bedöms inte vara tillämplig vid enskilda användares nyttjande av Dexcoms appar och tjänster eftersom bolaget använder användarnas 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. Dexcom (UK) Ltd. är därmed personuppgiftsansvarig för all behandling av enskildas personuppgifter i produkterna. Dataskyddsförordningen är tillämplig på den personuppgiftsbehandlingen av det skälet.

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

Tystnadsplikt

15.7 Personalen verksamma vid moderbolaget Dexcom, Inc. i USA omfattas 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 leverantörer vars medarbetare är fysiskt verksamma i Sverige. Tystnadsplikt för det personuppgiftsansvariga bolaget Dexcom och dess medarbetare måste i stället avtalsregleras. En sådan avtalad tystnadsplikt finns reglerad i Dexcoms integritetspolicy för enskilda användare[38] av Dexcom Clarity[39], och i Dexcoms personuppgiftsbiträdesavtal med bl.a. svenska vårdgivare. Några disciplinära eller andra sanktioner mot enskild medarbetare hos Dexcom, Inc. som bryter den avtalade tystnadsplikten, t.ex. i form av löneavdrag, avskedande, vite eller skadestånd, har inte identifierats. Avtalad tystnadsplikt innebär generellt sett ett svagare skydd än en lagstiftad, straffsanktionerad tystnadsplikt på individnivå som kan rendera böter eller fängelse.

15.8 Dexcom anlitar underbiträdena Google i Tyskland för applikationsförvaltning och lagring av hälsorelaterade personuppgifter i Dexcom Clarity samt, så långt kunnat identifieras, Twilio, Inc i USA för sms- och e-postmeddelanden. Lagring av Clarity-data

[38] Integritetspolicy för Dexcom den 25 februari 2021.
[39] Integritetspolicy för Dexcom den 25 februari 2021.

sker i Tyskland. Lagring av sms- och e-postmeddelanden sker i USA (Twilio). Lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter är inte tillämplig heller på dessa bolag eftersom data förvaltas i annat land än Sverige.

15.9 Lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter är inte tillämplig på Dexcom och anlitade leverantörs medarbetare. I Tyskland kompletteras dataskyddsförordningens av en federal lagstiftning, Bundesdatenschutzgesetz (BDSG). Enligt 42 § kan den som röjt eller lämnat ut personliga eller kommersiella uppgifter till en tredje person utan samtycke för ersättning samt med påverkan för ett stort antal personer dömas upp till tre års fängelse eller böter. Talan om ett sådant åtal kan enbart väckas av berörda individer, personuppgiftsansvarig eller delstatens dataskyddsmyndighet. Det finns således en straffsanktionerad tystnadsplikt i Tyskland för bl.a. anställda hos molntjänstleverantörer som har verksamhet i landet. I Sverige renderar brott mot en lagstadgad tystnadsplikt upp till ett års fängelse, vilket är ett lägre straff än den tyska straffpåföljden. Tyskland får därmed anses har ett fullgott skydd mot obehörigt röjande av personuppgifter hos personuppgiftsbiträden verksamma i Tyskland. I detta fall Google.

15.10 Dotterbolaget Dexcom (UK) Ltd. agerar i rollen både som personuppgiftsansvarig för enskilda användares Dexcom-konton och tillhörande appar respektive personuppgiftsbiträde åt svenska vårdgivare när dessa använder Dexcom Clarity. Det följer av brittisk lag att medarbetare hos personuppgiftsbiträden kan åtalas och dömas för brott mot brittiska Data Protection Act om de obehörigen röjer uppgifter som avser den personuppgiftsansvariges verksamhet, t.ex. svenska vårdgivare. Storbritannien får därmed anses har ett fullgott skydd mot obehörigt röjande av personuppgifter hos personuppgiftsbiträden verksamma i landet. I detta fall Dexcom (UK) Ltd. Vad gäller rollen som personuppgiftsansvarig för enskilda privata användares personuppgifter i Clarity-molnet finns ingen, såvitt kunnat utredas, straffsanktionerad tystnadsplikt i brittisk lagstiftning för Dexcom (UK) Ltd:s medarbetare vid hanteringen av personuppgifter relaterade till hälsa. I stället förlitar sig Dexcom på avtalad tystnadsplikt som ger ett sämre skydd än en lagstadgad tystnadsplikt.

15.11 Twilio, Inc., liksom andra amerikanska underleverantörer som Dexcom anlitar, lagrar data i USA. I USA finns inte, såvitt är känt, en straffsanktionerad tystnadsplikt specifikt för personuppgiftsbiträden som ska motverka obehörigt röjande av kunddata. Det innebär att när en vårdgivare använder Dexcoms tjänster för att bedriva distanssjukvård eller egenvård, enskilda individers hälsorelaterade uppgifter har ett svagare skydd vid förvar hos Dexcoms personuppgiftsbiträden än när de är fysiskt förvarade hos en svenska vårdgivare.

Överföringar av personuppgifter till USA och andra länder

15.12 Dexcom anlitar en flertal underleverantörer och dotterbolag för att behandla enskilda användares personuppgifter (18 stycken såvitt kan bedömas). Granskningen har därför begränsats till ett urval underleverantörer. Dexcom samt leverantörerna Google och Twilio, Inc. är amerikanska företag som, såvitt kan bedömas, enligt egna källor, policys

och avtalsvillkor, inte utesluter att de kan behöva överföra personuppgifter tillhörande både privatpersoners, patienters och anställd personal hos vårdgivare till USA och andra tredje länder och med ansvarsfriskrivningar för utlämnanden av uppgifter enligt bl.a. FISA 702 eller Cloud Act till amerikanska myndigheter (se avsnitt 12 och 14). I Dexcoms fall är bolaget tydlig med i sin integritetspolicy för enskilda användare av tjänsterna[40] att överföring av personuppgifter, inklusive hälsorelaterade uppgifter, kan ske ”*till exempel” till Filippinerna för ändamålen kundsupport och teknisk support*.” Det finns således ingen uttömmande beskrivning av till vilka tredjeländer och mottagare Dexcom lämnar ut registrerades personuppgifter. Inte heller anges med vilken rättslig grund denna överföring sker.

15.13 Beträffande överföringen av enskilda användares personuppgifter från EU/EES-området till USA för ändamålet support enligt uppgift i Clarity-appen, dvs. enskilda personer som använder Dexcom Clarity för egenvård enligt en vårdgivares förskrivning av Dexcoms produkter inom ramen för ett egenvårdsbeslut, sker enligt bolaget överföringen, såvitt förstås, i enlighet med stöd av undantaget för tredjelandsöverföring, artikel 49.1 a i dataskyddsförordningen (uttryckligt samtycke). Data är krypterade under överföring genom användning av krypteringsnycklar som hanteras på ett säkert sätt. Användaren samtycker till tredjelandsöverföringen genom ett uttryckligt samtycke antingen i Clarity-appen eller i Dexcom Clarity vid registrering av ett konto. Av appen framgår följande: ”*Om du har problem med ditt Dexcom-system eller om du har frågor hur du använder det kan Dexcoms tekniska supportpersonal få granska din hälsoinformation och annan användningsinformation för att felsöka dina problem eller svara på din fråga. I förekommande fall godkänner du överföringen av dina uppgifter utanför EES till Dexcom, Inc. med beaktande av lämpliga skyddsåtgärder för att möjliggöra förbättrad teknisk support.”* Genom en kryssruta accepterar den enskilda användaren överföringen till Dexcom, Inc., vilket inte nödvändigtvis innebär en överföring enbart till USA utan också till leverantörer i andra länder som Dexcom anlitar.

15.14 Av artikel 49.1 a i dataskyddsförordningen framgår att en tredjelandsöverföring får ske om den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder. Det är oklart med vilken mekanism Dexcom överför enskilda personers glukosuppgifter till åtminstone USA – standardavtalsklausulerna eller artikel 49.1 a? Eftersom Dexcom efterfrågar ett explicit samtycke för överföringen utgår denna rättsutredning från att Dexcom i stället för standardavtalsklausulerna nyttjar ett samtycke enligt artikel 49.1 a i dataskyddsförordningen för sin tredjelandsöverföring av personuppgifter.

15.15 Artikel 49.1 a i dataskyddsförordningen är en legitim grund som kan åberopas av Dexcom för sin tredjelandsöverföring av enskilda användares personuppgifter för avsedda ändamål. Överföring är dessutom enligt Dexcoms villkor under användarens

[40] Integritetspolicy för Dexcom den 25 februari 2021.

kontroll genom att denne kan stänga av överföringen av glukosvärden från sensorer och pumpar till Dexcom Clarity..

15.16 Det har inte föreskrivits i dataskyddsförordningen något visst innehåll i informationen till den registrerade om riskerna med tredjelandsöverföring baserad på ett uttryckligt samtycke, 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. Dexcom uppger dock inte i sin integritetspolicy för enskilda användare[41] på vad sätt bolagets leverantörer av tredjepartstjänster i tredjeländer inte uppfyller dataskydds- och säkerhetsbestämmelser enligt dataskyddsförordningen. Dexcom har inte heller uttömmande beskrivit till vilka tredjeländer man överför användarens uppgifter, till vilka mottagare, på vilken rättslig grund enligt artikel 6.1 i dataskyddsförordningen och på vilket sätt dessa länder brister i sitt dataskydd om samtycke utgör den rättsliga grunden för överföringen, t.ex. att utlänningar i USA saknar rättsliga och effektiva möjligheter att utöva kontroll över sina personuppgifter som är förvarade hos myndigheter.

15.17 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.[42]

15.18 Dexcom kunde ha varit mer specifik med till vilka tredjeländer man överför användarens uppgifter 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 skulle de hamna i förvar hos amerikanska myndigheter**.** Som minimum ska anges i informationen till registrerade tredjeländernas namn liksom kategorier av mottagare. I sistnämnda hänseende bedöms Dexcom uppfylla kraven i dataskyddsförordningen, men inte i det förstnämnda. **Denna brist på information om eventuella risker med sådana överföringar för ändamålen support och kundservice för de registrerade bedöms därmed innebära en hög risk för deras fri- och rättigheter. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt dataskyddsförordningen.**

[41] Integritetspolicy för Dexcom den 25 februari 2021.
[42] Beslut 2022-03-28, dnr DI-2019-4062.

15.19 Artikel 49.1 är vidare bara tillämplig om det saknas ett beslut om adekvat skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46). Av Dexcoms integritetspolicy för enskilda användare av tjänsterna[43] anför Dexcom att det använder sig av kommissionens standardavtalsklausuler vid överföring av personuppgifter från EU till tredjeland, t.ex. Filippinerna. Standardavtalsklausulerna är en skyddsåtgärd som är uttryckligen angiven i artikel 46 i dataskyddsförordningen. Dexcom kan således inte stödja sig på någon av bestämmelserna i artikel 49.1 eftersom artikel 46 är ”aktiverad”. **Dexcom rekommenderas att justera sitt samtycke för tredjelandsöverföring (se ovan) så att det reflekterar de korrekta mekanismerna för tredjelandsöverföring av svenska invånares personuppgifter, dvs. kommissionens standardavtalsklausuler alternativt att tydligt ange vilka uppgifter och ändamål för tredjelandsöverföring som omfattas av standardavtalsklausulerna och vilka andra uppgifter och ändamål som är undantagna dessa och i stället baseras på de särskilda undantagen i artikel 49.1 i dataskyddsförordningen**.

15.20 Dexcom har låtit meddela att de påstådda bristerna i punkterna 15.18 och 15.19 kommer att beaktas i en framtida översyn av integritetspolicyn för Clarity.

15.21

15.22 Beträffande Dexcoms personuppgiftsbiträdesavtal med svenska vårdgivare finns inget omnämnande av kommissionens standardavtalsklausuler som en mekanism för tredjelandsöverföring mellan Dexcom (UK) Ltd (personuppgiftsbiträde och exempelvis Dexcom, Inc. (underbiträde) för exempelvis kundsupport. Det framgår av artikel 28.3 a i dataskyddsförordningen att när personuppgifter 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 och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I det avtalet eller den rättsakten ska det enligt punkt a särskilt föreskrivas att personuppgiftsbiträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, ”inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation.”

15.23 Standardavtalsklausulerna är varken omnämnda i eller bilagda till Dexcoms avtalsvillkor inklusive personuppgiftsbiträdesavtal med svenska vårdgivare eftersom standardavtalsklausulerna normalt inte ska ingås mellan en svensk vårdgivare och Dexcom. Inc. utan mellan Dexcom (UK) Ltd. (dataexportör) och t.ex. Dexcom, Inc. (dataimportören). Det framgår inte att några standardavtalsklausuler kan tillhandahållas vårdgivare på begäran. Det är oklart vilken modul i standardavtalsklausulerna som används. Däremot framgår det av personuppgiftsbiträdetsavtalet ett åtagande från Dexcom (UK) Ltd. enligt följande: “Each and every transfer of data to a state which is

[43] Integritetspolicy för Dexcom den 25 februari 2021.

not a Member State of either the EU, the EEA or Switzerland shall only occur if the specific conditions of Articles 44 et seqq. GDPR have been fulfilled."

15.24 Den personuppgiftsansvarige är ansvarsskyldig för att personuppgiftsbehandling som utförs av personuppgiftsbiträdet följer den personuppgiftsansvariges instruktioner, inklusive tredjelandsöverföring. Det är oklart huruvida kommissionens standardavtalsklausuler ska utgöra en del av instruktionerna. Dataskyddsförordningen är inte tydlig på den punkten. Å andra sidan framgår av artikel 28.1 att personuppgiftsbiträdet ska kunna ge tillräckliga garantier för skyddet av den personuppgiftsansvariges personuppgifter genom tekniska och organisatoriska åtgärder. Det är således inte nödvändigt att den personuppgiftsansvarige i alla delar ska instruera personuppgiftsbiträdet hur denne ska förfara med personuppgifter och framför allt skydda dem. Dexcom har emellertid garanterat i det standardiserade personuppgiftsbiträdesavtal som tecknas med bl.a. svenska vårdgivare att tredjelandsöverföringar endast får ske med stöd av de överföringsmekanismer som framgår av dataskyddsförordningen. Att kommissionens standardavtalsklausuler inte är införda i Dexcoms avtalsvillkor med vårdgivare och att det därmed inte framgår vilka klausuler och moduler i standardavtalsklausulerna som är tillämpliga är således inte en brist.

15.25 Dexcoms avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver dock **kompletteras med tydliga skriftliga instruktion från vårdgivare till bolaget om en rätt att tredjelandsöverföra personuppgifter** till exempelvis Dexcom, Inc. i USA för nödvändig support och underhåll. Dexcom har låtit meddela att den påtalade bristen kommer att beaktas vid en framtida revision av avtalsvillkoren med svenska vårdgivare och personuppgiftsbiträdesavtal.

15.26 Dexcoms produkter och molntjänster syftar till att låta enskilda användare att effektivt övervaka och behandla sin diabetes. Dexcom är således inte en tillhandahållare av generella tjänster till allmänheten eller till företag utan erbjuder sina tjänster till en smal krets av användare för ett tydligt medicinskt syfte. Det väcker frågan om Dexcom Clarity 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 Dexcom Clarity är bara relaterade till enskilda personers glukosvärden. Dexcom använder därtill end-to-end kryptering i syfte att skydda överföringar av data och kunddata. Dexcom har vidare framfört[44] att krypering av data appliceras också vid vila (vid lagring på media, diskar, etc.) med hjälp av starka kryptografiska chiffer och protokoll. En fullständig diskkrypteringslösning är enligt Dexcom installerad på alla klientslutpunkter (bärbara och stationära datorer) för att kryptera data i vila. Dexcom anför att en lösning för hantering av mobila enheter tvingar fram kryptering på alla mobila enheter som hanteras. Dexcom säkerställer därmed att säkra dataöverföringsprotokoll (HTTPS och TLS) används för att kryptera konfidentiell och känslig data vid överföring över offentliga

[44] Mejl från Dexcom inklusive synpunkter på laglighetsprövningen den 3 juni 2022.

nätverk. Alla VPN-anslutningar är enligt Dexcom krypterade med starka chiffer/protokoll.

15.27 Endast leverantörer av elektroniska kommunikationstjänster (electronic communication service providers) omfattas av övervakningsåtgärder som sker med stöd av Section 702 FISA, vilket inbegriper 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.[45]

15.28 Det går därför inte att utesluta att Dexcom kan komma att omfattas av övervakningsprogram enligt Section 702 FISA på grund av att bolaget tillhandahåller tjänster ”till allmänheten”. **Däremot är sannolikheten högre för att Twilio – leverantör av sms-meddelande- och e-posttjänster – omfattas av ett övervakningsprogram enligt Sektion 702 FISA**. Motsvarande bedömning görs för de amerikanska leverantörerna Sumo Logic, Inc (logguppföljning), Zendesk, Inc (incidenthantering), Datadog, Inc. (logguppföljning), Snaplogic, Inc (plattforsmadministration), Cloudflare, Inc. (filtering oönskad kod) och Veeva, Inc (behandling av personuppgifter om hälso- och sjukvårdspersonal för marknadsföring).

15.29 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. 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).

15.30 Enligt artikel 48 i dataskyddsförordningen får domstolsbeslut eller beslut från myndigheter i tredjeland om krav på att lämna ut personuppgifter erkännas eller genomföras endast om det grundar sig på en internationell överenskommelse, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat. Cloud Act innebär att en amerikansk myndighet via amerikansk domstol kan slippa vända sig till ett annat lands myndigheter för att säkra e-bevisning hos en tjänsteleverantör och i stället utkräva uppgifter direkt av amerikanska tjänsteleverantörer, oavsett var de bedriver sin verksamhet i världen, t.ex. i Sverige, samt förbjuda leverantören att yppa för kunden om föreläggandet.

[45] 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 justitiedepartementets PM, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, https://www.justice.gov/file/442111/download

15.31 Av Dexcoms integritetspolicy för enskilda användare[46] framgår att bolaget kan ”bli skyldiga att lämna ut dina personuppgifter vid en domstol eller vid ett administrativt förfarande för att efterleva tillämplig lagstiftning, och för att framställa, utöva eller försvara juridiska krav och lagliga rättigheter.” Dexcom har således friskrivit sig från ansvar gentemot användaren om att lämna ut data om denne på begäran av amerikansk domstol enligt Cloud Act. Huruvida Dexcom avser att informera kunden om en sådan begäran eller bestrida den framgår inte.

15.32 Dexcom har låtit meddela[47] att man aldrig mottagit en begäran om att lämna ut uppgifter med stöd av FISA. Om Dexcom skulle få en sådan begäran, skulle Dexcom hantera den enligt sin interna policy för att svara på förfrågningar från statliga myndigheter. Bland annat kommer Dexcoms compliance och legal-avdelning hantera dessa förfrågningar och vidta lämpliga åtgärder enligt följande:

- Se till att det finns ett giltigt domstolsbeslut eller husrannsakan,
- konsultera externa rådgivare om lagligheten av förfrågan,
- skräddarsy eventuella svar till omfattningen av förfrågan, inklusive maskering eller redigering av data där det är möjligt, och
- se till att utlämnandet görs på ett säkert sätt (i överensstämmelse med andra Dexcom-krav) och begära att den efterfrågade myndigheten upprätthåller sekretessen för relevanta uppgifter.

15.33 Det finns således en kvarstående risk, trots organisatoriska och tekniska åtgärder från Dexcoms sida, för en otillåten behandling av personuppgifter i bolagets tjänster genom att amerikanska myndigheter kan vilja ta del av personuppgifterna. **Risken att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Dexcom får dock betraktas som mycket låg. Det finns andra risker, t.ex. cyberattacker mot molntjänster generellt, som får betraktas som högre och mer allvarliga. Det erinras också att själva rtCGM-systemet inte är molnbaserat och att G6-produkterna kan användas utan molnfunktionalitet.**

15.34 Dexcom har motsatt sig bedömningen att den allmänna risken för integritetsförluster för användare av bolagets produkter är högre när man använder internetkommunikation (e-post etc.) och är varken specifik för Dexcom eller USA.[48] I synnerhet menar Dexcom är detta inte en risk som är specifik för Twilio och anför att även i Sverige är allmänna elektroniska kommunikationstjänster skyldiga att möjliggöra hemlig avlyssning och lagra samt lämna ut uppgifter till brottsbekämpande myndigheter. Det är alltså missvisande att hänvisa till Twilio som en högre risk när enbart det faktum att patienten använder en internetuppkoppling i Sverige leder till risk för avlyssning och utlämnande av patientens data (oavsett om Twilio används eller inte). Dexcom anser vidare att det är missvisande att betona problemet med FISA 702-förfrågningar och hänvisar till Europadomstolens dom mot Sverige avseende brott mot artikel 8 i den europeiska

[46] Integritetspolicy för Dexcom den 25 februari 2021.
[47] Mejl från Dexcom inklusive synpunkter på laglighetsprövningen den 3 juni 2022.
[48] Kommentarer från Dexcom på laglighetsprövningen den 23 juni 2022.

människorättskonventionen genom den s.k. FRA-lagen.[49] Sammanfattningsvis anser Dexcom att användningen av Twilio inte är huvudproblemet eller att Twilio leder till att den registrerade ges en lägre nivå av dataskydd än vad som erbjuds enligt dataskyddsförordningen.

15.35 Vad Dexcom anfört i denna del föranleder ingen annan riskbedömning.

Personuppgiftsansvaret i trepartsförhållandet vårdgivare, Dexcom och enskild användare

15.36 Dexcom har skapat en lösning som inte har en helt tydlig separation mellan behandlingen av enskildas hälsokonton i Dexcom Clarity och vårdgivares konton i Dexcom Clarity, vilket behandlas i det följande I en handling benämnd Dexcom Clarity Data Security and Privacy skriver Dexcom bl.a. följande (min understrykning):

"*Dexcom processes data as a data processor for data input by clinics to establish the Clarity Clinic account, when data is accessed via a linked patient account, or uploaded from patient receivers to Dexcom Clarity via clinic account where no other Dexcom services are utilized by patient."*

15.37 Dexcom har förtydligat[50] att när vårdgivaren enbart laddar upp patientens mottagardata till sitt Clarity för vårdgivare-konto (exempelvis data laddas upp direkt från mottagaren till Clarity) delas datan inte med Dexcom via molnet och Dexcom anser sig därför vara vårdgivarens personuppgiftsbiträde i denna situation. När patienten skapar ett eget Dexcom-användarkonto och väljer att dela sin data i Clarity med Dexcom via molnet är Dexcom personuppgiftsansvarig för sådan data

15.38 Dexcoms rtCGM-system är verktyg enbart för vårdgivare för att bedriva diabetesvård. Dexcoms hårdvaruprodukter kan alltså inte inhandlas på konsumentmarknaden utan måste förskrivas av en läkare. Produkterna är avsedda att användas enbart i enlighet med en ordination av läkare inom ramen för antingen hälso- och sjukvård (distanssjukvård) eller egenvård enligt ett egenvårdsbeslut av en vårdgivare. Dexcoms hårdvaruprodukter finns inte till försäljning i Sverige för konsumentbruk, dvs. för självhjälp och egen monitorering och insulinbehandling. Däremot kan enskilda privata användare fritt och utan kostnad nyttja Dexcoms molnbaserade digitala tjänster och appar, såsom G6-appen, Clarity-appen, eller tredjepartsbaserade molntjänster, såsom Diasend/Glooko.

15.39 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 Dexcom Clarity och aktivt möjliggöra delning av sina glukosvärden med vårdgivaren via Dexcom Clarity. Oklarheten om personuppgiftsansvaret handlar om vårdgivarens direktåtkomst till en patients upprättade konto i Dexcom Clarity. Det ska dock framhållas att en patient kan välja att använda en mottagare och inte appen för att se sitt glukosvärde. I sådant fall

[49] Europadomstolen dom 25 maj 2021 ref. 35252/08
[50] Mejl från Dexcom inklusive synpunkter på laglighetsprövningen den 3 juni 2022.

kan vårdgivaren vid patientmöte ladda upp mottagardata till vårdgivarens Clarity klinikkonto. Patienten behöver inte skapa ett Dexcom-konto i detta scenario.

15.40 Det råder ingen tvekan om att Dexcom är personuppgiftsansvarig för patientens konto och personuppgifter i Dexcom Clarity. Det är Dexcom 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 Dexcom använder patientens 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 Dexcom personuppgiftsansvarig för behandlingen av patientens personuppgifter i produkten.[51] Dataskyddsförordningen är tillämplig på personuppgiftsbehandlingen.

15.41 De uppgifter som överförs till vårdgivarens konto i Dexcom Clarity är vårdgivaren personuppgiftsansvarig för. Dexcom är personuppgiftsbiträde i denna del. Men är vårdgivaren personuppgiftsansvarig även för de personuppgifter som överförs via direktåtkomsten? Och för vilka personuppgifter i Dexcom-kontot blir vårdgivaren personuppgiftsansvarig för genom direktåtkomsten i Dexcom Clarity? Bara de data som samlas in av patienten via sensor och pump, överförs och förvaras av vårdgivare i Dexcom Clarity? Eller även annan data i Dexcom-kontot, dvs. sådana uppgifter som inte överförs?

15.42 **Dexcoms 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 Dexcom Clarity när denne efterfrågar uppgifterna. Dexcom är personuppgiftsansvarig för den enskildes Dexcom-konto 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 Dexcoms produkter, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att Dexcoms produkter kopplas direkt till vårdgivarens klinik-konto i Dexcom Clarity eller att vårdgivaren skapar konton och tillhandahåller användaruppgifter åt patienter i Dexcom Clarity. Så är inte fallet nu.

15.43 Det finns 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

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

tar del av. Vid direktåtkomst anses de uppgifter som omfattas av åtkomsten utlämnade i och med att åtkomsten medges.

15.44 Av 5 kap. 4 § PDL framgår förvisso att en vårdgivares ”utlämnande genom direktåtkomst” till personuppgifter är tillåten endast i den utsträckning som anges i lag eller förordning. Här rör det sig inte om ett utlämnande av personuppgifter utan om en *insamling* av personuppgifter av en vårdgivare från en enskild persons konto hos en annan aktör. Å andra sidan framgår det av 2 kap. 6 § 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 region eller kommun*.” Det väcker frågan om en vårdgivare därmed är förbjuden att bereda sig direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Dexcom) eller om det är fritt fram eftersom direktåtkomsten ligger utanför PDL:s tillämpningsområde. Om en vårdgivare är förbjuden enligt PDL att bereda sig direktåtkomst till ett Dexcom-konto, kan vårdgivare inte heller med stöd av patientens samtycke få direktåtkomst till dennes personuppgifter i konto eftersom direktåtkomst är uttömmande reglerat i PDL. Genom en potentiell teknisk åtkomst blir vidare uppgifterna i kontot enligt svensk rätt att betrakta som inkomna och förvarade allmänna handlingar hos en myndighet, t.ex. en hälso- och sjukvårdsnämnd i en region (2 kap. 6 § tryckfrihetsförordningen).[52]

15.45 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.

15.46 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.

15.47 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

[52] 2 kap. 6 § tryckfrihetsförordningen: En upptagning som avses i 3 § anses förvarad hos en myndighet, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt.

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).

15.48 Den av Dexcom valda juridiska lösningen för Dexcom Clarity 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. En osäkerhetsfaktor i sammanhanget är den potentiell tekniska åtkomsten som innebär att uppgifterna i kontot anses som förvarade allmänna handlingar hos en offentlig vårdgivare. En annan osäkerhetsfaktor är om PDL förbjuder en vårdgivare att bereda sig direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Dexcom) eller om lagen tillåter sådan direktåtkomst eftersom den ligger utanför PDL:s tillämpningsområde och inte alls är reglerad.

15.49 Rättsläget är således oklart. Genom tydligare information i personuppgiftspolicy för enskilda användare och avtalsvillkoren för vårdgivare torde Dexcom kunna reducera väsentligen de risker som föreligger för registrerade vid ett otydligt personuppgiftsansvar på beskrivet sätt och att använda sig av direktåtkomst. Det är inte uteslutet att det finns ett visst ”spelrum” i brist på vägledning i lagstiftningen för både Dexcom och vårdgivare att reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke.

15.50 Andra alternativ, som ska betraktas som rekommendationer, är att Dexcom överväger en lösning i framtiden som innebär att vårdgivare inte får direktåtkomst till enskildas Dexcom-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 Clarity-molnet för att åstadkomma en tydlig ”separation of duties”. Dexcom 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 hälsokonto i Dexcom Clarity till vårdgivarens klinikkonto i Dexcom Clarity.

15.51 Det erinras att vid distanssjukvård med hjälp av Dexcoms produkter, dvs. hälso- och sjukvård per definition i hälso- och sjukvårdslagen, genom ordination av en vårdgivare om distansmonitorering av en patient, finns alltid alternativet för den enskilde att stänga av dataöverföringen från Dexcoms produkter till Dexcom-kontot. Patienter kan slippa en molnlagring av sina glukosvärden. Hen kan i stället enbart använda G6-mottagaren och

undvika att överföra personuppgifter till molnet. Det är också möjligt för patienter att inte ge vårdgivaren direktåtkomst till deras data i Clarity på distans och istället ladda upp data från mottagaren direkt i patientens journal i vårdgivarens Clarity-konto. Nackdelen är att patienten inte kan själv kan nyttja de analyser och glukosmönster som Clarity erbjuder. Men inget hindrar rättsligt sett att patienten får ta del av vårdgivarens insamlade glukosvärden via direktåtkomst till vårdgivarens klinikkonto, om denne i stället samlar in glukosdata från mätare.

Enskild användares delning av data med andra via -appen

15.52 En enskild person kan i Follow-appen dela sina data med upp till tio personer, t.ex. anhöriga och vårdnadshavare. Det finns inga rättsliga hinder för en sådan datadelning med anhöriga m.fl. inom ramen för en enskild användares nyttjande av ett hälsokonto och där Dexcom är personuppgiftsansvarig. Vårdgivare bör endast läsa data i Dexcom Clarity, särskilt indikerade för granskning av tidigare CGM-data.

Autentisering av användare

15.53 Inloggning i Dexcom-apparna samt i Clarity-molnet sker med enfaktorsautentisering (användarnamn och lösenord). Enfaktorsautentisering ger användaren en möjlighet till enkel avläsning av Dexcom-sändaren. Användares åtkomst till egen data i Dexcom Clarity (clarity.dexcom.eu) sker också med enfaktorsautentisering. Åtkomst kan än så länge inte ske med Bank-ID eller annat elektroniskt ID. Såvitt förstås loggar vårdgivare dessutom in på sitt klinik-konto i Dexcom Clarity med användarnamn och lösenord. De kan inte nyttja SITHS-kort eller annat slag av e-legitimation.

15.54 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.

15.55 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).

15.56 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”.

15.57 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.

15.58 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.

15.59 **Beträffande vårdgivares inloggning till sitt klinik-konto i Dexcom Clarity lever Dexcom i rollen som leverantör inte upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd.** Beträffande sedan en enskild persons inloggning till sitt konto på clarity.dexcom.eu lever Dexcom inte heller upp till kraven på stark autentisering. Beträffande slutligen apparna G6, Clarity och Follow 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 Dexcom Clarity ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.**

15.60 Dexcom har låtit meddela att implementering av stark autentisering finns med i Dexcoms road map för produktsäkerhet och stark autentisering kommer att finnas i de relevanta Dexcom produkterna inom nästa år.

Vårdgivares inbjudan via e-post till användare

15.61 När en patient läggs till i klinikens Dexcom Clarity patientlista skapas inte ett Dexcom-konto automatiskt för denna patient. Patienter måste i stället skapa sitt eget konto i Dexcom Clarity om de vill visa eller ta del av CGM-data som har laddats upp på kliniken. En inbjudan innehåller en delningskod som patienterna anger i sitt personliga Dexcom-konto eller i Clarity-appen. När patienten har angett koden börjar kontona automatiskt att dela information sinsemellan. Delningskoden och inbjudan till att dela data skickas via e-post till patienten.

15.62 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.

15.63 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.

15.64 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 Clarity 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 vårdgivaren som nyttjar Clarity som gör sig skyldig till den

otillåtna behandlingen av personuppgifter. Dexcom 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.

15.65 Dexcom har uppgivit i huvudsak följande[53]: Det bör förtydligas att detta endast är stämmer om patienten använder Clarity och behöver dela data med vårdgivaren. Observera att delningskoden och inbjudan att dela data skickas till patienten via e-post eller skrivs ut och ges till patienten. För att påbörja delandet av data i Clarity behöver patienten logga in i Clarity, fylla i delningskoden och sitt födelsedatum. Patienten befinner sig därför i en säker miljö när denne fyller i delningskoden och födelsedatum för att påbörja delandet. Men om en patient använder en mottagare och inte appen för att se sitt glukosvärde, kan kliniken ladda upp mottagardata till Clarity för vårdgivare-kontot istället utan att skicka en delningskod.

15.66 Vad Dexcom anfört påverkar inte bedömningen. Rekommendation kvarstår.

Framtida forskning

15.67 På flera ställen i Dexcoms integritetspolicy för enskilda användare[54] nämns forskning som ett ändamål för bolagets vidareanvändning av registrerades personuppgifter. Bl.a. delar Dexcom enskilda personers glukosdata med tjänsteleverantörer för ändamålet ”forskning”. När det gäller registrerades rätt att få begära radering av personuppgifter anför Dexcom att denna rätt inte gäller när en behandling krävs för bl.a. ”vetenskapliga forskningsändamål”. När en användare skapar för första gången ett konto i Dexcom Clarity, efterfrågar dock inte tjänsten samtycke av användaren för att låta Dexcom använda glukosdata, inom EU eller – vilket inte framgår med all önskvärd tydlighet – i tredjeland, för ändamålet framtida forskning. Det framgår inte heller om forskningen baseras på personuppgifter eller anonymiserade uppgifter. Den rättsliga grunden synes vara samtycke (artikel 6.1 a i dataskyddsförordningen), men avser forskningen behandling av känsliga personuppgifter, dvs. hälsorelaterade uppgifter, krävs därutöver att behandlingen sker med ett ”uttryckligt samtycke” av den registrerade enligt artikel 9.2 a eller med stöd av artikel 9.2 j och 89.1 såvida stöd finns i nationell rätt i det medlemsland inom EU där forskningen ska bedrivas. **Integritetspolicyn har stora brister vad gäller Dexcoms användning av enskilda användares glukosdata för ändamålet ”forskning**

15.68 Integritetspolicyn för enskilda användare specificerar inte alls vad för slags forskning det rör sig om eller vilka som ska bedriva forskningen.

15.69 Av principen om ändamålsbegränsning i dataskyddsförordningen (artikel 5.1 b) framgår emellertid att all behandling av personuppgifter ska ha ett ändamål. Ändamål ska vara

[53] Mejl från Dexcom inklusive synpunkter på laglighetsprövningen den 3 juni 2022.
[54] Integritetspolicy för Dexcom den 25 februari 2021.

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

15.70 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 Dexcoms integritetspolicy för enskilda användare eller av annan dokumentation tillgänglig för allmänheten.

15.71 **Dexcom Clarity bedöms mot denna bakgrund innefatta en otillåten personuppgiftsbehandling för framtida forskning**. Det saknar betydelse om det rör sig om i huvudsak oidentifierbara uppgifter eftersom framtagandet av anonymiserade uppgifter kräver en behandling av personuppgifter för det specifika ändamålet. Villkoret för enskilda användare om att dela sina data för framtida forskning vid nyttjande av Dexcom Clarity bör avskaffas. Ett alternativ är att Dexcom inhämtar samtycke till delning av data för redan etikgodkända forskningsstudier (inte framtida studier) i antingen Sverige eller andra länder.

15.72 Dexcom har förklarat att ”forskning” inte avser kliniska studier utan produktutveckling av befintliga och nya tjänster.[55] Dexcom meddelar att man avser att uppdatera sin integritetspolicy och förtydliga att ”forskning” inte avser kliniska studier.

Kakor och tredjepartsaktörer

15.73 Dexcom använder en mängd olika kakor i sina appar och på clarity.dexcom.eu, se avsnitt 12. Kakorna används för ett flertal olika ändamål. Förutom nödvändiga kakor använder Dexcom funktionella kakor (ca 13 stycken), prestandakakor (ca 22 stycken) och riktade kakor för främst marknadsföring (ca 110 stycken). Totalt ca 146 kakor! Tredjepartskakor, dvs. kakor som placeras i användarens dator av en annan aktör än Dexcom, förekommer inom alla kategorierna av kakor, men mest inom kategorin riktade kakor. Därutöver använder Dexcom och dess anlitade tredjepartsaktörer andra spårningstekniker, såsom web beacons, enhetsidentifierare och pixlar.[56]

15.74 Mer information om användning av Dexcoms kakor finns i bolagets cookiepolicy på dexcom.com. Flertalet av kakorna tillhandahålls av amerikanska leverantörer

[55] Dexcoms kommentarer på laglighetsprövningen den 23 juni 2022.
[56] Integritetspolicy för Dexcom den 25 februari 2021.

(Salesforce, Snapchat m.fl.). Överföring av personuppgifter till USA eller till annat tredjeland via Dexcoms underleverantörer m.fl. kan inte uteslutas. Det saknas information om sådan överföring sker. Det saknas också information med vilket rättsligt stöd tredjelandsöverföringen sker, om sådan överföring förekommer.

15.75 Överföring av personuppgifter till USA eller till annat tredjeland via Dexcom själv eller anlitade tredjepartsleverantörer av kakor kan inte uteslutas.. Den stora mängden kakor (ca 145 stycken) samt annan inbäddad spårningsteknik i Clarity-appen och i Clarity-molnet bedöms i sig innebära en risk för registrerades fri- och rättigheter. Å andra sidan är Dexcom transparent när det gäller användningen av kakor. Opt-in används som standard och användare kan uppdatera sina val när som helst i Dexcoms cookie-banners och statiska ikoner. Bannern gör det inte svårare att avvisa cookies än att acceptera, och valen kan ändras lika enkelt som första valet är att göra. En individualiserad lista över cookies och kategorier av cookies, tillsammans med ytterligare information om varje cookie är allmänt tillgänglig här på https://www.dexcom.com/en-IE/cookie-policy. Mot denna bakgrund innebär **tredjepartstjänsterna från Salesforce, Snapchat m.fl. en risk för otillåten behandling av personuppgifter**.. **Risken får dock betraktas som låg med hänsyn till Dexcoms påvisade transparens och användning av cookie-banner**. Några Google-relaterade kakor eller liknande tjänster förekommer inte enligt Dexcom i appar eller hemsidor.

På uppdrag av SKR

Manólis Nymark

Bilaga 1

Dexcom, Inc. | Corporate Headquarters
6340 Sequence Drive | San Diego, CA 92121
888.738.3646 | dexcom.com

5 juli 2022

Dexcom anser att skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Dexcom är därför djupt engagerade i skyddet och integriteten för våra kunder och deras personuppgifter. Var och en av våra produkter och tjänster är utformade med dataskydd i åtanke och vår behandling av personuppgifter sker i enlighet med den dataskyddslagstiftning som är tillämplig i var jurisdiktion där vi bedriver verksamhet. Vår ambition är att föregå med gott exempel för andra aktörer inom medicinteknikbranschen och att bidra till en hög dataskyddsnivå.

Vi uppskattar initiativet från Sveriges Kommuner och Regioner (“**SKR**”) att se över dataskyddet i ett urval av de CGM-produkter som finns tillgängliga på den svenska marknaden och för att Dexcom har fått möjlighet att tillhandahålla sina synpunkter i denna översyn. Även om diskussionerna har varit konstruktiva finns det ett par utestående punkter där vi inte fann samsyn och som vi därför skulle vilja ta upp i detta uttalande.

Tredjelandsöverföringar av personuppgifter

I laglighetsprövningen har anmärkningar gjorts om att Dexcom överför personuppgifter till tredje land och att sådana överföringar utgör en hög risk. Dexcom håller inte med om dessa anmärkningar och vill betona att varje tredjelandsöverföring är föremål för lämpliga skyddsåtgärder, såsom standardavtalsklausuler och samtycke enligt artikel 49 i den allmänna dataskyddsförordningen ("**GDPR**"). Med tanke på att dessa lämpliga skyddsåtgärder används och att personuppgifterna överförs för ändamål såsom teknisk support, drar vi slutsatsen att det inte finns någon risk för materiell eller icke-materiell skada för den berörda kunden.

FISA 702-förfrågningar

Anmärkningar har gjorts i laglighetsprövningen angående Dexcoms användning av Twilio och att Twilio löper risk att bli föremål för FISA 702-förfrågningar från amerikanska brottsbekämpande myndigheter. Även om inga bevis har presenterats för varför Twilio löper risk att bli föremål för sådana förfrågningar vill vi betona att förfrågningar från brottsbekämpande myndigheter (oavsett jurisdiktion) inte är en fråga som är specifik för Twilio.

I Sverige är elektroniska kommunikationstjänster skyldiga att tillåta hemlig avlyssning och lagra samt lämna ut uppgifter till brottsbekämpande myndigheter. Det är alltså missvisande att hänvisa till Twilio som en risk när enbart det faktum att kunden använder en internetuppkoppling i Sverige leder till risk för avlyssning och utlämnande av kundens data (oavsett om Twilio används eller inte).

Vi tycker också att det är missvisande att betona problemet med FISA 702-förfrågningar då Sveriges övervakningsmetoder nyligen ansågs vara ett brott mot artikel 8 i den europeiska

konventionen om mänskliga rättigheter (“**EKMR**”): echr-bulk-surveillance-sweden-sigint-judgment-pr-25-5-21.pdf (statewatch.org) .

En av huvudorsakerna till att Sveriges övervakningsmetoder ansågs otillfredsställande var frånvaron av en effektiv granskning i efterhand, vilket också har varit ett av huvudargumenten till att FISA 702-förfrågningar kan leda till en lägre skyddsnivå än vad som ges enligt GDPR.

Twilio behandlar kundens e-postadress, användarnamn och IP-adress. Först och främst ser vi inte varför denna information skulle vara av intresse för amerikanska brottsbekämpande myndigheter och i den mån uppgifterna lämnas ut är det oklart om de lämnas ut i klartext (notera gärna att USA-baserade företag inte är skyldiga att dekryptera data när de svarar på FISA 702-förfrågningar). För det andra är de rättsmedel som finns tillgängliga enligt medlemsländernas lagstiftning vid utlämnande av personuppgifter till brottsbekämpande myndigheter i EU/EES (som Sverige inte har upprätthållit) endast relevanta om kunden kan bevisa att denne lidit skada. Sannolikheten att kunden skulle lida skada (materiell eller icke-materiell) om Twilio lämnar ut e-post, användarnamn och IP-adress till en amerikansk brottsbekämpande myndighet på grund av en FISA 702-förfrågan framstår som exceptionellt låg (och till vår kännedom har ett sådant utlämnande aldrig har skett). Detta eftersom en FISA 702-förfrågan inte kan ske utan ett beslut om husrannsakan, det måste finnas sannolika skäl för allvarlig brottslighet (exempelvis terrorism eller sexuellt utnyttjande av en minderårig) och förfrågan måste avse en specifik individ. Således kommer en kund inte att få sina personuppgifter utlämnade slumpmässigt.

Sammanfattningsvis ser vi inte att användningen av Twilio är det huvudsakliga problemet eller att användandet av Twilio leder till att kunden blir föremål för en lägre nivå av dataskydd än vad som erbjuds enligt GDPR.

Överdrivna påståenden om överträdelser av GDPR

Ett genomgående tema i laglighetsprövningen är att en GDPR-överträdelse resulterar i administrativa sanktionsavgifter. Detta ger läsaren intrycket att vårdgivaren löper hög risk och kan bli föremål för vitessanktioner.

I verkligheten finns det dock två starka skäl till varför det inte finns någon sådan risk och varför vårdgivaren eventuellt oroar sig utan anledning:

1) De relevanta delarna avser handlingar/underlåtelse från Dexcom, inte svenska kommuner och regioner, och är därmed en risk som Dexcom teoretiskt sett kan vara föremål för, men inte en realistisk risk för vårdgivaren.

2) Alla potentiella överträdelser av GDPR leder inte automatiskt till vitessanktioner, särskilt med tanke på den rådande situationen i Sverige, där Hovrätten i Stockholm nyligen upphävde IMYs beslut att utfärda vitessanktioner mot fem vårdgivare (Fem sjukhus och regioner slipper sanktionsavgift enligt EU:s dataskyddsförordning - Sveriges Domstolar). Därmed är beviskravet ganska högt ställt för att IMY ska kunna utfärda administrativa sanktionsavgifter.

Därför anser vi att risken är liten eller icke-existerande för att vårdgivaren sanktioneras med vite på grund av en (potentiellt) ofullständig eller felaktig integritetspolicy (eller annan åtgärd) av Dexcom. Vi menar att hänvisningarna till vitessanktioner i laglighetsprövning ger en felaktig bild av den faktiska risken och inte korrekt återspeglar dataskyddstillsynen i Sverige.

Vi anser också att det är viktigt att tillägga att vi förutsätter att Dexcom skulle vara det primära målet för dataskyddstillsynen, inte vårdgivare i Sverige. Detta med anledning av att vårdgivare i Sverige inte behandlar några personuppgifter när patienten använder rtCGM-systemet från Dexcom, förutom i de situationer där (a) patienten aktivt bjuder in vårdgivaren att få tillgång till patientens personuppgifter i rtCGM-systemet på distans eller (b) vårdgivaren laddar upp personuppgifter från rtCGM-systemet på vårdmottagningen via USB. Även i situationerna som anges i (a) och (b) kan vårdgivaren inte göras ansvarig för (potentiella) felaktigheter av Dexcom. Enligt GDPR (och administrativ lagstiftning generellt) kan man bara bötfällas för sina egna misstag, inte andras misstag.

Åtgärder som kommer att övervägas och som är av relevans för laglighetsprövningen

Vi vill lyfta fram specifika uppdateringar till Dexcoms dataskydd som Dexcom sedan innan har övervägt eller för närvarande överväger och som är av relevans för laglighetsprövningen. Även om vi inte nödvändigtvis håller med om att dessa åtgärder är behövliga för att efterleva GDPR är vi införstådda med att det kan finnas möjligheter att förbättra tydligheten och styrkan i Dexcoms integritetsnotis och dataskydd. Dexcom kommer därför att överväga följande åtgärder:

- Revidera Dexcoms integritetsnotis och lägga till förtydliganden om följande punkter:
  - Kontaktuppgifter och rollfördelningen avseende de personuppgiftsansvariga i Dexcom-gruppen,
  - Vilken typ av tillsynsmyndigheters personuppgifter lämnas ut till (i synnerhet medicintekniska sådana),
  - Vilka tekniska skyddsåtgärder som vidtas när Dexcom behandlar personuppgifter;
  - Var Dexcoms underbiträden befinner sig geografiskt, och
  - Att forskning bedrivs för generell produktutveckling (ej kliniska studier).

- Implementering av multifaktorautentisering inom det kommande året för relevanta Dexcom-produkter, och

- Granska den text som används när Dexcom inhämtar samtycke från kunder i Clarity och överväga att ytterligare förtydliga legal grund och ändamål för tredjelandsöverföringar.

Kontakta oss

Vi uppmuntrar dig, oavsett om du är kund eller vårdgivare, att kontakta oss med eventuella frågor du har angående detta uttalande eller hur vi arbetar med dataskydd i allmänhet. Vårt dedikerade integritetsteam går att nå via e-post på privacy@dexcom.com och ser fram emot att höra från dig.