PROMEMORIA

2022-06-25

Laglighetsprövning av CareLink CGM/SAP-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 CareLink CGM/SAP-system består av ett flertal CE-märkta medicinteknisk och molntjänstbaserad produkter som utvecklas och tillhandahålls av det amerikanska företaget Medtronic MiniMed, Inc. Medtronic har ett flertal dotterbolag i Europa (Medtronic MiniMed och dess dotterbolag benämns fortsättningsvis ”Medtronic”, om inte annat anges). I Sverige representeras bolaget av Medtronic AB. Guardian Connect-systemet är ett sensorbaserat, CE-märkt system för glukosmätning. Guardian Connect-systemet består av en sensor (Enlite), en sändare (Guardian Connect), appen Guardian Connect och ett CareLink Personal-konto i molntjänsten CareLink Personal. CareLink Personal tillåter uppladdning av data från Medtronics produkter.

2 Medtronic erbjuder vidare bärbara insulinpumpar under produktnamnet MiniMed. Även dessa kan kopplas till en app, MiniMed Mobile-appen. Appen kräver att användaren tecknar ett CareLink Personal-konto som registreras i molntjänsten CareLink Personal. MiniMed insulinpumpar kan kopplas ihop med glukosövervakningssystemet Guardian Connect. MiniMed Mobile-appen ersätter i sådant fall Guardian Connect-appen för glukosövervakning.

3 Användare av både Guardian Connect glukosövervakning och MiniMed insulinpumpar kan dela sina glukosmätningar och andra data med fem andra personer. Mottagaren behöver inte ha en särskild app, även om det finns en sådan tillgänglig, appen CareLink Connect. Delning av data sker i tjänsten CareLink Personal på www.carelink.minimed.eu.

4 CareLink System är en molnbaserad lösning som är avsedd för vårdgivare. Via CareLink System kan en vårdgivare ta del av insulin- och glukosdata om en enskild person som har ett CareLink Personal-konto, efter samtycke av kontoinnehavaren. Den information som lagras i CareLink System är data som har registrerats i den Medtronic-produkt (insulinpump eller glukosmätare) som en enskild användare förfogar över. Dessa uppgifter samlas

normalt sett in i CareLink Personal och överförs därefter från CareLink Personal till CareLink System. Överföring kan även ske åt andra hållet, efter att data vid vårdbesök hos klinik laddats upp av vårdgivaren direkt i CareLink System och därefter överförs till CareLink Personal. Det är alltså samma typ av data som överförs till CareLink Personal från CareLink System som från CareLink System till CareLink Personal. Vårdgivaren har inte direktåtkomst till en enskild användares CareLink Personal-konto och kan alltså inte söka fritt bland informationen i CareLink Personal.

5 CareLink CGM/SAP-system 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.

6 Avtalspart för Medtronics CGM/SAP-tjänster är Medtronic MiniMed, Inc. i USA. Personuppgiftsansvaret för personuppgifter i CareLink Personal-konton är delat mellan Medtronic MiniMed, Inc. i USA och Medtronic International Trading sàrl i Schweiz. Vårdgivare är personuppgiftsansvariga för sin behandling av personuppgifter i Medtronics molntjänst CareLink System. Medtronic AB agerar i rollen som personuppgiftsbiträde åt svenska vårdgivare. Både Medtronic MiniMed, Inc., Medtronic International Trading sàrl i Schweiz och Medtronic AB anlitar bolaget Medtronic BV i Nederländerna respektive Amazon Web Services (AWS) i Tyskland (CareLink Personal enbart) för drift och support av sina tjänster. Drift av data i CareLink sker inom EU, men i vissa fall överför Medtronic enskilda användares personuppgifter i CareLink Personal till USA för ändamålen sms-meddelanden och chat (genom underleverantörerna Twilio och Clickatell (Pty) Ltd i USA) samt produktutveckling, statistik för utveckling av marknadsföringsprodukter och framtida forskning (Medtronic). Vårdgivares patientuppgifter och medarbetares personuppgifter överförs till USA bl.a. vid tredje linjens support. I huvudsak rör det sig om pseudonymiserade uppgifter med undantag för text- och chatmeddelanden respektive support. Överföringen är beskrivna respektive reglerade i Medtronics villkor för tjänsterna, både i personuppgiftspolicyn för enskilda privata användare av CareLink Personal respektive avtalsvillkor inklusive personuppgiftsbiträdesavtal för CareLink System med svenska vårdgivare.

7 Medtronic MiniMed, Inc. och Medtronic International Trading sàrl baserar all sin personuppgiftsbehandling i rollen som personuppgiftsansvariga för enskilda individers personuppgifter på ett uttryckligt samtycke. Medtronic har däremot inte angivit med önskvärd tydlighet vilket rättsligt stöd i dataskyddsförordningen privatpersoners personuppgifter överförs till USA eller andra tredjeländer. Utgångspunkten i denna rättsutredning är att bolagen lägger enskilda personers uttryckliga samtycke till grund för överföringen av personuppgifter mellan Sverige och USA i CareLink Personal med stöd av det specifika undantaget ”samtycke” i dataskyddsförordningen för tredjelandsöverföringar, artikel 49.1 a. Det framgår av det ”samtyckesavtal” som en enskild person godkänner vid upprättade av ett konto i CareLink Personal. Av artikel 49.1 a framgår att den registrerade har uttryckligen samtyckt till att uppgifterna får överföras till tredje land, 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.

8 Beträffande först Medtronics behandling av enskilda individers personuppgifter i bolagens appar och i molntjänsten CareLink Personal för ett flertal ändamål, såsom kontouppgifter, tillhandahållande av tjänsten, kommunikation med denne om programuppdateringar m.m. och överföring av användarens personuppgifter till USA, baserar Medtronic sin behandling på den rättsliga grunden ”samtycke” (artikel 6.1 a i dataskyddsförordningen). Det är inte en tillåten rättslig grund när samma behandling är nödvändig för att fullgöra ett ”avtal” om tjänsten med enskild användare. Medtronic har meddelat att man noterat den otydliga rättsliga grunden och avser att justera och tydliggöra korrekt rättslig grund i en ny version av personuppgiftspolicyn för enskilda privata användare i denna del.

9 Beträffande sedan den enskildes uttryckliga lämnade samtycke till Medtronic som villkor för överföring av personuppgifter till USA enligt artikel 49.1 a i dataskyddsförordningen uppger Medtronic i sin personuppgiftspolicy för enskilda användare att bolagets leverantörer av tredjepartstjänster uppfyller eventuellt inte alla dataskydds- och säkerhetsbestämmelser enligt användarens lands dataskyddslagar. Det har inte föreskrivits i dataskyddsförordningen något visst innehåll i informationen till den registrerade om riskerna med tredjelandsöverföring baserad på ett uttryckligt samtycke enligt artikel 49.1 a, 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. Denna brist på information om eventuella risker med sådana överföringar 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. Medtronic har låtit meddela att personuppgiftspolicyn för enskilda privata användare ger en missvisande bild av att personuppgifter överförs till tredje land baserat på samtycke. Enligt Medtronic överförs enskilda användares personuppgifter med stöd av enbart adekvansbeslut eller kommissionens standardavtalsklausuler. Medtronic har uppgivit att man avser att förtydliga informationen om bl.a. risker vid tredjelandsöverföring för enskilda användares personuppgifter i en ny version av personuppgiftspolicyn.

10 Medtronics överföringar av personuppgifter till USA uppfyller inte kravet på information i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, vad gäller riskerna för enskilda privata användare vid överföring av sms-meddelanden och chat (genom underleverantörerna Twilio och Clickatell (Pty) Ltd i USA) samt produktutveckling, statistik för utveckling av marknadsföringsprodukter och framtida forskning i USA (Medtronic). Även här avser Medtronic att förtydliga sin information om riskerna i en ny version av personuppgiftspolicyn för enskilda privata användare.

11 Medtronic kunde ha varit mer specifik med till vilka tredjeländer man överför användarens uppgifter och till vilka mottagare. Som minimum ska anges i informationen till registrerade tredjeländernas namn liksom kategorier av mottagare (artikel 13 e och f i dataskyddsförordningen). Denna brist på information om tredjelandsöverföringen bedöms därmed innebära en hög risk för enskilda privata användares fri- och rättigheter vid behandling av personuppgifter för ändamålen produktutveckling, statistik för utveckling av marknadsföringsprodukter och sms-meddelanden. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner enligt. Medtronic har låtit meddela att man avser att förtydliga informationen om bl.a. tredjeländer och kategorier av mottagare för enskilda användares personuppgifter i en ny version av personuppgiftspolicyn.

12 Artikel 49.1 i dataskyddsförordningen är vidare bara tillämplig om det saknas ett beslut om adekvat skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46). Medtronic uppger i sin personuppgiftspolicy för enskilda användare att man använder sig av kommissionens standardavtalsklausuler. Det är en skyddsåtgärd som är uttryckligen angiven i artikel 46 i dataskyddsförordningen. Medtronic kan således inte stödja sig på någon av bestämmelserna i artikel 49.1 eftersom artikel 46 är ”aktiverad”. Medtronic bör således justera sitt ”samtyckesavtal” (se ovan) så att det reflekterar de korrekta mekanismerna för tredjelandsöverföring, dvs. kommissionens standardavtalsklausuler. Medtronic har låtit meddela att personuppgiftspolicyn för enskilda privata användare ger en missvisande bild av att personuppgifter överförs till tredje land baserat på samtycke. Enligt Medtronic överförs enskilda användares personuppgifter med stöd av enbart adekvansbeslut eller kommissionens standardavtalsklausuler. Medtronic förklarar dock att man avser att förtydliga överföringsmekanismerna för enskilda användares personuppgifter till tredje land i en ny version av sekretessmeddelandet (personuppgiftspolicyn).

13 Medtronics avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver kompletteras med skriftliga instruktion från svenska vårdgivaren till Medtronic AB om en rätt att överföra personuppgifter till tillsynsmyndighet i bl.a. USA för ändamålet kvalitets- och säkerhetsövervakning inom området medicintekniska produkter.

14 Medtronic MiniMed, Inc. och underleverantörerna AWS, Twilio och Clickatell är amerikanska företag som, såvitt kan bedömas, enligt egna avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Både Medtronics och underleverantörerna AWS, Twilios och Clickatells 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 organisatoriska och tekniska åtgärder från Medtronics sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Medtronic får dock betraktas som mycket låg med hänsyn till bolagets kärnverksamhet (diabetesmonitorering) samt Medtronic ensam förfogar över krypteringsnyckeln för den krypterade data som behandlas av AWS. Det finns andra risker,

t.ex. cyberattacker mot molntjänster generellt, som får betraktas som högre och mer allvarliga.

15 Däremot är risken högre för att Twilio eller Clickatell – leverantör av sms-meddelande- och chattjänster – omfattas av ett övervakningsprogram enligt Sektion 702 FISA. Medtronic MiniMed, Inc. och Medtronic International Trading sàrls (Medtronic) har dock informerat användaren om risken för sämre dataskydd i underleverantörernas hemländer i samband med inhämtande av samtycke för mottagande av sms och chat i apparna – en funktionalitet som användaren kan avstå från. Twilio kommer från och med hösten 2022 att ha servrar inom EU. Medtronic överväger därför att framöver endast använda sig av Twilio, inte Clickatell. Vidare har Medtronic meddelat att man ser över möjligheten att på sikt övergå till en meddelandefunktion i Medtronics appar istället för via sms. Det skulle minimera de risker som här identifierats i förhållande till Sektion 702 FISA.

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

17 Beträffande vårdgivares inloggning till sitt klinik-konto i CareLink System lever Medtronic i rollen som leverantör upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Beträffande en enskild persons inloggning till sitt konto på www.carelink.minimed.eu och via apparna Guardian Connect, MiniMed Mobile och CareLink Connect 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 och på www.carelink.minimed.se (CareLink Personal) bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Medtronic har förklarat att det dock finns tekniska förutsättningar att införa tvåfaktorsautentisering i CareLink Personal. Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i CareLink System ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.

18 Tredjepartstjänsterna Google Analytics och Adobe Analytics innebär en risk för otillåten behandling av personuppgifter. Risken får betraktas som hög. Medtronic har anfört att det i Sverige inte har fattats något beslut avseende bolags användning av Google Analytics. Medtronic avvaktar därför de beslut i frågan som är att vänta från Integritetsskyddsmyndigheten för att därefter ta ställning till vilka eventuella förändringar detta kan innebära för de appar som tillhör CareLink Personal.

Innehållsförteckning

1 Bakgrund

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

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

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

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

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

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

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

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

1.8 Medicintekniska produktrådet (MTP-rådet) är en samverkan mellan regionerna inom medicinteknikområdet. MTP-rådet ger rekommendationer om ordnat införande av medicintekniska produkter. MTP-rådets tidigare rekommendationer har bidragit till att regionerna har ökat sin kunskap på området, men det finns fortfarande stor osäkerhet hur lagstiftningen inom dataskyddsområdet ska tolkas, främst när det gäller hur risker ska bedömas i samband överföring av personuppgifter till tredjeland. Detta har inneburit att Sveriges Kommuner och Regioner (SKR 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
- CareLink System/Personal och appar
- Dexcom Clarity och appar

[1] 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 Guardian Connect-appen, MiniMed Mobile-appen, CareLink Connect-appen samt molntjänsterna CareLink Personal respektive CareLink.

1.10 CareLink CGM/SAP-system består av ett flertal CE-märkta medicinteknisk och molntjänstbaserad produkter som utvecklas och tillhandahålls av det amerikanska företaget Medtronic MiniMed, Inc., fortsättningsvis benämnd Medtronic såvida inte annat anges. Medtronic har ett flertal dotterbolag i Europa. I Sverige representeras bolaget av Medtronic AB.

1.11 Guardian Connect-systemet är ett sensorbaserat, CE-märkt system för glukosmätning. Guardian Connect-systemet består av en sensor (Enlite), en sändare (Guardian Connect), appen Guardian Connect och ett CareLink Personal-konto i Medtronics molntjänst CareLink Personal. CareLink Personal tillåter uppladdning av data från Medtronics produkter. Programmet sammanställer rapporter, kurvor, diagram och grafer och kan på så sätt hjälpa användaren att förstå effekterna av insulindosering, matvanor, träning, och eventuella läkemedel. Guardian Connect-sensorn bärs på armen eller magen. Glukosnivån läses av med en mobil enhet med hjälp av Medtronics Guardian Connect-app, t.ex. en mobiltelefon. På den mobila enhetens skärm visas den aktuella glukosnivån. Glukosvärden överförs från sändaren till appen var femte minut om sändaren befinner sig inom räckhåll för den mobila enheten Var tjugofjärde timma skickar den mobila enhet alla data till användarens CareLink Personal-konto, såsom sensorns glukosmätningar och grafer, varningar, och händelsemarkeringar. Användaren kan välja att deaktivera sådana överföringar i appen genom att stänga av synkronisering till CareLink Personal. Mätvärden som överförs till Medtronics molnbaserade tjänst CareLink Personal sparas i tio år.

1.12 Att använda Guardian Connect-appen kräver alltid att användaren skapar ett CareLink Personal-konto i Medtronics molnbaserade tjänst CareLink Personal, men överföringen av glukosvärden kan stängas av. Guardian Connect subventioneras endast för patienter som använder insulinpump och har antingen haft två eller fler svåra hypoglykemier/år som kräver hjälp av annan person, har kvarstående långtidssocker på minst 70 mmol där optimerad insulinbehandling misslyckas eller är barn som tar minst 10 plasmaglukosprover/dygn som är medicinskt motiverade.

1.13 Medtronic erbjuder vidare bärbara insulinpumpar under produktnamnet MiniMed. Produkten är CE-märkt och användningsområdet är personer med diabetes typ-1, från 7 år och äldre. Även dessa kan kopplas till en app, MiniMed Mobile-appen. Appen kräver att användaren tecknar ett CareLink Personal-konto som registreras i molntjänsten CareLink Personal. MiniMed insulinpumpar kan kopplas ihop med glukosövervakningssystemet Guardian Connect. MiniMed Mobile-appen ersätter i sådant fall Guardian Connect-appen för glukosövervakning.

1.14 Användare av både Guardian Connect glukosövervakning och MiniMed insulinpumpar kan dela sina glukosmätningar och andra data med fem andra personer. Mottagaren behöver inte ha en särskild app, även om det finns en sådan tillgänglig, appen CareLink Connect. Delning av data sker i tjänsten CareLink Personal på www.carelink.minimed.eu genom att användaren loggar in med samma inloggningsuppgifter som för ett CareLink Personal-konto, fyller i obligatoriska uppgifter om mottagaren (förnamn och efternamn; gäller även en yrkesutövare hos en vårdgivare), skapar ett användarnamn och ett tillfälligt lösenord och sedan klickar på Spara. Därefter måste användaren kontakta mottagaren och lämna de tillfälliga inloggningsuppgifterna. Mottagaren har 24 timmar på sig att logga in på www.carelink.minimed.eu (från en internetansluten enhet) för att slutföra skapandet av kontot, bl.a. genom att ändra lösenordet. Mottagaren ombeds sedan uppge sitt mobilnummer och välja önskade sms-aviseringar. Därefter kan mottagaren om den så vill, ladda ner CareLink Connect-appen.

1.15 CareLink System är en molnbaserad lösning för vårdgivare för att bedriva diabetesvård. I CareLink System kan vårdgivare lagra uppgifter som samlats in från en enskild användares avläsare och från enskilda användares CareLink Personal-konton. Uppgifter från insulinpumpar, monitorer och blodsockermätare kan registreras i vårdgivarens klinik-konto, sparas och sedan användas för att generera olika rapporter och översikter, t.ex. behandlingsrekommendationer. Rapporterna kan ge svar på frågor kring behandlingen, t.ex. patientföljsamhet, mönster och avvikelser. CareLink System är en CE-märkt medicinteknisk produkt. En vårdgivare behöver en unik registreringskod för att kunna skapa ett klinik-konto i CareLink System. En anslutning till CareLink Personal möjliggör för vårdgivaren att fjärrövervaka patienters och andra invånares glukosdata i CareLink System baserat på patientens överföringsfrekvens till CareLink Personal. För att upprätta en anslutning till en patients CareLink Personal-konto krävs ett uttryckligt samtycke som registreras i CareLink System som ytterligare krav utöver att den enskilda individen vid ett engångstillfälle anger sitt användarnamn och lösenord. Informationsflödet mellan CareLink Personal och CareLink System är dubbelriktad. Den information som lagras i CareLink System är data om insulin- respektive glukosnivåer som registrerats i den enhet (insulinpump eller glukosmätare) som patienten har. Dessa uppgifter samlas normalt sett in i CareLink Personal och överförs därefter från CareLink Personal till CareLink System. Överföring kan även ske åt andra hållet, efter att data vid vårdbesök hos klinik laddats upp från vårdgivaren direkt i CareLink System och därefter överförs till CareLink Personal. Det är alltså samma typ av data som överförs till CareLink Personal från CareLink System som från CareLink System till CareLink Personal. Ingen annan typ av data överförs.

1.16 Vårdgivare kan således inte gå in i CareLink Personal och kan alltså inte heller söka fritt bland informationen i CareLink Personal. Medtronic lämnar ut information från CareLink Personal till CareLink System med stöd av ett samtycke från den enskilde. Vårdgivaren har därefter bara tillgång till informationen om den enskilde i CareLink System. Utlämnandet sker vid begäran från vårdgivaren.

2 Uppdrag och frågeställningar

2.1 SKR har begärt en laglighetsprövning av CareLink-apparna samt molntjänsterna CareLink Personal och CareLink System. 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.

3 Gällande rätt

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

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

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

3.4 Bestämmelser om sekretess och tystnadsplikt i hälso- och sjukvården respektive socialtjänsten finns i 25 kap. offentlighets- och sekretesslagen (2009:400; OSL). OSL är tillämplig på myndigheter inom dessa verksamheter. Bestämmelser om tystnadsplikt inom privat driven hälso- och sjukvård finns i 6 kap. patientsäkerhetslagen (2010:659.

3.5 Normalt råder sekretess och tystnadsplikt inom hälso- och för uppgift om enskilds hälsotillstånd och personliga förhållanden. Röjande av uppgift i en patientjournal inom en vårdgivare får ske för dem som deltar i vården eller behöver uppgifterna för att fullgöra sina arbetsuppgifter. En patient kan emellertid spärra elektroniska uppgifter om sig själv som finns på en vårdenhet eller i en vårdprocess för elektronisk åtkomst från andra vårdenheter eller vårdprocesser. Utlämnande av uppgift i en patientjournal mellan

vårdgivare kräver antingen patientens samtycke eller att den som har journalen i sitt förvar finner vid en menprövning att uppgiften kan lämnas ut utan men eller skada för patienten eller anhöriga. Ett tyst samtycke är också godtagbart.

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

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

4 Vilka registerförfattningar är tillämpliga på Medtronics appar och CareLink-molnet?

4.1 Medtronics CGM/SAP-system är verktyg enbart för vårdgivare för att bedriva diabetesvård. Medtronics produkter kan alltså inte inhandlas på konsumentmarknaden utan måste förskrivas av en läkare. Medtronic tillhandahåller en komplett systemlösning optimerad för att hälso- och sjukvården ska kunna utreda och erbjuda patienter möjligheten att kontinuerligt mäta glukoshalten i blodet och behandla sig själva med hjälp av insulinpumpar. Patienter kan egenmonitorera glukosövervakning och insulinpumpar med hjälp av Medtronics appar (Guardian Connect respektive MiniMed Mobile) och ett Connect Personal-konto. Mätvärden sparas automatiskt i Medtronics molnbaserade tjänst CareLink Personal i tio år, såvida inte patienten stänger av överföringen.

4.2 Enskilda privata användare har vidare möjlighet att dela sina mätvärden med upp till fem andra personer via Medtronics tjänst CareLink Connect. Det kräver att mottagaren också tecknar ett CareLink Personal-konto. Mottagarens behörighet tilldelas av den enskilda användaren. Vårdgivare kan teckna ett klinik-konto i molntjänsten CareLink System som är Medtronics vårdgivarportal och där ta del av en enskild individs insulin- och glukosdata från CareLink Personal-konto, eller tvärtom. Den information som lagras i CareLink System härrör från den enhet (insulinpump eller glukosmätare) som en enskild privat användare har. Dessa uppgifter samlas normalt sett in i CareLink Personal och överförs därefter från CareLink Personal till CareLink System. Överföring kan även ske åt andra hållet, efter att data vid vårdbesök hos klinik laddats upp från den Medicinska

Enheten direkt i CareLink System och därefter överförs till CareLink Personal. Det är alltså samma typ av data som överförs till CareLink Personal från CareLink System som från CareLink System till CareLink Personal. Ingen annan typ av data överförs. Vårdgivare kan alltså inte gå in i CareLink Personal och kan inte heller söka fritt bland informationen i CareLink Personal. Medtronic lämnar ut information från CareLink Personal till CareLink System med stöd av ett samtycke från den enskilde. Vårdgivaren har därefter bara tillgång till informationen om den enskilde i CareLink System. Utlämnandet sker vid begäran från vårdgivaren.

4.3 Av PDL framgår att lagen är tillämplig på vårdgivares behandling av personuppgifter inom hälso- och sjukvården (1 kap. 1 §). Om en vårdgivare förskriver 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/SAP-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.[2] Dataskyddsförordningen är tillämplig på personuppgiftsbehandlingen.

4.8 Egenmonitorering aktualiseras också vid egenvård med stöd av förskrivna hjälpmedel som kan, men inte nödvändigtvis alltid, innefattar en digital tjänst och ett hälsokonto. Av hjälpmedelsanvändaren 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. Medtronics CGM/SAP-system utgör exempel på den typen av produkter.

4.9 Sammanfattningsvis är Medtronics produkter 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 Medtronics produkter, och dataskyddsförordningen är tillämplig på Medtronics behandling av personuppgifter som sker inom ramen för den enskildes egenvård i hemmet.

5 Vem är personuppgiftsansvarig?

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

5.2 Vid användning av CareLink System för distanssjukvård och vid uppföljning av egenvård (egenmonitorering) är patientansvarig vårdgivare personuppgiftsansvarig för mottagna personuppgifter. Medtronic AB agerar i rollen som personuppgiftsbiträde. För all annan personuppgiftsbehandling är Medtronic personuppgiftsansvarig, dvs. för enskilda användares egna genererade data. Av Medtronics personuppgiftspolicy för enskilda användare av CareLink Personal[3] och tillhörande appar framgår emellertid att Medtronic MiniMed Inc. i USA ”fastställer behandling av användares personuppgifter (inklusive patienters hälsouppgifter) tillsammans med Medtronic International Trading sàrl i Schweiz.” Båda bolagen är således personuppgiftsansvariga. Fortsättningsvis används ”Medtronic” som beteckning för detta delade personuppgiftsansvar, om inte annat anges

5.3 Privatundantaget i dataskyddsförordningen är inte tillämplig på Medtronics behandling av personuppgifter om en enskild användare eftersom företaget använder enskild

[2] Artikel 29-gruppen, vägledning om appar på smarta enheter (02/2013), s. 9.
[3] CareLink Meddelande om personlig sekretess den 24 september 2020.

individs personuppgifter för egna ändamål eller delar dessa med en vårdgivare på uppdrag av den enskilde.

6 Rättslig grund och tillåtna ändamål för behandling av personuppgifter

Bedömning: Medtronic använder i rollen som personuppgiftsansvarig ett (1) samtycke som rättslig grund för att behandla enskilda personers personuppgifter i bolagets appar och i molntjänsten CareLink Personal för ett flertal ändamål, såsom kontouppgifter, tillhandahållande av tjänsten, kommunikation med denne om programuppdateringar m.m. och överföring av användarens personuppgifter till USA. Det är inte en tillåten rättslig grund när samma behandling är nödvändig för att fullgöra ett ”avtal” om tjänsten med enskild användare (artikel 6.1 b i dataskyddsförordningen). Medtronic har meddelat att man noterat den otydliga rättsliga grunden och avser att justera och tydliggöra korrekt rättslig grund i en ny version av personuppgiftspolicyn för enskilda privata användare i denna del.

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.[4]

6.2 Vårdgivares distanssjukvård av patient med stöd av en CareLink System genom CareLink Personal är således en tillåten behandling enligt PDL, såvida behandlingen är nödvändig för ändamålet och de grundläggande dataskyddsprinciperna i dataskyddsförordningen beaktas (se avsnitt 7). Även behandling av personuppgifter i samband med en egenvårdsbedömning och egenvårdsuppföljning är tillåten. Något samtycke krävs alltså inte av patienten för att en vårdgivare ska få behandla dennes personuppgifter inom ramen för distanssjukvård eller egenvårdsbedömning respektive egenvårduppföljning. Att en vårdgivare enbart förskriver t.ex. ett Guardian Connect-system för glukosövervakning åt en invånare för egenvård eller självhjälp konstituerar inte automatiskt ett personuppgiftsansvar för vårdgivaren för all behandling av personuppgifter i appar och CareLink Personal-kontot. Däremot torde en vårdgivare anses som personuppgiftsansvarig för konton i en molntjänst 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. I CareLink kan dock inte vårdgivare skapa CareLink Personal-konton åt enskilda personer.

6.3 Vid egenvård och självhjälp (egenmonitorering) genom hälsoappar m.m. utan inblandning av en vårdgivare samlar leverantören in och behandlar individens personuppgifter normalt med stöd av den rättsliga grunden ”avtal” (användarvillkor för

[4] SOU 2017:66 s. 227.

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 Medtronics *insamling* av enskilda användares personuppgifter som avser att nyttja bolagets tjänster för glukosövervakning och insulinbehandling är inte tillämplig. Här bortses från rättsliga grunder för andra ändamål, såsom marknadsföring, kvalitets- och säkerhetsövervakning av medicintekniska produkter och forskning.

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

6.5 I CareLink Personal och apparna behandlar emellertid Medtronic i rollen som personuppgiftsansvarig enskilda användares personuppgifter med stöd av enbart samtycke, dvs. ett (1) uttryckligt samtycke som rättslig grund för behandling av a) användarens kontouppgifter, b) användarens personuppgifter för att tillhandahålla tjänsten, c) användarens personuppgifter för kommunikation med denne om programuppdateringar m.m. samt d) överföring av användarens personuppgifter till USA. Detta samtycke inhämtas i samband med att användaren skapar för första gången ett CareLink Personal-konto i någon av apparna. Samtyckets omfattning framgår också av personuppgiftspolicyn för enskilda privata användare.[5]

6.6 CareLink erinrar om att användaren inte har någon skyldighet att lämna sitt samtycke, men att ”primära funktioner” i CareLink Personal och apparna inte kan användas, såsom att skapa olika rapporter över glukosövervakningen.[6] Därutöver inhämtar Medtronic ett separat samtycke för behandling av användarens personuppgifter för direktmarknadsföring, produktutveckling och framtida forskning. Användaren går inte miste om ”primära funktioner” i apparna och CareLink Personal, om denne inte lämnar sitt samtycke för dessa typer av personuppgiftsbehandlingar eller återkallar det.

6.7 Med samtycke avses enligt dataskyddsförordningen varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av

[5] CareLink, Meddelande om personlig sekretess den 24 september 2020, https://CareLink.minimed.eu/media/sv/privacy_statement.pdf
[6] Information vid skapande av CareLink Personal-konto i CareLink Personal-appen.

personuppgifter som rör honom eller henne (artikel 4.11). Samtycke är en av flera rättsliga grunder som kan åberopas av en personuppgiftsansvarig för behandling av personuppgifter (artikel 6.1). Övriga rättsliga grunder är, såvida behandlingen är nödvändig,

- avtal med den registrerade
- rättslig förpliktelse
- skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person
- utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
- intresseavvägning

6.8 Fråga är i vilken utsträckning ett samtycke kan användas som rättslig grund i stället för den rättsliga grunden ”avtal” av en leverantör för att behandla personuppgifter om användare i en digital tjänst i rollen som personuppgiftsansvarig. Vid bedömning av huruvida samtycke är frivilligt ska enligt dataskyddsförordningen största hänsyn bl.a. tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet (artikel 7.4). Innebörden av det sagda är att en registrerad inte ska samtycka till behandling av personuppgifter som är strikt nödvändig för att nyttja eller använda en tjänst. När såväl avtal som samtycke kan användas som rättslig grund för en nödvändig personuppgiftsbehandling är det inte tanken att båda ska slås ihop. Det framgår av Europeiska dataskyddsstyrelsens (EDPB) vägledning om samtycke: ”If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis.”[7]

6.9 Vidare ställer dataskyddsförordningen krav på att ett samtycke ska vara en ”specifik…viljeyttring, genom vilken den registrerade…genom en entydig bekräftande handling godtar behandlingen av personuppgifter som rör honom eller henne.” Att samtycka till ett flertal villkor i en digital tjänst kan knappast uppfylla kravet på att ett samtycke ska vara ”specifik” och ”entydig”. EDPB anför i sin vägledning om samtycke följande: “A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal.”[8]

6.10 Sammanfattningsvis är Medtronics samtycke som rättslig grund för att behandla enskilda privatpersoners personuppgifter i appar och CareLink Personal inte en tillåten rättslig grund när samma behandling är nödvändig för att fullgöra ett avtal, i detta fall Medtronics användarvillkor för privatpersoners användning av CareLink Personal. Medtronic bör justera sin information om bolagets personuppgiftsbehandling så att det

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

tydligt framgår att den rättsliga grunden för behandling av personuppgifter i tjänsten för i vart fall ändamålen registrering av kontouppgifter, tillhandahållande av tjänsten och kommunikation av viktiga meddelanden är ”avtal” (artikel 6.1 b i dataskyddsförordningen), dvs. användarvillkoren. Behandling av personuppgifter för tredjelandsöverföring samt kvalitets- och säkerhetsövervakning behandlas nedan. Därutöver krävs ett ”uttryckligt” samtycke för behandlingen av hälsorelaterade uppgifter (artikel 9.2 a). I denna del inhämtar Medtronic ett uttryckligt samtycke för olika kategorier av hälsodata genom ett aktivt val av användaren, vilket är korrekt. Medtronic har låtit meddelat att man noterat den otydliga rättsliga grunden och avser att justera och tydliggöra korrekt rättslig grund i en ny version av personuppgiftspolicyn för enskilda privata användare i denna del.

6.11 I Medtronics personuppgiftspolicy[9] redogör bolaget för de rättsliga grunderna för att behandla enskilda personers personuppgifter. I denna lämnas information om att Medtronic behandlar enskilda användares personuppgifter med stöd av den rättsliga grunden ”rättslig förpliktelse” enligt artikel 6.1 i dataskyddsförordningen. Skälet för att använda den rättsliga grunden är enligt Medtronic skyldigheter för bolaget som följer av bestämmelser om kvalitets- och säkerhetsövervakning av medicintekniska produkter, dvs. regulatoriska krav. Det får anses utgöra en relevant rättslig grund för insamling av personuppgifter för det specifika ändamålet. Det är emellertid inte helt klart vilka specifika personuppgifter som samlas in för det ändamålet. Medtronic 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 Medtronics tjänster. Det innebär att om en invånare säger upp sitt CareLink Personal-konto, och därmed den rättsliga grunden för Medtronics 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”.

6.12 Medtronic efterfrågar vidare ett uttryckligt samtycke för framtida forskning på en användares personuppgifter när denne tecknar ett CareLink Personal-konto. Framställningen återkommer till denna fråga i avsnitt 15.

7 Grundläggande krav, information och rättigheter för enskilda

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

[9] CareLink Meddelande om personlig sekretess den 24 september 2020, https://CareLink.minimed.eu/media/sv/privacy_statement.pdf

informera registrerade om personuppgiftsbehandlingen (artikel 12, 13 och 14). Integritet och konfidentialitet har också lyfts in i de grundläggande principerna.

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

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

7.4 Patienters och konsumenters rättigheter vid behandling av deras personuppgifter regleras i huvudsak i dataskyddsförordningen – inte i PDL med något undantag. Registrerades rättigheter har förstärkts i dataskyddsförordningen i syfte att ge den registrerade ökad kontroll över sina personuppgifter. Det finns åtta rättigheter i rättighetskatalogen. Flera rättigheter är nya. Inom hälso- och sjukvård är vissa av dessa rättigheter i dataskyddsförordningen beskurna eller reglerade i särskild ordning. Bl.a. får en patient inte motsätta sig behandling av personuppgifter inom hälso- och sjukvård. Vidare kan de inte åberopa rätten att bli bortglömd. I hälso- och sjukvården får en patient i stället begära journalförstöring med stöd av PDL hos Inspektionen för vård och omsorg (IVO).

8 Anlitande av personuppgiftsbiträden

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

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

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

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

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

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

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

8.8 I dataskyddsförordningen föreskrivs dessutom följande rörande avtalets innehåll.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.10 Vid vårdgivares nyttjande av CareLink System är Medtronic AB personuppgiftsbiträde.

9 Skydd av personuppgifter

9.1 En allmän bestämmelse om den personuppgiftsansvariges ansvar för personuppgifter finns i artikel 24 i dataskyddsförordningen. Av den följer att den personuppgiftsansvarige, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen (se punkt 7.2). Rutiner för dataskydd, dokumenterade riskbedömningar, dokumentation på förändringar i digitala tjänster är exempel på åtgärder för att kunna visa ansvarsskyldighet. Tekniska och organisatoriska åtgärder ska ses över och uppdateras vid behov, vilket ska dokumenteras. Vidare anges i dataskyddsförordningen att om det står i proportion till behandlingen, ska åtgärderna omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

9.2 En precisering av det nämnda ansvaret finns i artikel 25 i dataskyddsförordningen som handlar om inbyggt dataskydd och dataskydd som standard. Enligt den artikeln ska den personuppgiftsansvarige, med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter

och friheter, genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering. Åtgärderna ska vara utformade för ett effektivt genomförande av dataskyddsprinciper, såsom uppgiftsminimering, och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Åtgärderna ska vidtas både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen.

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

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

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

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

- Åtgärder ska vidtas för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

10 Tredjelandsöverföring

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

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

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

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

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

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

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

10.8 I artikel 49.5 i dataskyddsförordningen ges möjlighet att i unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen

fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland eller en internationell organisation, om beslut om adekvat skyddsnivå saknas.

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

10.10 Europeiska dataskyddsstyrelsen (EDPB) har publicerat rekommendationer om adekvata skyddsåtgärder för tredjelandsöverföring. Rekommendationerna är ett svar på EU-domstolens dom i Schrems II.[10] EDPB har vidare publicerat ett utkast till riktlinjer som klargör vad som utgör, och inte utgör, en överföring av personuppgifter till tredjeland.[11] Riktlinjerna är i skrivande stund föremål för synpunkter.

11 Sanktionsavgifter

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

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

12 Applikationerna Guardian Connect, MiniMed Mobile och CareLink Connect samt molntjänsterna CareLink Personal respektive CareLink System

12.1 Medtronic är leverantör, tillika tillverkare, av apparna Guardian Connect, MiniMed Mobile och CareLink Connect samt molntjänsterna CareLink Personal och CareLink System. CGM-systemet Guardian Connect respektive SAP-systemet MiniMed är båda FDA-godkända och CE-märkta produkter.

12.2 Guardian Connect-appen tillsammans med Guardian Connect-sensorn tillåter användare att mäta och registrera glukosvärden när som helst och var som helst. Analys av data och larm vid överskridande av godtagbara blodsockervärden sker i Medtronics molntjänst CareLink Personal. Bärbara insulinpumpar under produktnamnet MiniMed kan kopplas

[10] 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.
[11] Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

till en app, MiniMed Mobile-appen. Managering av pumpen och glukosövervakning sker i molntjänsten CareLink Personal. Användaren kan dela sina data med anhöriga. Appen kräver att användaren tecknar ett konto i CareLink Personal. Vårdgivare kan skapa ett klinikkonto i molntjänsten CareLink System. CareLink System kan lagra uppgifter som samlats in från en enskild användares avläsare och från enskilda användares CareLink Personal-konton. 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 Medtronic har hela CareLink CGM/SAP-systemet byggts med säkerhet i åtanke.[12] Lämpliga skyddsåtgärder inkluderar individuella användarkonton till vilka åtkomst endast ges med ett giltigt användarnamn och lösenord, och tvåfaktorsautentisering för medarbetare hos vårdgivare. 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 CareLink Personal. Servern för CareLink Personal övervakas kontinuerligt för skydd mot eventuella attacker och intrång. Medtronic 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 Medtronic anlitar dotterbolaget Medtronic BV i Nederländerna för drift och underhåll av servrar för CareLink Personal och CareLink System (se vidare avsnitt 13). Bolaget tillhandahåller också andra och tredje linjens support om lokal support inte klarar av att hantera en fråga. Medtronic anlitar vidare Amazon Web Service (AWS) för lagring av personuppgifter i CareLink Personal i Tyskland. Medtronic har dock för avsikt att framöver även lagra uppgifter i CareLink System hos AWS i Tyskland. AWS har inte tillgång till personuppgifter. Enligt Medtronic förfogar enbart Medtronic över krypteringsnycklarna, s.k. Hold-Your-Own-Key (HYOK). Amazon Web Services EMEA SARL är ett registrerat bolag i Luxemburg. All data i CareLink är krypterad, både i vila och vid transport. Medtronic 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 (Nederländerna) för bättre integritetsskydd.

12.5 Guardian Connect-sensorer och MiniMed insulinpumpar överför personliga glukosvärden och annan data på ett säkert sätt till appar och avläsare med krypterad Bluetooth-teknik. Medtronic framhåller att hela CareLink-plattformen har byggts med integritet i åtanke. EU-medborgare och medborgare inom ESS garanteras av Medtronic en rätt att få utöva sina rättigheter enligt dataskyddsförordningen. Medtronic BV i Nederländerna respektive AWS i Luxemburg betraktas av Medtronic som en betrodda

[12] CareLink Meddelande om personlig sekretess den 24 september 2020.

molntjänstleverantörer som är certifierad enligt ISO 27001 Ledningssystem för informationssäkerhet.

12.6 Av Medtronics personuppgiftspolicy för enskilda användare[13] framgår att bolaget delar sammanställd ”affärsverksamhetsdata (till exempel det totala antalet användare av blodglukosmätare)” med F. Hoffmann-La Roche Ltd. i Schweiz. F. Hoffmann-La Roche Ltd är tillverkare av Medtronics blodglukosmätare. Personuppgifter delas vidare med Medtronic BV respektive Medtronic Bakken Research Center BV, båda i Nederländerna, för att efterleva kvalitets- och säkerhetskrav beträffande medicintekniska produkter. Därtill delas krypterade data med AWS. Medtronic Bakken Research Center BV tar dessutom emot användares personuppgifter (inklusive hälsouppgifter) för att förbättra CareLink Personal samt kompatibla enheter och diabeteshanteringsverktyg eller som del av utveckling av nya produkter och tjänster för diabeteshantering. Medtronic International Trading sàrl i Schweiz och Medtronic MiniMed Inc. i USA *utvecklar* marknadsförings- och kampanjmaterial utifrån sammanställd statistik som samlas in från enskildas personuppgifter (inklusive hälsouppgifter).[14] Det är oklart vilka slag av personuppgifter som används för detta ändamål. Medtronic AB använder enskilda användares personuppgifter för direktmarknadsföringssyften. Anonymiserade uppgifter om användare verkar också delas med Medtronic MiniMed Inc. i USA för ändamålen produktutveckling och framtida forskning, men bolaget utesluter inte att vissa användare kan identifieras vid sådan överföring.[15]

12.7 Medtronic sparar användares glukosvärden och annan data i molnet, dvs. i CareLink Personal, i tio år från senaste registreringsdatum. Ett CareLink Personal-konto krävs alltid för att använda Medtronics produkter, men användaren kan stänga dataöverföring från Medtronics produkter till molnet. En användare kan således begränsa överföring av data från appen till molnet. Medtronics avläsare sparar däremot inte glukosvärden i molnet utan enbart i läsaren. Data kan delas med en vårdgivare genom att denne tankar av data i avläsaren till Medtronics molntjänst för vårdgivare, CareLink System.

12.8 Inloggning i Medtronics appar sker utan någon stark autentisering. Användares åtkomst till egen data i CareLink Personal (https://www.medtronic-diabetes.se) sker med enfaktorsautentisering (användarnamn och lösenord). Åtkomst kan än så länge inte ske med Bank-ID eller annat elektroniskt ID. Vårdgivare loggar däremot in på sitt klinik-konto i CareLink System med tvåfaktorsautentisering. Det sker genom engångslösenord via sms eller e-post. De kan emellertid inte nyttja SITHS-kort eller annat slag av e-legitimation. I CareLink Personal-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.

12.9 Användare av Medtronics produkter kan dela sina elektroniska glukosvärden med en vårdgivare som har ett konto i molntjänsten CareLink System och där skapat en patientprofil för användaren. Den information som lagras i CareLink System är data om

[13] CareLink Meddelande om personlig sekretess den 24 september 2020.
[14] CareLink Meddelande om personlig sekretess den 24 september 2020.
[15] Samtyckesinformation i samband med tecknande av ett CareLink Personal-konto.

insulin- respektive glukosnivåer som registrerats i den enhet (insulinpump eller glukosmätare) som en användare av Medtronics produkter har. Dessa uppgifter samlas normalt sett in i CareLink Personal och överförs därefter från CareLink Personal till CareLink System. Överföring kan även ske åt andra hållet, efter att data vid vårdbesök hos klinik laddats upp från vårdgivaren direkt i CareLink System och därefter överförs till CareLink Personal. Det är alltså samma typ av data som överförs till CareLink Personal från CareLink System som från CareLink System till CareLink Personal. Vårdgivare kan alltså inte gå in i CareLink Personal och kan inte heller söka fritt bland informationen i CareLink Personal. Medtronic lämnar ut information från CareLink Personal till CareLink System med stöd av ett samtycke från den enskilde. Vårdgivaren har därefter bara tillgång till informationen om den enskilde i CareLink System. Utlämnandet sker vid begäran från vårdgivaren

12.10 Medtronic hävdar att bolaget använder sig av kommissionens standardavtalsklausuler (SCC) från 2021 vid överföring av privatpersoners personuppgifter i CareLink Personal från EU till USA.[16] Det sker för ändamålen produktutveckling, sms-meddelanden och framtida forskning. Det innebär att Medtronic åtar sig att respektera de rättigheter som EU-medborgare kommer i åtnjutande av enligt dataskyddsförordningen.[17] Av personuppgiftspolicyn för enskilda användare[18] hänvisas emellertid inte till relevanta moduler i SCC:n beroende på vem som är avsändare och mottagare av personuppgifter inom EU respektive tredjeland. Däremot erbjuds den enskilda användaren att få en kopia av standardavtalsklausulerna som används för dataöverföringar över gränser via en e-postadress.

I Medtronics avtalsvillkor för CareLink System inklusive personuppgiftsbiträdesavtal med vårdgivare[19] åberopas också kommissionens SCC för tredjelandsöverföring.

12.11 När en användare skapar för första gången sitt konto i CareLink Personal, efterfrågar tjänsten samtycke av användaren för att låta Medtronic använda glukosdata utan koppling till användaren för ändamålet framtida forskning. Av informationen som lämnas i samband härmed samt av Medtronics personuppgiftspolicy för bolagets alla appar och CareLink Personal-konton[20] framgår att sammanställd data inte innehåller någon information som kan identifiera användaren direkt, men ”de utesluter inte fullständigt möjligheten att identifiera dig”.[21] Framställningen återkommer till frågan om forskning i avsnitt 15.

12.12 Av personuppgiftspolicyn[22] framgår vidare att Medtronic anlitar leverantörerna Twilio, Inc. respektive Clickatell (Pty) Ltd i USA för sms- och chatmeddelanden, innehållande en patients hälsouppgifter, till användare av appen CareLink Connect utan kryptering och att uppgifterna kommer att vara synliga för leverantören som kan vara belägen

[16] CareLink Meddelande om personlig sekretess den 24 september 2020..
[17] CareLink Meddelande om personlig sekretess den 24 september 2020.
[18] CareLink Meddelande om personlig sekretess den 24 september 2020.
[19] Avtal om Medtronic CareLink TM-tjänster (odaterad).
[20] CareLink Meddelande om personlig sekretess den 24 september 2020.
[21] Samtyckesinformation i samband med tecknande av CareLink Personal-konto.
[22] CareLink Meddelande om personlig sekretess den 24 september 2020.

”utanför användarens land”. Medtronic upplyser om att Twilios respektive Clickatells hemland USA respektive Sydafrika, inte uppfyller alla dataskydds- och säkerhetsbestämmelser enligt dataskyddsförordningen för användare inom EU/EES.[23]

12.13 Av Medtronics personuppgiftspolicy[24] för enskilda användare av CareLink Personal framgår att bolaget kan röja den information som samlas in från användare, inklusive hälsouppgifter, för att uppfylla ”alla rimliga begäranden från behöriga enheter eller ombud för brottsbekämpning, rättsliga myndigheter, statliga organ eller myndigheter, inklusive dataskyddsmyndigheter, i vilket fall bearbetningen begränsas till vad som minst krävs för att uppfylla föreläggandet.” Av policyn framgår inte om Medtronic informerar användare om rättsliga processer som söker tillgång till dennes information, såsom domstolsbeslut eller stämningar.

12.14 Av Medtronics avtalsvillkor inklusive personuppgiftsbiträdesavtal för CareLink System med vårdgivare[25] framgår följande villkor när Medtronic behandlar vårdgivarens personuppgifter: ”*Efterkomma rimliga begäranden från behörig brottsbekämpande personal eller representanter, rättsliga myndigheter, offentliga myndigheter eller organ, inklusive behöriga dataskyddsmyndigheter, varvid behandlingen begränsas till miniminivån för att uppfylla begäran. Medtronic kommer i vilket fall att underrätta Vårdenheten om en sådan begäran, förutom om förhandsanmälan inte är tillåten på grund av skyldighet till sekretess som åläggs Medtronic enligt tillämplig lag eller av begärande person, representant, myndighet eller organ.*”

12.15 Det erinras att enligt punkt 15.1 a (modul 1, 2, 3 och 4) i kommissionens standardavtalsklausuler (SCC) ska personuppgiftsbiträdet snarast underrätta den personuppgiftsansvarige om bl.a. en begäran från en myndighet eller domstol om utfående av personuppgifter som biträdet behandlar för den personuppgiftsansvariges räkning. Punkt 15.1 b stipulerar emellertid att såvida personuppgiftsbiträdet är förbjuden enligt lagstiftningen i hemlandet att yppa för den personuppgiftsansvarige om ett sådant föreläggande, biträdet ska göra sitt bästa (eng. use its best efforts) för att häva yppandeförbudet i syfte att kunna underrätta den personuppgiftsansvarige så snart som möjligt.

12.16 Enligt personuppgiftspolicyn[26] för CareLink Personal och tillhörande appar använder Medtronic kakor, som Google Analytics och Adobe Analytics. Dessa används för att hjälpa bolaget att förbättra sin service, prestanda och användarupplevelser. Google Analytics och Adobe Analytics används inte i CareLink Personal, utan endast i vissa av de appar tillhörande CareLink Personal som Medtronic tillhandahåller enskilda. I appen MiniMed Mobile används endast Adobe Analytics, inte Google Analytics. Enligt Medtronic samlas följande information om användarna genom Adobe Analytics: öppnade sidor och interagerade sidor efter varje start av mobilapplikationen, antal gånger som mobilapplikationerna öppnas och används dagligen och månatligen samt den dag

[23] CareLink Meddelande om personlig sekretess den 24 september 2020
[24] CareLink Meddelande om personlig sekretess den 24 september 2020.
[25] Avtal om Medtronic CareLink TM-tjänster (odaterad).
[26] CareLink Meddelande om personlig sekretess den 24 september 2020.

och timme då mobilapplikationen i fråga startades, sessionstid i mobilapplikationen och den totala sessionslängden, antal gånger mobilapplikationen kraschar och dagar sedan senaste användning. Följande uppgifter samlas in genom Google Analytics: butik från vilken appen laddades ned och installerades, versionsnamn (Android) eller paketversion (iOS), användarens bosättningsland, varumärket för användarens mobila enhet (t.ex. Motorola, LG eller Samsung), den mobila enhetens kategori (t.ex. telefon eller surfplatta), den mobila enhetens modellnamn för (t.ex. iPhone5), tid då användaren först öppnade appen, om appen öppnades för första gången inom de senaste 7 dagarna, om appen öppnades för första gången för mer än 7 dagar sedan och enhetens operativsystemversion (OS) (t.ex. 9.3.2). Någon information huruvida IP-adress samlas in eller inte finns inte, trots att båda tredjepartsapplikationerna kan samla in sådan uppgifter.

12.17 Någon information om hur man kan ta bort Google Analytics kakor respektive Adobe Analytics kakor finns inte. Däremot allmän information om att kakor kan regleras och begränsas i användarens webbläsare.

13 Tredjepartsapplikationer och tredjepartsaktörer avseende CareLink Personal och CareLink System

13.1 Som redovisas i avsnitt 12 driftas Medtronics back-end för CareLink Personal och CareLink System av det nederländska dotterbolaget Medtronic BV. Bolaget ansvarar även för andra linjens support för användare inom Europa. Medtronic BV är ett bolag inom Medtronic-koncernen och agerar här i rollen som personuppgiftsbiträde åt Medtronic och underbiträde till Medtronic AB som är det bolag som agerar i rollen som personuppgiftsbiträde åt svenska vårdgivare. Vidare anlitar Medtronic AWS i Tyskland för lagring av personuppgifter i CareLink Personal och som agerar i rollen som personuppgiftsbiträde åt Medtronic och underbiträde till Medtronic AB. Medtronic har dock för avsikt att framöver även lagra uppgifter i CareLink System hos AWS i Tyskland

13.2 Av Medtronics personuppgiftspolicy för enskilda användare av CareLink Personal framgår att bolaget delar sammanställd ”affärsverksamhetsdata (till exempel det totala antalet användare av blodglukosmätare)” med F. Hoffmann-La Roche Ltd. i Schweiz. F. Hoffmann-La Roche Ltd är tillverkare av Medtronics blodglukosmätare. Personuppgifter delas vidare med Medtronic BV respektive Medtronic Bakken Research Center BV, båda i Nederländerna, för att efterleva kvalitets- och säkerhetskrav beträffande medicintekniska produkter. Medtronic delar krypterade data med AWS i Tyskland. Medtronic Bakken Research Center BV tar dessutom emot användares personuppgifter (inklusive hälsouppgifter) för att förbättra CareLink Personal samt kompatibla enheter och diabeteshanteringsverktyg eller som del av utveckling av nya produkter och tjänster för diabeteshantering. Medtronic International Trading sàrl i Schweiz och Medtronic MiniMed Inc. i USA utvecklar marknadsförings- och kampanjmaterial utifrån sammanställd statistik som samlas in från enskildas personuppgifter (inklusive hälsouppgifter). Det är oklart vilka slag av personuppgifter som används för detta ändamål.

13.3 Som också redovisas i avsnitt 12 överför Medtronic både enskilda användares och hälso- och sjukvårdspersonals personuppgifter till bl.a. USA för ändamålet support. I CareLink Personal överförs dessutom sms-meddelanden, chat, produktutveckling, statistik för utveckling av marknadsföringsprodukter och framtida forskning. I huvudsak rör det sig om pseudonymiserade uppgifter med undantag för text- och chatmeddelanden (användare av CareLink Personal) och support (vårdgivares medarbetare). Medtronic informerar dock att bolaget inte helt kan utesluta att vissa individers överförda uppgifter undantagsvis kan hänföras till dem, dvs. avser personuppgifter. Några absoluta garantier för att européers personuppgifter stannar i Europa ges inte av Medtronic.

13.4 Medtronic förklarar i sina användarvillkor för vårdgivare att bolaget stödjer sin tredjelandsöverföring till USA av personuppgifter om verksamhet och personal på kommissionens standardavtalsklausuler (SCC). Beträffande tredjelandsöverföring av enskilda användares personuppgifter i CareLink Personal till USA stödjer sig Medtronic också på SCC.

13.5 Lagring av enskilda användares glukosdata i CareLink Personal sker hos det nederländska bolaget Medtronic BV respektive AWS. Medtronic BV ingår i Medtronic-koncernen. Medtronic BV och AWS agerar här i rollen som personuppgiftsbiträden åt moderbolaget Medtronic MiniMed, Inc. i USA och Medtronic International Trading sàrl i Schweiz. Av Medtronics personuppgiftspolicy för enskilda användare av CareLink Personal och tillhörande appar framgår nämligen att Medtronic MiniMed Inc. i USA ”fastställer behandling av användares personuppgifter (inklusive patienters hälsouppgifter) tillsammans med Medtronic International Trading sàrl i Schweiz.” Båda bolagen är således personuppgiftsansvariga för behandlingen av personuppgifter i CareLink Personal. Det har inte gått att ta del av personuppgiftsbiträdesavtalet mellan Medtronic i USA respektive Medtronic BV i Nederländerna och AWS i Tyskland.

13.6 Lagring i AWS sker på det bolagets datacenter i Tyskland. AWS agerar här i rollen som personuppgiftsbiträde åt Medtronic. Av AWS integritetspolicy[27] framgår bl.a. under rubriken ”Location of Personal Information” följande: “*Amazon Web Services, Inc. is located in the United States, and our affiliated companies are located throughout the world. Depending on the scope of your interactions with AWS Offerings, your personal information may be stored in or accessed from multiple countries, including the United States. Whenever we transfer personal information to other jurisdictions, we will ensure that the information is transferred in accordance with this Privacy Notice and as permitted by applicable data protection laws*.”

13.7 I AWS kan kunden, dvs. Medtronic, välja region där data ska tekniskt lagras.[28] AWS skriver: “*We will not move or replicate your content outside of your chosen AWS Region(s) without your consent, except in each case as necessary to comply with the law or a binding order of a governmental body*. AWS skriver vidare följande: “*We will not*

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

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

13.8 AWS informerar att tredjelandsöverföringen till USA inte sker med stöd av kommissionens beslut om skölden för privatlivet (Privacy Shield, se avsnitt 14). Under rubriken EU-US Privacy Shield anför AWS följande[29]: "*Since the Court of Justice of the European Union has validated the use of Standard Contractual Clauses (SCCs) as a mechanism for transferring data outside the European Union, our customers can continue to rely on the SCCs included in the AWS GDPR Data Processing Addendum if they choose to transfer their data outside the European Union in compliance with GDPR. The AWS GDPR Data Processing Addendum with Standard Contractual Clauses is part of the AWS Service Terms and is available automatically for all customers transferring personal data from the EU to any of the AWS regions around the world, including in the US.*"

13.9 Medtronic tillämpar enligt egen uppgift en Hold-Your-Own-Key-lösning (HYOK).[30] Det innebär att patientuppgifter krypteras och dekrypteras av någon av dotterbolagen i Europa, oklart vilken, och att enbart dotterbolaget förfogar över krypteringsnyckeln. AWS lagrar således enbart krypterade uppgifter, vilka krypterats av Medtronic. AWS förfogar inte själv över någon krypteringsnyckel eller andra medel för att få tillgång till vårdgivares patientuppgifter eller privata användares egeninsamlade personuppgifter i klartext.

13.10 Medtronic använder Google Analytics och Adobe Analytics i sina appar, vilka kräver kakor. Google Analytics och Adobe Analytics används inte i CareLink Personal, utan endast i vissa av de appar tillhörande CareLink Personal som Medtronic tillhandahåller enskilda. I appen MiniMed Mobile används endast Adobe Analytics, inte Google Analytics. Både Google Analytics och Adobe Analytics används för att föra statistik över användningen av Medtronics appar. Tjänsterna tillhandahålls av amerikanska leverantörer (Google och Adobe). Överföring av personuppgifter till USA eller till annat tredjeland via Medtronics underleverantör Google respektive Adobe kan inte uteslutas.

14 Molntjänster och rättsläge

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

[29] https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/
[30] Mejlkonversation med Medtronic.

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 (Medtronic 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[31]).
    - Det tredje alternativet är att ändå ta i anspråk molntjänsten därför att det inte finns några andra realistiska alternativ för myndigheten att bedriva sin verksamhet effektivt och acceptera riskerna som kan medföra vitessanktioner från tillsynsmyndighet och/eller skadeståndsanspråk från registrerade.

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

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

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

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

14.15 EU-domstolen har i Schrems II-domen uttalat att överföring av personuppgifter till ett tredjeland förutsätter att landet har en skyddsreglering som är 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 standardavtalsklausuler (SCC) för tredjelandsöverföring i syfte att binda t.ex. leverantör att effektuera rättsmedel för registrerade motsvarande de som finns i dataskyddsförordningen. Standardavtalsklausulerna är inte bilagda CareLink Systems-avtalet eftersom dessa inte ingås mellan vårdgivare och Medtronic utan mellan Medtronic AB och Medtronic MiniMed, Inc i USA. Standardavtalsklausulerna kan tillhandahållas vårdgivare på begäran. Den modul som används är den från biträde till biträde, dvs. Modul 3. Amerikanska myndigheter är emellertid inte bundna av standardavtalsklausulerna, 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.[32]

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

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

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

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

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

15 Har personuppgifter i Medtronics appar samt i tjänsterna CareLink Personal respektive CareLink System ett godtagbart skydd?

Bedömning: CareLink CGM/SAP-system 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.

Avtalspart för Medtronics CGM/SAP-tjänster är Medtronic MiniMed, Inc. i USA. Personuppgiftsansvaret för personuppgifter i CareLink Personal-konton är delat mellan Medtronic MiniMed, Inc. i USA och Medtronic International Trading sàrl i Schweiz. Vårdgivare är personuppgiftsansvariga för sin behandling av personuppgifter i Medtronics molntjänst CareLink System. Medtronic AB agerar i rollen som personuppgiftsbiträde åt svenska vårdgivare. Både Medtronic MiniMed, Inc och Medtronic AB anlitar bolaget Medtronic BV i Nederländerna respektive Amazon Web Services (AWS) i Tyskland (CareLink Personal enbart) för drift och support av sina tjänster. Drift av Medtronics data sker inom EU, men i vissa fall överförs personuppgifter om enskilda privata användare till USA för ändamålen sms-meddelanden och chat (genom underleverantörerna Twilio och Clickatell (Pty) Ltd i USA) samt produktutveckling, statistik för utveckling av marknadsföringsprodukter och framtida forskning (Medtronic). Vårdgivares patientuppgifter och medarbetares personuppgifter överförs till USA bl.a. vid tredje linjens support. I huvudsak rör det sig om pseudonymiserade uppgifter med undantag för text- och chatmeddelanden respektive support. Överföringen är beskrivna respektive reglerade i Medtronics villkor för tjänsterna, både i personuppgiftspolicyn för enskilda privata användare av CareLink Personal respektive avtalsvillkor inklusive personuppgiftsbiträdesavtal för CareLink System med svenska vårdgivare.

Medtronic MiniMed, Inc och Medtronic International Trading sàrl (Medtronic) baserar all sin personuppgiftsbehandling i rollen som personuppgiftsansvariga för enskilda individers personuppgifter på ett uttryckligt samtycke. Medtronic har däremot inte angivit med önskvärd tydlighet vilket rättsligt stöd i dataskyddsförordningen privatpersoners personuppgifter överförs till USA eller andra tredjeländer. Utgångspunkten i denna rättsutredning är att bolagen lägger enskilda personers uttryckliga samtycke till grund för överföringen av personuppgifter mellan Sverige och USA i CareLink Personal med stöd av det specifika undantaget ”samtycke” i dataskyddsförordningen för tredjelandsöverföringar, artikel 49.1 a. Det framgår av det ”samtyckesavtal” som en enskild person godkänner vid upprättade av ett konto i CareLink Personal. Av artikel 49.1 a framgår att den registrerade har uttryckligen samtyckt till att uppgifterna får överföras till tredje land, 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.

Beträffande först Medtronic MiniMed, Inc. och Medtronic International Trading sàrls (Medtronic) behandling av enskilda individers personuppgifter i bolagens appar och i molntjänsten CareLink Personal för ett flertal ändamål, såsom kontouppgifter, tillhandahållande av tjänsten, kommunikation med denne om programuppdateringar m.m. och överföring av användarens personuppgifter till USA, baserar bolagen sin behandling på den rättsliga grunden ”samtycke” (artikel 6.1 a i dataskyddsförordningen). Det är inte en tillåten rättslig grund när samma behandling är nödvändig för att fullgöra ett ”avtal” om tjänsten med enskild användare. Medtronic har meddelat att man noterat den otydliga rättsliga grunden och avser att justera och tydliggöra korrekt rättslig grund i en ny version av personuppgiftspolicyn för enskilda privata användare i denna del.

Beträffande sedan den enskildes uttryckliga lämnade samtycke till Medtronic MiniMed, Inc. och Medtronic International Trading sàrl (Medtronic) som villkor för överföring av personuppgifter till USA enligt artikel 49.1 a uppger Medtronic i sin personuppgiftspolicy för enskilda användare att bolagets leverantörer av tredjepartstjänster uppfyller eventuellt inte alla dataskydds- och säkerhetsbestämmelser enligt användarens lands dataskyddslagar. Det har inte föreskrivits i dataskyddsförordningen något visst innehåll i informationen till den registrerade om riskerna med tredjelandsöverföring baserad på ett uttryckligt samtycke enligt artikel 49.1 a, 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. Denna brist på information om eventuella risker med sådana överföringar 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. Medtronic har låtit meddela att personuppgiftspolicyn för enskilda privata användare ger en missvisande bild av att personuppgifter överförs till tredje land baserat på samtycke. Enligt Medtronic överförs enskilda användares personuppgifter med stöd av enbart adekvansbeslut eller kommissionens standardavtalsklausuler. Medtronic har låtit meddela att man avser att förtydliga informationen om bl.a. risker vid tredjelandsöverföring för enskilda användares personuppgifter i en ny version av sekretessmeddelandet (personuppgiftspolicyn).

Medtronic MiniMed, Inc. och Medtronic International Trading sàrls (Medtronic) överföringar av personuppgifter till USA uppfyller inte kravet på information i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, vad gäller riskerna för enskilda privata användare vid överföring av sms-meddelanden och chat (genom underleverantörerna Twilio och Clickatell (Pty) Ltd i USA) samt produktutveckling, statistik för utveckling av marknadsföringsprodukter och framtida forskning i USA (Medtronic). Även här avser Medtronic att förtydliga sin information om riskerna i en ny version av personuppgiftspolicyn för enskilda privata användare.

Medtronic kunde ha varit mer specifik med till vilka tredjeländer man överför användarens uppgifter och till vilka mottagare. Som minimum ska anges i informationen till registrerade tredjeländernas namn liksom kategorier av mottagare (artikel 13 e och f i dataskyddsförordningen). Denna brist på information om tredjelandsöverföringen bedöms därmed innebära en hög risk för enskilda privata användares fri- och rättigheter vid behandling av personuppgifter för ändamålen produktutveckling, statistik för utveckling av marknadsföringsprodukter och sms-meddelanden. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner Medtronic har låtit meddela att man avser att förtydliga informationen om bl.a. tredjeländer och kategorier av mottagare för enskilda användares personuppgifter i en ny version av sekretessmeddelandet (personuppgiftspolicyn).

Artikel 49.1 är vidare bara tillämplig om det saknas ett beslut om adekvat skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46). Medtronic uppger i sin personuppgiftspolicy för enskilda användare att man använder sig av kommissionens standardavtalsklausuler. Det är en skyddsåtgärd som är uttryckligen angiven i artikel 46 i dataskyddsförordningen. Medtronic kan således inte stödja sig på någon av bestämmelserna i artikel 49.1 eftersom artikel 46 är ”aktiverad”. Medtronic bör således justera sitt ”samtyckesavtal” (se ovan) så att det reflekterar de korrekta mekanismerna för tredjelandsöverföring, dvs. kommissionens standardavtalsklausuler. Medtronic har låtit meddela att personuppgiftspolicyn för enskilda privata användare ger en missvisande bild av att personuppgifter överförs till tredje land baserat på samtycke. Enligt Medtronic överförs enskilda användares personuppgifter med stöd av enbart adekvansbeslut eller kommissionens standardavtalsklausuler. Medtronic förklarar dock att man avser att förtydliga överföringsmekanismerna för enskilda användares personuppgifter till tredje land i en ny version av sekretessmeddelandet (personuppgiftspolicyn).

Medtronics avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver kompletteras med skriftliga instruktion från svenska vårdgivaren till Medtronic AB om en rätt att överföra personuppgifter till tillsynsmyndighet i bl.a. USA för ändamålet kvalitets- och säkerhetsövervakning inom området medicintekniska produkter.

Medtronic MiniMed, Inc. och underleverantörerna AWS, Twilio och Clickatell är amerikanska företag som, såvitt kan bedömas, enligt egna avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Både Medtronics och underleverantörerna AWS, Twilios och Clickatells 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 organisatoriska och tekniska åtgärder från Medtronics sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska

myndigheter vill ta del av kunduppgifter förvarade hos Medtronic får dock betraktas som mycket låg med hänsyn till bolagets kärnverksamhet (diabetesmonitorering) samt Medtronic ensam förfogar över krypteringsnyckeln för den krypterade data som behandlas av AWS. Det finns andra risker, t.ex. cyberattacker mot molntjänster, som får betraktas som högre och mer allvarliga.

Däremot är risken högre för att Twilio eller Clickatell – leverantör av sms-meddelande- och chattjänster – omfattas av ett övervakningsprogram enligt Sektion 702 FISA. Medtronic MiniMed, Inc. och Medtronic International Trading sàrls (Medtronic) har dock informerat användaren om risken för sämre dataskydd i underleverantörernas hemländer i samband med inhämtande av samtycke för mottagande av sms och chat i apparna – en funktionalitet som användaren kan avstå från. Twilio kommer från och med hösten 2022 att ha servrar inom EU. Medtronic överväger därför att framöver endast använda sig av Twilio, inte Clickatell. Vidare har Medtronic meddelat att man ser över möjligheten att på sikt övergå till en meddelandefunktion i Medtronics appar istället för via sms. Det skulle minimera de risker som här identifierats i förhållande till Sektion 702 FISA.

Medtronic MiniMed, Inc. och Medtronic International Trading sàrls (Medtronic) 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 CareLink System när denne efterfrågar uppgifterna. Medtronic är personuppgiftsansvarig för den enskildes CareLink Personal-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 Medtronics produkter, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att Medtronics produkter kopplas direkt till vårdgivarens klinik-konto i CareLink System eller att vårdgivaren skapar konton och tillhandahåller användaruppgifter åt patienter i CareLink Personal. Så är inte fallet nu.

Beträffande vårdgivares inloggning till sitt klinik-konto i CareLink System lever Medtronic i rollen som leverantör upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Beträffande en enskild persons inloggning till sitt konto på www.carelink.minimed.eu och via apparna Guardian Connect, MiniMed Mobile och CareLink Connect 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 och på www.carelink.minimed.se (CareLink Personal) bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Medtronic har förklarat att det dock finns tekniska förutsättningar att införa tvåfaktorsautentisering i CareLink

Personal.[33] Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i CareLink System ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.

Tredjepartstjänsterna Google Analytics och Adobe Analytics innebär en risk för otillåten behandling av personuppgifter. Risken får betraktas som hög. Medtronic har anfört att det i Sverige inte har fattats något beslut avseende bolags användning av Google Analytics. Medtronic avvaktar därför de beslut i frågan som är att vänta från Integritetsskyddsmyndigheten för att därefter ta ställning till vilka eventuella förändringar detta kan innebära för de appar som tillhör CareLink Personal.

15.1 Föreliggande laglighetsprövningen av Medtronics CGM/SAP-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 Medtronic MiniMed, Inc. är ett amerikansk bolag. Bolaget har ett fast verksamhetsställe i Sverige genom Medtronic AB. Avtalspart för Medtronics tjänster är Medtronic MiniMed, Inc. i USA. Personuppgiftsansvaret för appar och molntjänster är delat mellan Medtronic MiniMed, Inc. i USA och Medtronic International Trading sàrl i Schweiz. I rollen som personuppgiftsansvarig, vilken roll Medtronic har beträffande behandling av personuppgifter vid egenvård, är dataskyddsförordningen tillämplig på personuppgiftsbehandlingen i Medtronics 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 Medtronic AB som agerar i rollen som personuppgiftsbiträde åt svenska vårdgivare.

[33] Information till SKR gällande Medtronics produkter den 3 juni 2022.

15.5 Det s.k. privatundantaget i artikel 2.2 c i dataskyddsförordningen bedöms inte vara tillämplig vid enskilda användares nyttjande av Medtronics 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. Medtronic, dvs. Medtronic MiniMed, Inc. och Medtronic International Trading sàrl är därmed tillsammans personuppgiftsansvariga 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 Personal hos Medtronic AB omfattas av en lagreglerad och straffsanktionerad tystnadsplikt enligt lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. Svenska patienters och andra invånares personuppgifter som hanteras av Medtronic AB har därmed ett godtagbart skydd när de behandlas av det bolaget i rollen som personuppgiftsbiträde.

15.8 Personal verksamma vid moderbolaget Medtronic MiniMed, Inc. i USA samt Medtronic International Trading sàrl i Schweiz omfattas däremot inte av en lagreglerad och straffsanktionerad tystnadsplikt enligt lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. Lagen gäller i praktiken bara för aktörer vars medarbetare är fysiskt verksamma i Sverige. Tystnadsplikt för de personuppgiftsansvariga bolagen Medtronic MiniMed, Inc. respektive Medtronic International Trading sàrl och dess medarbetare måste i stället avtalsregleras. En sådan avtalad tystnadsplikt finns reglerad i både Medtronics personuppgiftspolicy för användare av CareLink Personal[34], och i avtalsvillkoren inklusive personuppgiftsbiträdesavtal med vårdgivare.[35] Några disciplinära eller andra sanktioner mot enskild medarbetare hos Medtronic MiniMed, Inc. respektive Medtronic International Trading sàrl i Schweiz 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.

15.9 Medtronic MiniMed, Inc. respektive Medtronic International Trading sàrl samt personuppgiftsbiträdet Medtronic AB anlitar underbiträdena Medtronic BV i Nederländerna för lagring av hälsorelaterade personuppgifter i CareLink Personal och CareLink System. Information som behandlas inom CareLink Personal lagras både hos AWS i Tyskland och hos Medtronic BV i Nederländerna. När det gäller CareLink System lagras informationen bara hos Medtronic BV i Nederländerna. Medtronic har dock för avsikt att inom kort även börja lagra vissa uppgifter i CareLink System hos

[34] CareLink Meddelande om personlig sekretess den 24 september 2020.
[35] Avtal om Medtronic CareLink TM-tjänster (odaterad).

AWS i Tyskland. . Medtronic MiniMed, Inc. respektive Medtronic International Trading sàrl anlitar också Twilio, Inc respektive Clickatell (Pty) Ltd i USA för sms- och chatmeddelanden i CareLink Personal. Lagring av CareLink-data sker i Nederländerna och Tyskland. Lagring av sms-textmeddelanden sker i USA (Twilio) respektive Irland (Clickatell). (Twilio kommer från och med hösten 2022 att ha servrar inom EU. Medtronic överväger därför att framöver endast använda sig av Twilio, inte Clickatell.) Lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter är inte heller tillämplig heller på dessa bolag eftersom data förvaltas i annat land än Sverige.

15.10 Medtronic BV är verksamma i Nederländerna. I Nederländerna kompletteras dataskyddsförordningens av en nationell dataskyddslag, Uitvoeringswet Algemene Verordening gegevensbescherming (UAVG) 2018. Lagen innehåller inte, såvitt kan bedömas, några bestämmelser som reglerar en straffsanktionerad tystnadsplikt för medarbetare hos personuppgiftsbiträden i syfte att motverka obehörigt röjande av personuppgifter. Inte heller har någon annan lagstiftning identifierats som säkerställer ett motsvarande straffrättsligt skydd för medarbetare hos personuppgiftsbiträden verksamma i Nederländerna. Det har inte gått att med tillfredsställande säkerhet fastställa om det finns en straffsanktionerad individuell tystnadsplikt i Nederländerna för anställda hos personuppgiftsbiträden som har verksamhet i det landet, även om det inte kan helt uteslutas. Twilio, Inc. lagrar data i USA. I USA finns inte heller, såvitt är känt, en straffsanktionerad tystnadsplikt specifikt för personuppgiftsbiträden som ska motverka obehörigt röjande av kunddata. Det innebär att när en vårdgivare använder Medtronics tjänster för att bedriva distanssjukvård eller egenvård, enskilda individers hälsorelaterade uppgifter har ett svagare skydd vid förvar hos Medtronics personuppgiftsbiträden (med undantag för Medtronic AB) än när de är fysiskt förvarade hos en svenska vårdgivare.

15.11 AWS är verksamma i Tyskland. I Tyskland kompletteras dataskyddsförordningen 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 AWS.

15.12 Clickatell (Pty) Ltd lagrar sin data på Irland hos tjänsteleverantören Amazon. På Irland kompletteras dataskyddsförordningens av en nationell dataskyddslag, Data Protection Act 2018. Enligt 144 § kan enskilda medarbetare hos ett personuppgiftsbiträde som röjt eller lämnat ut personuppgifter till en tredje person utan godkännande av den personuppgiftsansvarige dömas upp till fem års fängelse eller 50.000 euro i böter. Det finns således en straffsanktionerad individuell tystnadsplikt på Irland för anställda hos molntjänstleverantörer som har verksamhet i det landet som ger ett godtagbart skydd.

Överföringar av personuppgifter till USA och andra länder

15.13 Medtronic samt leverantörerna AWS, Twilio, Inc. och Clickatell (Pty) Ltd 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 Medtronics fall är bolaget tydlig med i sin personuppgiftspolicy för enskilda användare av tjänsterna[36] att överföring av personuppgifter, inklusive hälsorelaterade uppgifter, kan ske för ändamålen produktutveckling, statistik för utveckling av marknadsföringsprodukter, sms-meddelanden och framtida forskning. Beträffande vårdgivare avser överföringen bl.a., men inte begränsat till, personuppgifter för ändamålet support (tredje linjens support).[37]

15.14 Medtronic har emellertid en lösning på plats som innebär att enskilda användares personuppgifter lagras i krypterad form i AWS:s servrar och databasapplikationer och att endast Medtronic förfogar över krypteringsnyckeln, inte AWS. Det är oklart vilket av dotterbolagen i Europa som läser in krypterade data lagrat hos AWS i sitt eget back-end system – Medtronic BV eller Medtronic AB eller båda två bolagen? Där dekrypteras den så att Medtronics applikationer kan utföra analyser och presentera resultat för respektive inloggad användare. All överföring av data är krypterad. All lagring och trafik mellan något av dotterbolagen och AWS sker således i krypterad form.

15.15 Beträffande överföringen av enskilda användares personuppgifter till USA, dvs. enskilda personer som använder CareLink Personal för egenvård enligt en vårdgivares förskrivning av Medtronics produkter inom ramen för ett egenvårdsbeslut, sker enligt Medtronic överföringen, såvitt förstås, i enlighet med kommissionens standardavtalsklausuler, Modul 3 i klausulerna. Data är krypterade under överföring genom användning av krypteringsnycklar som hanteras på ett säkert sätt.

15.16 Vid upprättande av ett konto i CareLink Personal möts användaren dock av ett ”samtyckesavtal”. Av det framgår följande: ”*Jag samtycker till insamling och behandling av mina personuppgifter (inklusive hälsouppgifter) utförd av Medtronic och dess databearbetningstjänster i samband med användningen av CareLink Personal och tillhörande mobilapplikationer, vilket kan inbegripa överföringar till USA*.” Texten följs av en ja- och nej-knapp. Såvitt förstås samtycker användaren till tredjelandsöverföringen genom ett uttryckligt samtycke antingen i appen eller i CareLink Personal vid registrering av ett konto.

15.17 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

[36] CareLink Meddelande om personlig sekretess den 24 september 2020.
[37] Avtal om Medtronic CareLink TM-tjänster (odaterad).

registrerade *när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder*. Det är oklart med vilken mekanism Medtronic överför enskilda personers glukosuppgifter till åtminstone USA – standardavtalsklausulerna eller artikel 49.1 a? Eftersom Medtronic efterfrågar ett explicit samtycke för överföringen utgår denna rättsutredning från att Medtronic i stället för standardavtalsklausulerna nyttjar ett samtycke enligt artikel 49.1 a i dataskyddsförordningen för sin tredjelandsöverföring av personuppgifter. De uppgifter som överförs i dessa sammanhang är pseudonymiserade personuppgifter, men Medtronic utesluter inte att enskilda individers personuppgifter kan identifieras.

15.18 Artikel 49.1 a i dataskyddsförordningen är en legitim grund som kan åberopas av Medtronic för sin tredjelandsöverföring av enskilda användares personuppgifter för avsedda ändamål. Överföring är dessutom enligt Medtronics villkor under användarens kontroll genom att denne kan stänga av överföringen av glukosvärden från sensorer och pumpar till CareLink Personal.

15.19 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. Bland annat uppger Medtronic i sin personuppgiftspolicy för enskilda användare[38] att bolagets ”*leverantörer av tredjepartstjänster uppfyller eventuellt inte alla dataskydds- och säkerhetsbestämmelser enligt ditt lands dataskyddslagar*.”

15.20 Enligt artikel 13 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.[39]

15.21 Medtronic kunde ha varit mer specifik med till vilka tredjeländer man överför användarens uppgifter, till vilka mottagare och på vilket sätt dessa länder brister i sitt dataskydd. t.ex. att utlänningar i USA saknar rättsliga och effektiva möjligheter att utöva kontroll över sina personuppgifter som är förvarade hos myndigheter.**.** Som minimum ska anges i informationen till registrerade tredjeländernas namn liksom kategorier av mottagare. Dessa brister avseende dels information om eventuella risker med

[38] CareLink Meddelande om personlig sekretess den 24 september 2020.
[39] Beslut 2022-03-28, dnr DI-2019-4062.

tredjelandsöverföringar för de registrerade, dels information om specifika mottagarländer och kategorier av mottagare bedöms innebära en hög risk för enskilda privata användares fri- och rättigheter vid behandling av personuppgifter för bl.a. ändamålen produktutveckling, statistik för utveckling av marknadsföringsprodukter och sms-meddelanden. Det erinras att brister i information till registrerade i sig kan innebära en otillåten behandling av personuppgifter som kan föranleda vitessanktioner. Medtronic har låtit meddela[40] att man avser att förtydliga informationen om risker med tredjelandsöverföringen, namngivna tredjeländer och kategorier av mottagare för enskilda användares personuppgifter i en ny version av sekretessmeddelandet (personuppgiftspolicyn).

15.22 Artikel 49.1 är vidare bara tillämplig om det saknas ett beslut om adekvat skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46). Av Medtronics personuppgiftspolicy för enskilda användare[41] anför bolaget att om bolaget överför användares personuppgifter (inklusive hälsouppgifter) till ett land som inte är medlem av Europeiska ekonomiska samarbetsområdet och för vilket inget beslut om adekvat skyddsnivå av kommissionen föreligger, kommer överföringen att ske utifrån kommissionens standardavtalsklausuler eller en av de andra överföringsmekanismerna i enlighet med dataskyddsförordningen. Standardavtalsklausulerna är en skyddsåtgärd som är uttryckligen angiven i artikel 46 i dataskyddsförordningen. Medtronic kan således inte stödja sig på någon av bestämmelserna i artikel 49.1 eftersom artikel 46 är ”aktiverad”. **Medtronic rekommenderas att justera sitt ”samtyckesavtal” (se ovan) så att det reflekterar de korrekta mekanismerna för tredjelandsöverföring, dvs. kommissionens standardavtalsklausuler**. Medtronic har uppgivit[42] att personuppgiftspolicyn för enskilda privata användare ger en missvisande bild av att personuppgifter överförs till tredje land baserat på samtycke. Enligt Medtronic överförs enskilda användares personuppgifter med stöd av enbart adekvansbeslut eller kommissionens standardavtalsklausuler. Medtronic förklarar dock att man avser att förtydliga överföringsmekanismerna för enskilda användares personuppgifter till tredje land i en ny version av sekretessmeddelandet (personuppgiftspolicyn).

15.23 Beträffande Medtronics åberopande av kommissionens standardavtalsklausuler i bolagets personuppgiftsbiträdesavtal[43] med vårdgivare är dessa inte inbäddade i avtalsvillkoren med vårdgivare. 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

[40] PM Information till SKR gällande Medtronics produkter den 16 maj 2022.
[41] CareLink Meddelande om personlig sekretess den 24 september 2020.
[42] PM Information till SKR gällande Medtronics produkter den 16 maj 2022.
[43] Avtal om Medtronic CareLink TM-tjänster (odaterad.

får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, ”inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation.”

15.24 Medtronic har uppgett att standardavtalsklausulerna inte är en bilaga till Medtronics avtalsvillkor inklusive personuppgiftsbiträdesavtal med svenska vårdgivare eftersom standardavtalsklausulerna inte ingås mellan en svensk vårdgivare och Medtronic utan mellan Medtronic AB (dataexportör) och Medtronic MiniMed, Inc. (dataimportören). Standardavtalsklausulerna kan tillhandahållas vårdgivare på begäran. Den modul som används är den från biträde till biträde, dvs. Modul 3. Medtronic åberopar standardavtalsklausulerna för att överföra vårdgivares personuppgifter till USA i syfte att genomföra bl.a. support, om det är absolut nödvändigt, dvs. om supporten i Europa inte kan lösa frågan.

15.25 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 oklar 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. Som minimum får förordningen anses kräva att den personuppgiftsansvarige anger med vilka mekanismer tredjelandsöverföring får ske. Så har skett. Medtronics avtalsvillkor inklusive personuppgiftsbiträdesavtal med vårdgivare anger att överföringsmekanismen är kommissionens standardavtalsklausuler. Att kommissionens standardavtalsklausuler inte är införda i Medtronics avtalsvillkor med vårdgivare och att det därmed inte framgår vilka klausuler och moduler i standardavtalsklausulerna som är tillämpliga är således *inte* en brist.

15.26 Medtronic har vidare ha ett behov av att överföra personuppgifter tillhörande vårdgivaren till myndighet i USA på grund av regulatoriska krav. En tillverkare av medicintekniska produkter, såsom Medtronic, har som regel ett ansvar för produktföljning som ska rapporteras till tillsynsmyndigheten, t.ex. incidenter med produkten. Det rör sig här om rapportering av personuppgifter i pseudonymiserad form. Villkoren för en sådan överföring regleras närmare i kommissionens standardavtalsklausuler, modul 3 (personuppgiftsbiträde [Medtronic AB] till personuppgiftsbiträde [Medtronic MiniMed, Inc]), punkt 8.8.

15.27 Emellertid framgår det av aktuell punkt i kommissionens standardavtalsvillkor att en ytterligare förutsättning för en tillåten överföring till tredje part, dvs. en amerikansk myndighet som utövar kvalitets- och säkerhetsövervakning av medicintekniska produkter, är att denna förpliktar sig att följa klausulerna i standardavtalsvillkoren eller

att någon av fyra fallsituationer är för handen.[44] Såvitt är känt har ingen amerikansk myndighet öppet deklarerat att de är bundna av standardavtalsklausulerna. Tvärtom är amerikanska myndigheter inte bundna av kommissionens avtalsvillkor, se vidare nedan. Vad som återstår är att någon av de fyra fallsituationerna är för handen. Av intresse är den tredje och fjärde fallsituationen, nämligen att överföringen sker dels för att den är nödvändig för att fastställa, utöva eller försvara rättsliga anspråk inom ramen för särskilda administrativa, lagstiftande eller rättsliga förfaranden, dels för att den är nödvändig för att skydda den registrerades vitala intressen eller någon annan fysisk persons vitala intressen.

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

15.29 Det är alltså tillåtet enligt kommissionens standardavtalsklausuler att överföra personuppgifter till en tredje part, i detta fall en amerikansk tillsynsmyndighet, när det är nödvändigt för att antingen fastställa, utöva eller försvara rättsliga anspråk inom ramen för särskilda administrativa, lagstiftande eller rättsliga förfaranden eller för att skydda den registrerades vitala intressen eller någon annan fysisk persons vitala intressen. En tillverkare av medicintekniska produkter har som regel lagstadgad skyldighet att göra marknadsuppföljning som ska rapporteras till tillsynsmyndigheten, t.ex. incidenter kopplade till produkten. Syftet med att rapportera incidenter är att värna om skyddet för patienter som kollektiv när det gäller produktens användning. Allvarliga brister kan bl.a. leda till marknadsförbud. Övervägande skäl tala således att Medtronic har rättsligt stöd för överföringen av personuppgifter om både patientuppgifter och hälso- och sjukvårdspersonal i pseudonymiserad form, men även i individform, i rollen som personuppgiftsbiträde åt en vårdgivare under förutsättning att en vårdgivare tecknar Medtronics avtalsvillkor om CareLink System och att Medtronic säkerställer att det finns en skriftlig instruktion från vårdgivaren till bolaget om att denna överföring får ske till tillsynsmyndighet i bl.a. USA för ändamålet regulatoriska krav inom produktsegmentet medicinteknik. **En sådan instruktion saknas och behöver tillföras Medtronics avtalsvillkor med vårdgivare avseende CareLink System.**

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

15.30 Medtronics produkter och molntjänster syftar till att låta enskilda användare att effektivt övervaka och behandla sin diabetes. Medtronic 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 CareLink Personal respektive CareLink System 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 CareLink Personal och CareLink System är bara relaterade till enskilda personers glukosvärden. Medtronic använder därtill end-to-end kryptering i syfte att skydda överföringar av data och kunddata.

15.31 Endast leverantörer av elektroniska kommunikationstjänster (electronic communication service providers) omfattas av övervakningsåtgärder som sker med stöd av Section 702 FISA, vilket inebergiper telekomoperatörer (telecommunication carriers), tjänsteleverantörer som tillhandahåller olika kommunikationstjänster (t.ex. tjänster för kommunikation över internet, ECS) och molntjänstleverantörer som tillhandhåller sådana tjänster ”till allmänheten” (remote computing services, RCS). Till skillnad från leverantörer av fjärrdatortjänster (RCS) behöver en ECS inte tillhandahålla tjänster till allmänheten; att ge eventuella användare – såsom företagets egna anställda – möjlighet att skicka eller ta emot kommunikation är tillräckligt.[45]

15.32 Det går därför inte att utesluta att Medtronic kan komma att omfattas av övervakningsprogram enligt Section 702 FISA på grund av att bolaget tillhandahåller tjänster ”till allmänheten”. **Däremot är risken högre för att Twilio eller Clickatell – leverantör av sms-meddelande- och chattjänster i CareLink Personal– omfattas av ett övervakningsprogram enligt Sektion 702 FISA**. Medtronic har dock informerat användaren om risken för sämre dataskydd i underleverantörernas hemland USA i samband med inhämtande av samtycke för mottagande av sms och chat i apparna – en funktionalitet som användaren kan avstå från. Twilio kommer från och med hösten 2022 att ha servrar inom EU. Medtronic överväger därför att framöver endast använda sig av Twilio, inte Clickatell. Vidare har Medtronic meddelat att man ser över möjligheten att på sikt övergå till en meddelandefunktion i Medtronics appar istället för via sms. Det skulle minimera de risker som här identifierats i förhållande till Sektion 702 FISA.

15.33 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 standardavtalsklausuler ”släcker” inte på något sätt dessa brister,

[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

såvida det inte finns adekvata skyddsåtgärder som effektivt förhindrar att amerikanska myndigheter från att ta del av svenska vårdgivares personuppgifter.

15.34 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.

15.35 Av Medtronics personuppgiftspolicy för enskilda användare[46] framgår att bolaget kan ”ombes att behandla användares personuppgifter (inklusive patienters hälsouppgifter) för att uppfylla alla rimliga begäranden från behöriga enheter eller ombud för brottsbekämpning, rättsliga myndigheter, statliga organ eller myndigheter, inklusive dataskyddsmyndigheter, i vilket fall bearbetningen begränsas till vad som minst krävs för att uppfylla föreläggandet.” En motsvarande ansvarsbegränsning finns i Medtronics avtalsvillkor inklusive personuppgiftsbiträdesavtal för CareLink Personal med vårdgivare.[47] Medtronic har således friskrivit sig från ansvar gentemot användare respektive vårdgivare om att lämna ut data om denne på begäran av amerikansk domstol enligt Cloud Act. I avtalsvillkoren för vårdgivare är Medtronic tydliga med att de måste respektera ett yppandeförbud från t.ex. amerikansk domstol i samband med en domstolsorder.

15.36 Det finns således en kvarstående risk, trots organisatoriska och tekniska åtgärder från Medtronics 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 Medtronics kunduppgifter får dock betraktas som mycket låg med hänsyn till kärnverksamheten (diabetesmonitorering) samt att Medtronic ensam förfogar över krypteringsnyckeln för data som behandlas av AWS**. **Det finns andra risker, t.ex. cyberattacker mot molntjänster, som får betraktas som högre och mer allvarliga.**

Personuppgiftsansvaret i trepartsförhållandet vårdgivare, Medtronic och enskild användare

15.37 Medtronics CGM/SAP-system är verktyg enbart för vårdgivare för att bedriva diabetesvård. Medtronics produkter 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. Medtronics

[46] CareLink Meddelande om personlig sekretess den 24 september 2020.
[47] Avtal om Medtronic CareLink TM-tjänster (odaterad).

produkter finns inte till försäljning i Sverige för konsumentbruk, dvs. för självhjälp och egen monitorering och insulinbehandling.

15.38 Medtronic har skapat en lösning som har en helt tydlig separation mellan behandlingen av enskildas hälsokonton i CareLink Personal och vårdgivares konton i CareLink System. I personuppgiftspolicyn för enskilda användare[48] skriver Medtronic bl.a. följande:

"*Genom att upprätta en länk till CareLink TM Personal kan en sjukvårdsinrättning se patienters hälsouppgifter från kompatibla enheter och diabetesövervakningsverktyg som har överförts till CareLink TM Personal (till exempel blodglukosnivåer och loggboksposter) i CareLink TM System. CareLink TM System används av vårdinrättningar och vårdgivare som underlag för behandlingsbeslut och för bättre interaktioner.*

När en länk upprättas mellan CareLink TM Personal och CareLink TM System får patienter på grund av det dubbelriktade datautbytet mellan dessa system också direkt åtkomst i CareLink TM Personal till sina enhetsdata i den form de ursprungligen överfördes till CareLink TM System. För att upprätta länken integreras en funktion för uttryckligt samtycke i CareLink TM System som patienten måste godkänna, utöver en konfidentiell engångsinmatning av det unika användarnamnet och lösenordet. En patient kan när som helst besluta att avlänka sitt CareLink TM Personal-konto från CareLink TM System i inställningarna för sitt CareLink TM Personal-konto, vilket stoppar eventuell ytterligare delning av framtida uppgifter relaterade till CareLink TM Personal med CareLink TM System-kontot i fråga.

Observera att när en patient samtycker till att upprätta en länk mellan CareLink TM Personal och CareLink TM System, byts följande personuppgiftskategorier ut och behandlas för alla syften som patienten har samtyckt till i CareLink TM Personal:
- "Hälsouppgifter" avser olika typer av hälsorelaterade data som genereras och mäts med kompatibla enheter och diabetesövervakningsverktyg som vårdgivaren har överfört till CareLink TM System."

15.39 Medtronic har vidare uppgivit att den information som lagras i CareLink System är data om insulin- respektive glukosnivåer som registrerats i den enhet (insulinpump eller glukosmätare) ("Medicinsk Enhet") som den enskilda användaren förfogar över.[49] Dessa uppgifter samlas enligt Medtronic normalt sett in i CareLink Personal och överförs därefter från CareLink Personal till CareLink System. Medtronic förklarar att överföring kan även ske åt andra hållet, efter att data vid vårdbesök hos klinik laddats upp av en vårdgivare direkt i CareLink System och därefter överförs till CareLink Personal. Det är enligt Medtronic alltså samma typ av data som överförs till CareLink Personal från CareLink System som från CareLink System till CareLink Personal. Ingen annan typ av data överförs. Medtronic torde här mena att direktåtkomst inte förekommer i tjänsten.

[48] CareLink Meddelande om personlig sekretess den 24 september 2020
[49] PM Information till SKR gällande Medtronics produkter den 16 maj 2022.

Med direktåtkomst menas vanligen att någon har direkt tillgång till någon annans databas eller register och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i databasen eller registret. Begreppet brukar också anses innefatta att den som är ansvarig för databasen eller registret inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av. Vid direktåtkomst anses de uppgifter som omfattas av åtkomsten utlämnade i och med att åtkomsten medges.

15.40 Det innebär att vårdgivare inte kan gå in i CareLink Personal och kan alltså inte heller söka fritt bland informationen i CareLink Personal. Medtronic lämnar ut information från CareLink Personal till CareLink System med stöd av ett samtycke från den enskilde. Vårdgivaren har därefter bara tillgång till informationen om den enskilde i CareLink System. Utlämnandet sker vid begäran från vårdgivaren.

15.41 Såvitt kan bedömas har Medtronic skapat tydliga ansvarsförhållanden mellan sig själv i rollen som personuppgiftsansvarig för enskildas CareLink Personal-konton och vårdgivare, tillika personuppgiftsansvariga för sin behandling av personuppgifter i CareLink System, vid delning av insulin- och glukosdata. Det beror på att överföringen av uppgifter mellan den enskildes CareLink Personal-konto hos Medtronic och en vårdgivare som förfogar över ett CareLink System-konto, vilken är dubbelriktad, inte sker genom direktåtkomst utan på ett kontrollerats och säkert sätt genom s.k. ADB-utlämnande, dvs. filöverföring. Den arkitektur som Medtronic har skapat balanserarar väl vårdgivares behov av data kontra enskildas behov av skydd för sin personliga integritet, och får anses ändamålsenlig ur ett juridiskt perspektiv för självhjälp och egenvård. Arkitekturen innebär att vårdgivare inte behöver ta ett större juridiskt ansvar än nödvändigt för tjänsten och att den enskilde användaren, tillika patienten, får ett stort mått av självbestämmande över sina egna insamlade uppgifter.

15.42 Vid behandling av patientuppgifter i CareLink Connect-appen respektive CareLink System är patientansvarig vårdgivare personuppgiftsansvarig. Det är inte helt klarlagt hur vårdgivare använder sig av Medtronics diabetesprodukter. Såvitt förstås kan en svensk vårdgivare inte koppla en patients mätare eller pump direkt till vårdgivarens konto i CareLink System i syfte att ge vård och utan att patienten har ett eget användarkonto i samma system. Vårdgivare skapar inte heller konton åt patienter i CareLink Personal. Det enda tillämpliga användarfallet är att en patient skapar ett användarkonto i CareLink Personal och ger vårdgivaren tillgång till överförd data från användarkontot för att vårdgivaren ska kunna behandla dennes personuppgifter. (Här bortses från att en patient kan koppla t.ex. sin insulin-pump till en avläsare hos vårdgivaren och överföra glukosdata till CareLink System vid ett vårdbesök.)

15.43 Det råder således ingen tvekan om att Medtronic är personuppgiftsansvarig för patientens konto och personuppgifter i CareLink Personal. Det är Medtronic 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 Medtronic 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 Medtronic

personuppgiftsansvarig för behandlingen av patientens personuppgifter i produkten.[50] Dataskyddsförordningen är tillämplig på personuppgiftsbehandlingen. De uppgifter som överförs till vårdgivarens konto i CareLink System är vårdgivaren personuppgiftsansvarig för. Medtronic AB är personuppgiftsbiträde i denna del.

15.44 **Medtronic MiniMed, Inc. och Medtronic International Trading sàrls (Medtronic) 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 CareLink System när denne efterfrågar uppgifterna. Medtronic är personuppgiftsansvarig för den enskildes CareLink Personal-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 Medtronics produkter, ställer lagstiftningen krav på att vårdgivaren har full kontroll över alla moment eller arbetsuppgifter i vården. Det skulle förutsätta att Medtronics produkter kopplas direkt till vårdgivarens klinik-konto i CareLink System eller att vårdgivaren skapar konton och tillhandahåller användaruppgifter åt patienter i CareLink Personal. Så är inte fallet nu.

Enskild användares delning av data med andra via -appen

15.45 En enskild person kan i CareLink Personal dela sina data med upp till 5 personer, t.ex. anhöriga, såvida dessa förfogar över en dator eller en CareLink Connect-app. 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 Medtronic är personuppgiftsansvarig. Beträffande delning med en vårdgivare genom CareLink Personal-konto, se under rubriken Personuppgiftsansvaret i trepartsförhållanden vårdgivare, Medtronic och enskild användare i detta avsnitt.

Autentisering av användare

15.46 Inloggning i Guardian Connect- respektive MiniMed Mobile-apparna samt CareLink Connect-appen sker med enfaktorsautentisering (användarnamn och lösenord). Enfaktorsautentisering ger användaren en möjlighet till enkel avläsning av Guardian Connect-sändaren. Användares åtkomst till egen data i CareLink Personal (www.carelink.minimed.eu) sker också med enfaktorsautentisering. Åtkomst kan än så länge inte ske med Bank-ID eller annat elektroniskt ID. Vårdgivare däremot loggar in på sitt klinik-konto i CareLink System med tvåfaktorsautentisering. Det sker genom engångslösenord via sms eller e-post. . De kan inte nyttja SITHS-kort eller annat slag av e-legitimation vid inloggning till tjänsten.

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

15.47 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.

15.48 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).

15.49 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”.

15.50 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.

15.51 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.

15.52 **Beträffande vårdgivares inloggning till sitt klinik-konto i CareLink System lever Medtronic i rollen som leverantör upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd.** Beträffande en enskild persons inloggning till sitt konto på www.carelink.minimed.eu och via apparna Guardian Connect, MiniMed Mobile och CareLink Connect 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 och på www.carelink.minimed.se (CareLink Personal) bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Medtronic har förklarat att det dock finns tekniska förutsättningar att införa tvåfaktorsautentisering i CareLink Personal.[51] Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i CareLink System ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.**

Framtida forskning

15.53 När en användare skapar för första gången ett konto i CareLink Personal, efterfrågar tjänsten samtycke av användaren för att låta Medtronic använda glukosdata, inom EU eller i USA, utan koppling till användaren för ändamålet framtida forskning. Av informationen som lämnas i samband härmed samt av Medtronics personuppgiftspolicy för enskilda användare[52] av bolagets tjänster framgår att sammanställd data inte innehåller någon information som kan identifiera användaren direkt, men ”de utesluter inte fullständigt möjligheten att identifiera dig”. Det är ett frivilligt samtycke och inte ett villkor för att använda tjänsten.

15.54 Varken informationen som lämnas vid skapandet av ett konto eller personuppgiftspolicyn för enskilda användare specificerar vad för slags forskning det rör sig om eller vilka som ska bedriva forskningen. Vad som framgår är att Medtronic hävdar att bolaget enbart kommer att använda sig anonymiserade data.

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

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

[51] Information till SKR gällande Medtronics produkter den 3 juni 2022.
[52] CareLink Meddelande om personlig sekretess den 24 september 2020.

”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.

15.57 Medtronic har uppgivit[53] att den information som lämnas i Medtronics samtyckesformulär specificerar dock att uppgifterna kommer att användas för att ”forska om och utveckla nya produkter och tjänster för diabetesbehandling och förbättra befintliga produkter och tjänster samt att övergripande förbättra behandlingsregimerna och patienternas behandling”. Formuleringen är enligt Medtronic avsevärt mer specificerad än ”framtida forskning”.

15.58 Av skäl 33 i dataskyddsförordningen framgår 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 enligt skäl 33 kunna ge sitt samtycke till vissa områden för forskning, när vedertagna etiska standarder för forskning iakttas.

15.59 Mot bakgrund av vad Medtronic har anfört bedöms CareLink Personal innefatta en tillåten personuppgiftsbehandling såvida användaren väljer att samtycka till framtida forskning..

Kakor och tredjepartsaktörer

15.60 Medtronic använder Google Analytics och Adobe Analytics i sina appar, vilka kräver kakor. Både Google Analytics och Adobe Analytics används för att samla in information om användningen av Medtronics appar i syfte att förbättra användarupplevelsen. Google Analytics och Adobe Analytics används inte i CareLink Personal, utan endast i vissa av de appar tillhörande CareLink Personal som Medtronic tillhandahåller enskilda. I appen MiniMed Mobile används endast Adobe Analytics, inte Google Analytics. Tjänsterna tillhandahålls av amerikanska leverantörer (Google och Adobe).. Kakorna bedöms som nödvändiga för tjänstens funktionalitet. Eventuella personuppgifter som överförs till USA via dessa kakor är Medtronic mottagare av. Överföringen har, såvitt förstås, stöd i artikel 49.1 a (samtycke) i dataskyddsförordningen.

15.61 Google Analytics används av Medtronic för att samla in information om användningen av mobilapplikationen i syfte att förbättra användarupplevelsen. Den typ av information som samlas in är aggregerad och avidentifierad. Prestandaövervakningsdata kan inkludera appversion, land, OS-nivå, enhet, radio- och operatörsinformation. Det är oklart om data innehåller information sensorers och pumpars serienummer eller några andra personuppgifter, däribland hälsorelaterad information.

[53] PM Information till SKR gällande Medtronics produkter den 16 maj 2022.

15.62 Överföring av personuppgifter till USA eller till annat tredjeland via Medtronics underleverantörer Google respektive Adobe kan dock inte uteslutas. Både Google Analytics och Adobe Analytics registrerar IP-nummer hos användare av appar. I fallet med Google Analytics kan Google sannolikt hänföra IP-nummer från en enskild privat användares app till eventuellt Google-konto som användaren också använder. Google kan därmed identifiera individen och rikta direktreklam om vårdrelaterade tjänster eftersom Guardian Connect-appen är en hälsoapp. Det finns också en risk för en otillåten överföring av personuppgifter av Google till tredjeland (USA) på grund av bristande information till registrerade. Vidare har den österrikiska dataskyddsmyndigheten, Datenschutzbehörde, i ett beslut[54] ansett att varaktig användning av ett tyskt företag av Google Analytics inneburit ett brott mot dataskyddsförordningen. Kommissionens standardavtalsklausuler, som Google använder, ger enligt dataskyddsmyndigheten inte ett tillräckligt skydd eftersom bolaget är en aktör som är föremål för övervakningsbegäran av amerikanska underrättelsemyndigheter enligt Section 702 FISA. **Tredjepartstjänsterna Google Analytics och Adobe Analytics innebär en risk för otillåten behandling av personuppgifter**. **Risken får betraktas som hög**.

15.63 Medtronic har i huvudsak anfört följande:[55] Den typ av uppgifter (aggregerad data) som överförs till Google respektive Adobe tar sikte på att samla in information om användningen av Medtronics appar, såsom information om från vilken appbutik en viss app har laddats ner och hur ofta appen öppnats inom en viss tidsperiod. Användningen av Google Analytics och Adobe Analytics är begränsad till vad som är strikt nödvändigt för att mäta bl.a. appstatistik och apprestanda. Den metadata som samlas in kan inte användas för marknadsföring. Funktionen för riktad reklam är inaktiverad. Av allt att döma saknas även anledning att tro att den begränsade överföring av data som sker till Google och Adobe skulle vara av intresse för amerikansk underrättelsetjänst.[56] Baserat på bl.a. ovanstående kan risken inte, enligt Medtronic, anses vara hög. Vad avser själva tredjelandsöverföringen till USA noteras att det finns olika lokala beslut från tillsynsmyndigheter[57] och att EU och USA därutöver förhandlar en principöverenskommelse avseende överföring av personuppgifter från EU till USA, vilken får antas kommer att undanröja bl.a. de hinder som EU-domstolens dom ”Schrems II” inneburit. I sammanhanget kan även nämnas att det beslut den österrikiska dataskyddsmyndigheten Datenschutzbehörde meddelade, bedömde cookies på en webbsida och alltså inte Google Analytics SDK, som är den tjänst som används av Medtronic. Det måste även, i Medtronics mening, skiljas på situationen där aktörer som Google och Adobe samlar in och använder personuppgifter för egna ändamål och medel och situationer där de endast är biträden. Även om anmärkningar om bristande transparens skulle kunna riktas mot bolagens egna personuppgiftsbehandling betyder inte det att samma anmärkningar kan göras gällande i deras roll som personuppgiftsbiträde,

[54] Datenschutzbehörde den 22 december 2021, D155.027, 2021-0.586.257.
[55] Information till SKR gällande Medtronics produkter den 3 juni 2022.
[56] Inklusive med beaktande av ”The White Paper ‘Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.’ of September 2020”, utfärdad av amerikanska myndigheter.
[57] T ex har den franska dataskyddsmyndigheten CNIL funnit att en överföring till Google kan ske med stöd av den registrerades samtycke enligt Artikel 49 GDPR.

och därigenom läggas den personuppgiftsansvarige till last. Det kan noteras att det i Sverige inte har fattats något beslut avseende bolags användning av Google Analytics. Medtronic avvaktar därför de beslut i frågan som är att vänta från Integritetsskyddsmyndigheten för att därefter ta ställning till vilka eventuella förändringar detta kan innebära för de appar som tillhör CareLink Personal.

15.64 Vad Medtronic anfört i denna del föranleder ingen annan bedömning. Riskbedömningen kvarstår.

På uppdrag av SKR

Manólis Nymark

Bilaga 1

Medtronic

Information till SKR gällande Medtronic produkter.

TILL:	Manolis Nymark
FRÅN:	Medtronic AB
DATUM:	20 juni 2022
ANGÅENDE:	Laglighetsprövning av Medtronics produkter

1 BAKGRUND

1.1 Denna skrivelse har tagits fram för att bemöta de synpunkter som framförts i det uppdaterade utkast till laglighetsprövning Manolis Nymark tagit fram (”**SKR Analysen**”) och som tillhandahållits Medtronic AB den 16 juni 2022.

1.2 Medtronic vill inledningsvis framhålla att bolagen tar de aktuella frågorna på allvar och anser att de är av högsta relevans för den typ av produkter och tjänster som Medtronic tillhandahåller.

1.3 I samband med tillhandahållande av det första utkastet av SKR Analysen har Manolis Nymark efterfrågat synpunkter avseende de sakförhållanden som framförs i rapporten. Medtronic önskar framföra de synpunkter och kommentarer som framgår av punkterna 2–6.

2 IT-OUTSOURCING

2.1 Det har i SKR Analysen (punkt 14 samt punkt 15.7 och framåt) redogjorts för den problematik som föreligger vid outsourcing av IT-drift från myndighet till privat aktör när sådana tjänster tillhandahålls utanför Sveriges gränser.

2.2 Problematiken ligger i att myndighetens information, som kan träffas av tystnadsplikt enligt svensk lag, blir tillgänglig på platser där svensk lag inte gäller, varvid de personer som har tillgång till uppgifterna kan komma att röja informationen utan konsekvenser enligt svensk rätt.

2.3 Ytterligare en problematik är att bestämmelser i det mottagande landets lagstiftning kan innebära en rätt för det landets myndigheter att bereda sig tillgång till uppgifterna.

2.4 Information som behandlas inom CareLink Personal lagras både hos AWS i Tyskland och hos Medtronic BV i Nederländerna. När det gäller CareLink System lagras informationen bara hos Medtronic BV i Nederländerna. Medtronic har dock för avsikt att inom kort även börja lagra vissa uppgifter i CareLink System hos AWS i Tyskland.

2.5 SKR Analysen förefaller redogöra för risker kopplade till lagringen avseende såväl CareLink Personal som CareLink System. Någon myndighetsdata lagras dock inte i CareLink Personal.

2.6 **CareLink Personal**

2.6.1 Såsom har redogjorts för i SKR Analysen är CareLink Personal ett system för vilket Medtronic självt är ansvarigt. Det tillhandahålls ingen tjänst till vårdgivaren genom CareLink Personal och den information som lagras i CareLink Personal är inte vårdgivarens information utan Medtronics. Riskerna för informationen i CareLink Personal ligger alltså på Medtronic och inte på vårdgivaren.

2.6.2 Information kan visserligen överföras från CareLink System till CareLink Personal. Detta får dock, såvitt Medtronic förstår, jämföras med att uppgifterna lämnar vårdgivaren och överlämnas till patienten, på samma sätt som i övrigt gäller vid utlämnande av allmän handling.

2.6.3 När informationen har överförts till patienten kan det, såvitt Medtronic förstår, inte längre anses vara vårdgivarens ansvar hur uppgifterna hanteras av patienten. Vårdgivarens ansvar ligger istället i att göra en korrekt sekretessbedömning innan utlämnandet till patienten sker.

2.6.4 Med ovan resonemang vill Medtronic visa att det inte sker någon lagring av *myndighetsdata* inom ramen för CareLink Personal och - för tydlighetens skull - att det som redogjorts för i SKR Analysen avseende problematiken vid IT-outsourcing inte är relevant i förhållande till CareLink Personal, eftersom den överförda datan inte omfattas av reglerna i OSL.

2.6.5 Medtronic kan upplysningsvis nämna att Medtronic har för avsikt att lansera en funktion där det finns möjlighet för vårdgivaren att spärra informationsflöden från CareLink System till CareLink Personal.

2.6.6 Bolaget Twilio anlitas endast för tjänster inom CareLink Personal, inte CareLink System. Medtronic anser därför inte att det är relevant att bedöma Medtronic MiniMed, Inc. Medtronic International Trading sàrl, Twilio och Clickatell i SKR Analysen, såsom skett i punkten 15.8-15.9.

2.7 **CareLink System**

Tystnadsplikt enligt offentlighets- och sekretesslagen

2.7.1 När det gäller CareLink System lagras uppgifter av Medtronic AB för vårdgivarens räkning och Medtronic AB är således personuppgiftsbiträde till vårdgivaren. Den data som lagras är myndighetsdata och träffas, precis som redogjorts för i SKR Analysen, därför av reglerna i OSL.

2.7.2 Såvitt Medtronic förstår röjer vårdgivaren sekretessen i förhållande till Medtronic AB och dess underleverantörer med stöd av den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL. Vårdgivarna får idag antas ha bedömt att sådant utlämnande kan ske.

2.7.3 Den ”menprövning” som redogörs för i SKR Analysen punkten 14.11 och framåt, uppfattas ta avstamp i denna bestämmelse. Det ska dock noteras att det i IT-driftsutredningen föreslås att en ny sekretessbrytande bestämmelse ska införas i OSL, som ger ett tydligare stöd för att lämna ut uppgifter inom ramen för en utkontraktering av IT-drift (se SOU 2021:1 s. 293).

2.7.4 Det bör därför i Medtronics mening, i avvaktan på det nya lagförslaget, inte dras några allt för långtgående slutsatser om vad nuvarande reglering innebär i förhållande till Medtronics lagring av uppgifter inom CareLink System.

2.7.5 Det har i SKR Analysen punkten 14.11 även redogjorts för att vårdgivaren vid ”menprövningen” måste ta hänsyn till huruvida det mottagande landets lagstiftning innehåller en straffsanktionerad sekretessbestämmelse, oaktat om det mottagande landet är ett EU-land eller ett tredje land. Sådana hänsyn får dock, i enlighet med vad som framförts i IT-driftsutredningen (SOU 2021:1 s. 300), anses stå i strid med EU-rättens likabehandlingsprincip, varför en sådan prövning endast ska ske i förhållande till tredje land.

2.7.6 En ”menprövning” i strid med EU-rättens likabehandlingsprincip kan i förlängningen leda till en olaglig diskriminering av Medtronic.

2.7.7 Medtronic menar därför att en eventuell avsaknad av lagstadgad tystnadsplikt i ett annat EU-land inte kan tas i beaktande vid bedömning av eventuella risker för vårdgivaren.

GDPR

2.7.8 I SKR Analysen förs även ett resonemang kring att reglerna om tystnadsplikt i OSL ska ha bäring på vårdgivarens val av personuppgiftsbiträde i enlighet med

artikel 28(2) GDPR. Som framgår av IT-driftsutredningen (SOU 2021:1 s. 202–203 och 338) är dock den ”omsorgsplikt” som nämns i SKR Analysen endast tänkt att tillämpas i förhållande till *tredje land* och alltså inte i förhållande till andra EU-länder.

2.7.9 Det kan därför inte, enligt Medtronics mening, vara ett krav att en personuppgiftsansvarig, *från ett GDPR-perspektiv*, skulle behöva bedöma riskerna med en överföring till ett annat EU-land. En sådan tolkning får anses strida mot kärnan i GDPR (och EU-rätten i stort) som bygger på ett ömsesidigt förtroende mellan medlemsstaterna. Det finns inte heller stöd för att göra någon åtskillnad i förhållande till sådana uppgifter som är att betrakta som ”känsliga personuppgifter” enligt artikel 9 GDPR, så länge uppgifterna behandlas inom EU.

Tredjelandsöverföring

2.7.10 IT-driftsutredningen (SOU 2021:1 s. 215) har därutöver konstaterat att det inte är fråga om en tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om den personuppgiftsansvarige eller personuppgiftsbiträdet som behandlar personuppgifterna är bunden av tredjelands lagstiftning som innebär att denne kan åläggas att lämna ut uppgifter direkt till ett tredjelands myndigheter. Tredjelandsöverföringen sker först i samband med att uppgifterna överförs till myndigheter eller annan mottagare i tredjeland.

2.7.11 Personuppgiftsbiträde till vårdgivaren för personuppgiftsbehandlingen som sker i CareLink System är det svenska bolaget Medtronic AB. Data i CareLink System lagras i Nederländerna och behandlas inte för de syften (exempelvis forskning, meddelandetjänster eller framtagande av marknadsförings- och utbildningsmaterial) för vilka personuppgifter eller aggregerad data kan komma att överföras till tredje land. Sådan överföring baseras på personuppgifter som hämtas från CareLink Personal.

2.7.12 Den enda tredjelandsöverföring som blir aktuell i förhållande till CareLink System, och för vilken vårdgivaren är personuppgiftsansvarig, är sådan överföring som sker i samband med tillhandahållande av support och då endast i de fall då ett supportärende inte kan lösas inom EU.

3 LEGAL GRUND FÖR BEHANDLING OCH SAMTYCKE TILL BEHANDLING AV KÄNSLIGA PERSONUPPGIFTER

3.1 Medtronic noterar den otydlighet rörande laglig grund för behandlingen som anges i Medtronics Sekretessmeddelande och som redogjorts för i bl.a. punkt 6.3-6.11 i SKR Analysen.

3.2 Medtronic menar dock att även om informationen i Sekretessmeddelandet exempelvis felaktigt skulle ange ”samtycke” som laglig grund, när det rör sig om behandling som rätteligen borde stödjas på ”fullgörande av avtal”, innebär detta inte att det saknas en laglig grund för behandlingen enligt Artikel 6. Detta

eftersom det faktiskt föreligger förutsättningar för behandlingen enligt Artikel 6(1)(b). Däremot kan en sådan otydlighet utgöra ett brott mot Artikel 13–14 GDPR.

3.3 När det gäller de samtycken som en användare har möjlighet att ta ställning till vid registrering av konto i CareLink Personal noterar Medtronic att det kan finnas en viss otydlighet avseende om det rör sig om ett samtycke enligt artikel 6 eller artikel 9 GDPR.

3.4 Som framförts i punkten 15.59 SKR Analysen är behandlingen för ”framtida forskning” i CareLink Personal definierad på så sätt som krävs enligt GDPR.

3.5 Däremot kan det anses vara en brist att det inte med tydlighet framgår till vilket bolag (Medtronic MiniMed Inc) eller i vart fall till vilken *kategori av mottagare* uppgifterna överförs för sådan forskning.

3.6 Därtill kan den formulering som finns i samtyckesformuläret, precis som har påpekats i SKR Analysen, ge en missvisande bild av att personuppgifter överförs till tredje land baserat på samtycke.

3.7 Som framgår av Medtronics Sekretessmeddelande överförs personuppgifter endast till tredje land baserat på standardavtalsklausuler, om inget beslut om adekvat skyddsnivå föreligger.

3.8 Det bör dock i förhållande till ovanstående tas i beaktande vilken risk denna otydlighet kan medföra för den enskilde. Även om anonymiseringen utgör ett behandlingssteg är de uppgifter som därefter överförs till Medtronic MiniMed Inc aggregerade till den grad att det som regel inte rör sig om personuppgifter.

3.9 Medtronic har trots det, i sitt Sekretessmeddelande, tagit höjd för att det inte kan uteslutas att identifiering i något enskilt fall skulle kunna vara möjlig. Riskerna förknippade med denna bristfälliga information får därför enligt Medtronics bedömning anses vara minimala.

3.10 Medtronic är för närvarande i processen att uppdatera sitt Sekretessmeddelande och nya samtycken och kommer därvid att ta ovanstående problematik i beaktande. Även om eventuell bristande laguppfyllelse avseende ovan endast är relevant i förhållande till CareLink Personal, inte CareLink System, och att såväl ansvar som risk för denna behandling ligger på Medtronic, inte på vårdgivaren, är Medtronic öppen för en vidare dialog med SKR i frågan, om så önskas.

4 TWILIO, CLICKATELL, GOOGLE OCH ADOBE

4.1 Medtronic noterar de risker som enligt SKR Analysen bedömts föreligga avseende överföring till bolagen Twilio och Clickatell samt avseende Adobe och Google. Medtronic vill dock trycka på att denna behandling sker inom CareLink

Personal, inte CareLink System, och att risk och ansvar i denna del därför faller på Medtronic, inte vårdgivaren. Dessutom anser Medtronic att de aktuella riskerna är låga.

4.2 Avseende Twilio och Clickatell noteras att risken i SKR Analysen har bedömts vara mycket låg, med hänsyn till den typ av data som hanteras i Medtronics kärnverksamhet, se SKR Analysen 15.36.

4.3 Gällande informationen i Medtronics Sekretessmeddelande har det i SKR Analysen, punkterna 9-10 i sammanfattningen, framförts att informationen brister i förhållande till den tydlighet som krävs enligt Artikel 12 GDPR. Denna bedömning förefaller ta avstamp i situationen att överföringen till bolaget Twilio i USA skulle grunda sig på samtycke enligt Artikel 49 GDPR. Som framgår av punkten 12 (i sammanfattningen) i SKR Analysen sker överföring av personuppgifter dock med stöd av standardavtalsklausuler, inte med stöd av samtycke.

4.4 När det gäller Clickatell lagras uppgifterna inte i USA utan på servrar på Irland. Twilio kommer från och med hösten 2022 att ha servrar inom EU. Medtronic överväger att framöver endast använda sig av Twilio, inte Clickatell.

4.5 Medtronic vill även i detta sammanhang framhålla att IT-driftsutredningen (SOU 2021:1 s. 215) funnit att den omständigheten att ett bolag träffas av lagstiftning såsom FISA 702 inte *i sig* innebär att det sker en överföring av personuppgifter till tredje land.

4.6 Upplysningsvis kan även nämnas att Medtronic ser över möjligheten att på sikt övergå till en meddelandefunktion i Medtronics appar istället för via SMS, vilket ytterligare skulle minimera de risker som enligt SKR Analysen ska föreligga i förhållande till FISA 702.

4.7 När det gäller Google Analytics respektive Adobe Analytics noterar Medtronic vad som framförts i SKR Analysen men har en avvikande uppfattning. För tydlighets skull kan noteras att Google Analytics och Adobe Analytics inte används i CareLink Personal, utan endast i vissa av de appar tillhörande CareLink Personal som Medtronic tillhandahåller enskilda. I appen MiniMed Mobile används endast Adobe Analytics, inte Google Analytics.

4.8 Den typ av uppgifter (aggregerad data) som överförs till Google respektive Adobe tar sikte på att samla in information om användningen av Medtronics appar, såsom information om från vilken appbutik en viss app har laddats ner och hur ofta appen öppnats inom en viss tidsperiod. Användningen av Google Analytics och Adobe Analytics är begränsad till vad som är strikt nödvändigt för att mäta bl.a. appstatistik och apprestanda. Den metadata som samlas in kan inte användas för marknadsföring. Funktionen för riktad reklam är inaktiverad.

4.9 Av allt att döma[58] saknas även anledning att tro att den begränsade överföring av data som sker till Google och Adobe skulle vara av intresse för amerikansk underrättelsetjänst.

4.10 Baserat på bl.a. ovanstående kan risken inte, enligt Medtronic, anses vara hög.

4.11 Vad avser själva tredjelandsöverföringen till USA noteras att det finns olika lokala beslut från tillsynsmyndigheter och att EU och USA därutöver förhandlar en principöverenskommelse avseende överföring av personuppgifter från EU till USA, vilken får antas kommer att undanröja bl.a. de hinder som EU-domstolens dom ”Schrems II” inneburit.

4.12 Därutöver kan noteras att beslutet från den österrikiska dataskyddsmyndigheten Datenschutzbehörde som nämns i punkterna 15.62–63 i SKR Analysen, samt ett efterföljande beslut i samma fråga från den franska dataskyddsmyndigheten CNIL, avsåg de kompletterande skyddsåtgärder som ska användas tillsammans med de överföringsverktyg som avses i Artikel 46 GDPR och inte överföring baserat på samtycke enligt Artikel 49.1.a GDPR.

4.13 I sammanhanget kan även nämnas att beslutet från österrikiska Datenschutzbehörde avsåg cookies på en webbsida och alltså inte Google Analytics SDK, som är den tjänst som används av Medtronic.

4.14 Det måste även, i Medtronics mening, skiljas på situationen där aktörer som Google och Adobe samlar in och använder personuppgifter för *egna ändamål och medel* och situationer där de endast är biträden. Även om anmärkningar om bristande transparens skulle kunna riktas mot bolagens egna personuppgiftsbehandling betyder inte det att samma anmärkningar kan göras gällande i deras roll som personuppgiftsbiträde, och därigenom läggas den personuppgiftsansvarige till last.

4.15 Därtill kan noteras att risken vid motsvarande överföring till Clickatell och Twilio enligt SKR Analysen har bedömts vara låg.

4.16 Det kan noteras att det i Sverige inte har fattats något beslut avseende bolags användning av Google Analytics. Medtronic avvaktar därför de beslut i frågan som är att vänta från Integritetsskyddsmyndigheten för att därefter ta ställning till vilka eventuella förändringar detta kan innebära för de appar som tillhör CareLink Personal.

[58] Inklusive med beaktande av ”The White Paper ‘*Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.*’ of September 2020”, utfärdad av amerikanska myndigheter.

4.17 Oaktat ovan kommer Medtronic självklart att se över om och hur man kan uppdatera informationen i Medtronics Sekretessmeddelande med tydligare information om riskerna med överföringen.

5 ÖVRIGT

5.1 Såsom framgår av punkten 15.56 i SKR Analysen finns inga krav på tvåfaktorsautentisering i CareLink Personal. Om det är önskemål om att införa tvåfaktorsautentisering i CareLink Personal så genomför vi detta.

5.2 Om det av SKR, trots avsaknad av krav i författning, bedöms vara en förutsättning för Regionernas fortsatta användning av Medtronics produkter kommer Medtronic självklart att införa tvåfaktorsautentisering i CareLink Personal. Medtronic är i färd med att se över hur lång tid det skulle ta att införa sådan autentisering.

5.3 Det har i punkterna 15.24-15.25 i SKR Analysen anmärkts på att det i såväl Sekretessmeddelande för CareLink Personal, som i avtal med Regionerna angående CareLink System, saknas en kopia av standardavtalsklausulerna som används för överföring till tredje land samt en hänvisning till relevanta moduler. I denna del vill Medtronic understryka att det varken enligt Artikel 13–14, eller Artikel 28 GDPR krävs att standardavtalsklausulerna tillhandahålls på detta sätt. Inte heller finns något sådant krav i själva standardavtalsklausulerna.

5.4 Det sker ingen tredjelandsöverföring mellan vårdgivare och Medtronic AB när Medtronic AB agerar personuppgiftsbiträde till Regionerna inom ramen för CareLink System. Överföringen sker istället mellan Medtronic AB och dess underleverantör när ärenden hanteras för support.

5.5 Det är för Medtronic oklart vilka brister SKR Analysen vill peka på med ovanstående resonemang.

5.6 I enlighet med vad som gäller för registrerade enligt standardavtalsklausulerna och för de vårdgivare för vilka Medtronic AB agerar som personuppgiftsbiträde enligt Artikel 28 GDPR, finns en rätt att på begäran ta del av dessa klausuler.

6 AVSLUTANDE KOMMENTARER

6.1 Medtronic uppskattar möjligheten att på ett djupgående plan se över Medtronics regelefterlevnad inom ett område som är centralt för Medtronics kärnverksamhet. Regelefterlevnad är centralt för Medtronic, oaktat om det faller inom vårdgivarens eller Medtronics ansvar.

6.2 Medtronic noterar dock att SKR Analysen utgör en *laglighetsprövning* och att vad som i varje enskilt fall är *mest lämpligt* torde falla utanför ramen för bedömningen.

6.3 Medtronic kommer att överväga hur identifierade svagheter i Medtronics dataskyddsarbete kan åtgärdas och ser vid behov fram emot vidare diskussioner med SKR avseende hur eventuella risker som kan ha relevans för vårdgivarens personuppgiftsbehandling kan minimeras.

6.4 Även om rena lämplighetsbedömningar inte kan anses ha bäring på huruvida Medtronics produkter är lagliga eller inte är Medtronic självklart öppen för en vidare diskussion även i dessa frågor.

6.5 Medtronic har i de legala delarna av denna analys tagit hjälp av Wistrand Advokatbyrå i Stockholm.