PROMEMORIA

2022-03-31

Laglighetsprövning av FreeStyle Libre CGM-system med avseende på dataskydd och annat integritetsskydd

Sammanfattande bedömning av regelefterlevnad och risker

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

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

1 FreeStyle Libre CGM-system är en CE-märkt medicinteknisk och molntjänstbaserad produkt som utvecklas och tillhandahålls av det amerikanska företaget Abbott Diabetes Care, Inc (Abbott). FreeStyle Libre är ett sensorbaserat system för glukosmätning. FreeStyle Libre-sensor bärs på armen. Glukosnivån läses av med en särskild avläsare eller med en mobil enhet med hjälp av Abbotts LibreLink-app, t.ex. en mobiltelefon. Används LibreLink-appen sparas användarens mätvärden automatiskt i Abbotts molnbaserade LibreView datahanteringssystem tills vidare. Att använda LibreLink-appen som avläsare kräver alltså att användaren skapar ett LibreView-konto i Abbotts molnbaserade LibreView datahanteringssystem. Freestyle Libre-sensorn kan införskaffas av enskilda individer för att monitorera glukosvärden i blodet på egen hand eller under ansvar av en vårdgivare.

2 Vårdgivare har möjlighet att skapa konton i LibreView datahanteringssystemet i syfte att skapa en LibreView-klinik och dela information inom LibreView-kliniken. Det är Abbotts tjänst för vårdgivare som vill monitorera en patient eller ta del av data om glukosvärden för ändamålet hälso- och sjukvård eller egenvård avseende patienter med sjukdomen diabetes. En vårdgivare kan även skapa profiler över sina patienter och ladda ner glukosdata via direktåtkomst från en invånares LibreView-konto, med dennes godkännande. En vårdgivare kan också enbart använda LibreLinkUp-appen. En enskild person kan i sin LibreLink-app dela sina data med upp till 25 personer, både anhöriga och enskilda yrkesutövare inom hälso- och sjukvården, såvida dessa förfogar över en LibreLinkUp-app.

3 Avtalspart för Abbotts CGM-tjänster är Abbott Diabetes Care Inc. i USA (Abbott). Abbott anlitar leverantörerna Amazon Web Services (AWS) för drift av sina tjänster. Teknisk support m.m. tillhandahålls av Abbott själv från EU och USA. Drift av Abbotts data sker på Irland, men i vissa fall överförs personuppgifter till USA för ändamålen support (Abbott) samt kvalitets- och säkerhetsövervakning av medicintekniska produkter (myndigheter). Överföringen är reglerad i Abbots villkor för tjänsterna, både i villkoren för enskilda privata

användare respektive vårdgivare. Överföringarna bedöms utgöra en tillåten tredjelandsöverföring.

4 Abbott och AWS är emellertid amerikanska företag som, såvitt kan bedömas, enligt avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Abbotts och AWS avtal innehåller bl.a. ansvarsfriskrivningar för det fallet att de skulle tvingas av amerikansk myndighet eller domstol att lämna ut uppgifter enligt bl.a. FISA 702 eller Cloud Act. Det finns således en risk, trots föredömliga organisatoriska och tekniska åtgärder från Abbotts sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Abbott får dock betraktas som mycket låg med hänsyn till bolagets kärnverksamhet (diabetesmonitorering) samt att det irländska dotterbolaget Abbott Ltd. 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.

5 Abbotts avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver dock kompletteras med skriftliga instruktioner från vårdgivare till bolaget om en rätt att överföra personuppgifter dels till Abbott i USA för nödvändig support och underhåll, dels till tillsynsmyndighet i bl.a. USA för ändamålet kvalitets- och säkerhetsövervakning inom området medicintekniska produkter. Abbott kan i dessa fall inte stödja sig på artikel 49.1 i dataskyddsförordningen för överföringen av personuppgifter som en vårdgivare är personuppgiftsansvarig för eftersom kommissionens standardavtalsvillkor används som rättsligt stöd enligt artikel 46 och därmed exkluderar användning av undantagssituationerna för tredjelandsöverföring enligt artikel 49.1. Abbott har meddelat att bolaget inte ser några hinder för att lägga till berörda instruktioner i personuppgiftsbiträdesavtal med vårdgivare.

6 Den av Abbott valda juridiska lösningen för LibreView datahanteringssystemet bedöms ge upphov till otydliga ansvarsförhållanden för personuppgiftsbehandlingen när en vårdgivare inför en tidsbegränsad vårdepisod (distanssjukvård) antingen skapar ett LibreLink-konto åt en patient alternativt får direktåtkomst till en patients LibreLink-konto, som denne skapat själv. I det förstnämnda fallet är det oklart vem som är personuppgiftsansvarig för LibreLink-kontot efter avslutad vårdepisod. I det senare fallet är det också oklart om en vårdgivare får ett utsträckt personuppgiftsansvar för all glukosdata i kontot genom direktåtkomsten. En osäkerhetsfaktor i sammanhanget är den potentiell tekniska åtkomsten som innebär att uppgifterna i kontot anses som förvarade allmänna handlingar hos en offentlig vårdgivare. En annan osäkerhetsfaktor är om PDL förbjuder en vårdgivare att bereda sig direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Abbott) eller om lagen tillåter sådan direktåtkomst eftersom den ligger utanför PDL:s tillämpningsområde och inte alls är reglerad.

7 Rättsläget är således oklart. Genom tydligare information i avtalsvillkoren för enskilda användare respektive vårdgivare torde Abbott kunna reducera väsentligen de risker som föreligger för registrerade vid ett otydligt personuppgiftsansvar på beskrivet sätt. Det är inte

uteslutet att det finns ett visst ”spelrum” i brist på vägledning i lagstiftningen för både Abbott och vårdgivare att reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke och att använda sig av direktåtkomst. Abbott har meddelat att bolaget avser att förtydliga för enskilda användare och vårdgivare om Abbotts respektive vårdgivares personuppgiftsansvar vid distanssjukvård i integritetspolicys, personuppgiftsbiträdesavtal och användarvillkor. Abbott har vidare meddelat att bolaget överväger en framtida lösning som gör det möjligt för vårdgivare att genom API:er begära att få ta del av uppgifter från en enskild användares LibreLink-konto och överföra dem till vårdgivarens eget vårdinformationssystem, dvs. genom en fråga-svar-lösning.

8 Abbotts avtalsvillkor med vårdgivare, innebärande att en offentlig vårdgivare, t.ex. en region, ska anses ha överlåtit kontrollen, och därmed ägandeskapet, över patientuppgifter till Abbott, tillika personuppgiftsbiträde, när bolaget gör felsökningar, ger support, tillhandahåller tjänsten eller bedriver forskning (”research”), kan vara i strid med de grundläggande dataskyddsprinciperna i dataskyddsförordningen. Det är inte skäligt att en leverantör ger sig själv sådana långtgående anspråk på personuppgifter hos en personuppgiftsansvarig, varför avtalsvillkoren kan vara i strid med principen om korrekthet i artikel 5.1 a i dataskyddsförordningen. Det är helt enkelt inte branschpraxis eller sedvana att ett personuppgiftsbiträde gör anspråk på att vara personuppgiftsansvarig över en kunds personuppgifter eller data för nu nämnda ändamål. Abbott rekommenderas att se över avtalsvillkoren för vårdgivare.

9 Beträffande vårdgivares inloggning till sitt klinik-konto på LibreView datahanteringssystem lever Abbott upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Beträffande sedan en enskild persons inloggning till sitt konto på www.libreview.com lever Abbott också upp till kraven på stark autentisering. Beträffande slutligen LibreLink- respektive LibreLinkUp-apparna omfattas dessa förvisso inte av Socialstyrelsens föreskrifter. Något krav på stark autentisering i författning finns inte. Rekommendationen är dock att enskilds inloggning till hälsodata i apparna bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i LibreView datahanteringssystem ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter

10 Tredjepartstjänsten Google Analytics och Google reCAPTCHA innebär en risk för otillåten behandling av personuppgifter. Risken får betraktas som hög. Med beaktande av den senaste utvecklingen och de beslut som dataskyddsmyndigheterna har fattat och förväntas fatta inom en snar framtid i detta avseende, har Abbott meddelat att bolaget utvärderar och följer noggrant utvecklingen i samband med användningen av kakor och liknande verktyg i samband med apparna LibreLink och LibreLinkUp.

Innehållsförteckning

1 Bakgrund

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

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

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

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

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

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

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

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

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

- FreeStyle LibreLink-appen och LibreView 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 FreeStyle LibreLink-appen och LibreView datahanteringssystem.

1.10 FreeStyle Libre CGM-system är en CE-märkt medicinteknisk och molntjänstbaserad produkt som utvecklas och tillhandahålls av det amerikanska företaget Abbott Diabetes Care, Inc (Abbott). I Sverige representeras bolaget av Abbott Scandinavia AB. FreeStyle Libre är ett sensorbaserat system för glukosmätning. FreeStyle Libre är CE-märkt för två åldersgrupper av personer med diabetes, barn i åldern 4-17 år under övervakning av vuxen, och för vuxna. FreeStyle Libre-sensor bärs på armen. Glukosnivån läses av med en särskild avläsare eller med en mobil enhet med hjälp av Abbotts LibreLink-app, t.ex. en mobiltelefon. På avläsarens eller den mobila enhetens skärm visas den aktuella glukosnivån. Från avläsaren kan data föras över till mjukvara trådlöst eller via kabel och sparas. FreeStyle Libre-sensorn kan lagra mätvärden upp till åtta timmar och mätvärdena förs vid avläsning (”flash”) över till avläsaren som kan lagra data i upp till tre månader. Används LibreLink-appen sparas användarens mätvärden automatiskt i Abbotts molnbaserade LibreView datahanteringssystem tills vidare. Vid användning av LibreLink-appen skapas automatiskt ett LibreView-konto i Abbots molnbaserade LibreView datahanteringssystem. Användarens glukosdata laddas automatiskt upp till LibreView-kontot när den mobila enheten är ansluten till Wi-Fi eller har en mobil dataanslutning. Från och med version 3 av appen kommer dock en användare att kunna välja huruvida värden ska sparas i molnet eller lokalt i appen Vid längre tid än åtta timmar mellan två avläsningar förloras data motsvarande tiden som överstiger åtta timmar.

1.11 Vårdgivare har möjlighet att skapa konton i LibreView datahanteringssystemet i syfte att skapa en LibreView-klinik och dela information inom LibreView-kliniken (exempelvis med sjuksköterskor, läkare, terapeuter och nutritionister). Det är således Abbotts tjänst för vårdgivare som vill monitorera en patient eller ta del av data om glukosvärden för ändamålet hälso- och sjukvård eller egenvård avseende patienter med sjukdomen diabetes. En vårdgivare kan också, med patientens godkännande, skapa profiler för sina patienter och ladda upp glukosdata från patientens avläsare till sitt LibreView-konto. Yrkesutövare kan också bjuda in sina patienter att ansluta till vårdgivarens LibreView-konto för att dela sin glukosdata per distans, för patienter som laddar upp en avläsare till sitt LibreView-konto eller för de som använder LibreLink-appen. Patienter kan ansluta och dela sin glukosdata med upp till 50 LibreView-vårdkliniker via LibreView datahanteringssystem eller LibreLink-appen. Dessutom kan patienter som använder LibreLink-appen dela sin glukosinformation med upp till 20 anhöriga m.m. som använder LibreLinkUp-appen..

2 Uppdrag och frågeställningar

2.1 SKR har begärt en laglighetsprövning av FreeStyle LibreLink-appen och LibreView datahanteringssystem. Laglighetsprövningen är avgränsad till själva behandlingen och skyddet av personuppgifter i LibreLink-appen och inkluderar bl.a. eventuella

tredjepartsapplikationer, datahantering och lagring av personuppgifter. Uppdraget är att redovisa om personuppgiftsbehandlingen i produkten är förenlig med gällande rätt.

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

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

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

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

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

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

2.8 Granskade 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 tillämplig på LibreLink- respektive LibreLinkUp-apparna och LibreView datahanteringssystem?

4.1 Som redovisats är FreeStyle Libre CGM-system ett verktyg för patienter att kontinuerligt mäta glukoshalten i blodet. Sensorn är gratis för typ 1-diabetiker medan typ 2-diabetiker i normalfallet får inhandla sensorn på egen hand. FreeStyle Libre kan således köpas av konsumenter, tillika diabetiker, som ser ett värde i att monitorerar sin glukosvärden trots att de inte kvalificerar sig för produkten inom ramen för rådande regionala riktlinjer för subventionerade förbrukningsartiklar.

4.2 Vårdgivare har möjlighet att skapa konton i LibreView datahanteringssystemet i syfte att skapa en LibreView-klinik och dela information inom LibreView-kliniken (exempelvis med sjuksköterskor, läkare, terapeuter och nutritionister). Det är Abbotts tjänst för vårdgivare som vill monitorera en patient eller ta del av data om glukosvärden för ändamålet hälso- och sjukvård eller egenvård avseende patienter med sjukdomen diabetes. En vårdgivare kan även skapa LibreView-konton åt sina patienter samt bjuda in dem att skapa ett eget LibreView-konto och dela sina glukosdata med vårdgivaren. En vårdgivare kan också, med patientens godkännande, skapa profiler för sina patienter och ladda upp glukosdata från patientens avläsare till sitt LibreView-konto.

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

4.4 Ett CGM-system kan även förskrivas inom ramen för **egenvård**. Bestämmelser om egenvård finns i Socialstyrelsens föreskrifter (SOSFS 2009:6) om bedömningen av om en hälso- och sjukvårdsåtgärd kan utföras som egenvård. Med egenvård avses enligt

föreskrifterna en hälso- och sjukvårdsåtgärd som legitimerad hälso- och sjukvårdspersonal bedömt att en patient själv kan utföra. Av föreskrifterna framgår vidare att egenvård inte är hälso- och sjukvård enligt hälso- och sjukvårdslagen. Föreskrifterna ska tillämpas i samband med att en legitimerad yrkesutövare

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

4.5 Egenvård är således medicinska arbetsuppgifter som förskrivaren bedömt att patienten kan utföra själv eller av någon annan som ska bistå patienten. Vårdgivaren ansvarar enbart för egenvårdsbedömningen och uppföljningen av egenvårdsbeslutet – det är hälso- och sjukvård. PDL är tillämplig på en vårdgivares behandling av personuppgifter i den delen. Individens egen vård faller utanför PDL:s tillämpningsområde. Den personuppgiftsbehandlingen får betraktas som ett led i en verksamhet av rent privat natur. Dataskyddsförordningen är inte tillämplig på behandling av personuppgifter som är av rent privat natur (artikel 2.1 c dataskyddsförordningen). Leverantören av tjänsten är inte personuppgiftsansvarig. Se dock nedan avsnitt 4.7.

4.6 En annan form av självhjälp är **egenmonitorering**. Det finns idag ett stort utbud av konsumentprodukter, och CE-märkta medicintekniska produkter, som vänder sig till konsumenter med intresse för sin egen hälsa. Det rör sig om klockor och appar som låter konsumenter monitorera sin egen hälsa och livsstil över tid. Produkterna är som regel molntjänstbaserade och kräver att konsumenter ingår ett avtal och tecknar ett hälsokonto hos tillverkaren där data kan sparas och analyseras. FreeStyle Libre är en sådan produkt. 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. Insamlade uppgifter kan sedan lämnas ut till en vårdgivare. Hjälpmedelsanvändarens egenmonitorering är inte hälso- och sjukvård. Vårdgivarens behandling av mottagna personuppgifter är däremot hälso- och sjukvård.

5 Vem är personuppgiftsansvarig?

5.1 Av 2 kap. 6 § PDL följer att en vårdgivare, oavsett om den är offentlig eller privat, är personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. I

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

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 FreeStyle Libre för distanssjukvård samt för uppföljning av egenvård (egenmonitorering) är patientansvarig vårdgivare personuppgiftsansvarig. För all annan personuppgiftsbehandling är Abbott personuppgiftsansvarig, t.ex. för LibreLink-konton som enskilda individer skapar i LibreView datahanteringssystem i rollen som konsument. Personuppgiftsansvaret för vårdgivare respektive Abbott behandlas i avsnitt 15.

6 Rättslig grund och tillåtna ändamål för behandling av personuppgifter

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.[3]

6.2 Vårdgivares distanssjukvård av patient med stöd av ett LibreView-klinikkonto, LibreView datahanteringssystem eller LibreLinkUp-appen 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 en FreeStyle Libre-sensor åt en invånare för egenvård eller självhjälp konstituerar inte automatiskt ett personuppgiftsansvar för vårdgivaren för all behandling av personuppgifter i LibreLink-appen och LibreView datahanteringssystem. Däremot torde en vårdgivare anses som personuppgiftsansvarig för LibreView-konton 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.

6.3 Vid egenvård och självhjälp (egenmonitorering) genom hälsoappar m.m. utan inblandning av en vårdgivare samlar leverantören in och behandlar individens personuppgifter normalt med stöd av den rättsliga grunden ”avtal” (användarvillkor för tjänsten) för behandlingen av hälsorelaterade uppgifter (artikel 6.1 b i dataskyddsförordningen). Individen har rätt att när som helst säga upp avtalet, varvid uppgifter på ett hälsokonto hos leverantören ska raderas. Individen kan vidare begära dataportabilitet av uppgifter som denne själv tillfört hälsokontot till sig själv eller till en

[3] SOU 2017:66 s. 227.

annan personuppgiftsansvarig. Någon annan relevant rättslig grund i artikel 6.1 i dataskyddsförordningen för Abbotts *insamling* av enskilda användares personuppgifter för deras nyttjande av bolagets tjänster för glukosövervakning är inte tillämplig. Här bortses från rättsliga grunder för andra ändamål, såsom marknadsföring, kvalitets- och säkerhetsövervakning av medicintekniska produkter och forskning.

6.4 I en handling benämnd *Återkoppling till region*, daterad den 11 mars 2021 som upprättats av Abbott hävdas att bolaget behandlar invånares personuppgifter med stöd av de rättsliga grunderna ”uppgift av allmänt intresse” respektive ”rättslig förpliktelse” enligt artikel 6.1 i dataskyddsförordningen. Skälet för att använda den förstnämnda rättsliga grunden är enligt Abbott att invånaren mottar ersättning eller i annat fall är berättigade till offentlig finansiering för användning av Abbotts medicintekniska produkter. Emellertid bedriver inte Abbott offentligt finansierad verksamhet, vilket är en förutsättning för att kunna åberopa denna specifika rättsliga grund (se prop. 2017/18:105 s. 58).

6.5 Till stöd för den rättsliga grunden rättslig förpliktelse åberopar Abbott i den nämnda handlingen reglering av kvalitets- och säkerhetsövervakning av medicintekniska produkter, dvs. regulatoriska krav. Det får anses utgöra en relevant rättslig grund för insamling av personuppgifter för det specifika ändamålet. Det är emellertid inte helt klart vilka specifika personuppgifter som samlas in för det ändamålet. Abbott 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 Abbotts Diabetes Care tjänster. Det innebär att om en invånare säger upp sitt LibreView-konto, och därmed den rättsliga grunden för Abbotts insamling av personuppgifter för ändamålet egenmonitorering eller distanssjukvård, nämligen avtalet för tjänsten, får bolaget fortsättningsvis behandla vissa insamlade personuppgifter för ändamålet regulatoriska krav med stöd av den rättsliga grunden ”rättslig förpliktelse”.

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

6.7 I LibreLink-appen och LibreView datahanteringssystem behandlar Abbott i rollen som personuppgiftsansvarig enskilda konsumenters, dvs. enskilda privatpersoners användning av produkten utan inblandning av en vårdgivare, personuppgifter med stöd av det avtal (Allmänna villkor) som användaren tecknar i samband med öppnande av ett LibreLink-konto, vilket är korrekt. Det framgår av Abbotts personuppgiftspolicy för användare av LibreLink-appen och LibreView datahanteringssystem (november 2021). Av personuppgiftspolicyn framgår vidare att Abbott behandlar en konsuments

hälsorelaterade uppgifter, som ju utgör känsliga personuppgifter, med stöd av ett uttryckligt samtycke, som också inhämtas när användaren tecknar ett LibreLink-konto. Abbott har således säkerställt de rättsliga grunderna och villkoren för behandling av enskilda personers hälsorelaterade personuppgifter på ett korrekt sätt och fullgjort sin informationsskyldighet i dessa delar enligt dataskyddsförordningen.

6.8 Abbott inhämtar vidare ett uttryckligt samtycke för framtida forskning på en användares personuppgifter när denne tecknar ett LibreLink-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 informera registrerade om personuppgiftsbehandlingen (artikel 13 och 14). Integritet och konfidentialitet har också lyfts in i de grundläggande principerna.

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

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

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

8 Anlitande av personuppgiftsbiträden

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

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

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

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

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

8.6 Av dataskyddsförordningen framgår att när uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för

personuppgiftsbiträdet med avseende på den personuppgiftsansvarige (artikel 28.3). Sådana avtal brukar enligt svenskt språkbruk benämnas personuppgiftsbiträdesavtal.

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

8.8 I dataskyddsförordningen föreskrivs dessutom följande rörande avtalets innehåll.

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

- Avtalet ska till sitt innehåll säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt (artikel 28.3, led b).
- Det ska framgå av avtalet att personuppgiftsbiträdet ska vidta alla de tekniska och organisatoriska åtgärder som krävs enligt dataskyddsförordningen för att säkerställa en lämplig säkerhetsnivå (artikel 28.3 led c och artikel 32).

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

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

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

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

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

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

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

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

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

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

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

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

9 Skydd av personuppgifter

9.1 En allmän bestämmelse om den personuppgiftsansvariges ansvar för personuppgifter finns i artikel 24 i dataskyddsförordningen. Av den följer att den

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

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

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

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

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

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

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

10 Tredjelandsöverföring

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

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

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

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

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

personers grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke (f), eller om överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information (g).

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

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

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

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

10.10 Europeiska dataskyddsstyrelsen (EDPB) har publicerat rekommendationer om adekvata skyddsåtgärder för tredjelandsöverföring. Rekommendationerna är ett svar på EU-domstolens dom i Schrems II.[4] EDPB har vidare publicerat ett utkast till riktlinjer som klargör vad som utgör, och inte utgör, en överföring av personuppgifter till tredjeland.[5] 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

[4] 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.
[5] Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

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 FreeStyle LibreLink och LibreLinkUp samt LibreView datahanteringssystem

12.1 Abbott är leverantör av FreeStyle LibreLink-appen, LibreView datahanteringssystem och LibreLinkUp-appen. Freestyle Libre CGM-system är både en FDA-godkänd och CE-märkt produkt. Det dokumenterade användningsområdet är ett sensorbaserat system för glukosmätning. FreeStyle Libre är CE-märkt för två åldersgrupper av personer med diabetes, barn i åldern 4 -17 år under övervakning av vuxen, och för vuxna personer.

12.2 LibreLink-appen tillsammans med FreeStyle Libre 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 Abbotts LibreView datahanteringssystem.

12.3 Enligt Abbott har hela FreeStyle Libre-systemet byggts med säkerhet i åtanke.[6] Systemet använder Amazon Web Services (AWS) infrastruktur (se vidare avsnitt 13). Teknisk support tillhandahålls av Abbott. All data i LibreView datahanteringssystem är krypterad, både i vila och vid transport. Abbott använder ett distribuerat molnlagringssystem för att skydda mot dataförlust i händelse av en naturlig eller annan katastrofal händelse. Glukosdata förvaras separerad från privata användares kontouppgifter. Européers kundinformation lagras inom EU (Irland respektive Frankrike – i det senare fallet enbart franska användare) för bättre integritetsskydd. Abbott uppfyller vidare krav i HIPAA som bl.a. innefattar strikta åtkomstkontroller för Abbotts personal och fortlöpande säkerhetsutbildning för alla medarbetare.

12.4 FreeStyle Libre-sensorer överför personliga glukosvärden på ett säkert sätt till LibreLink-appar och avläsare med NFC-teknik (närfältskommunikation) och Bluetooth-teknik. NFC har en utökad skyddsnivå på så sätt att omedelbar fysisk närhet krävs. Krypterade Bluetooth-anslutningar för FreeStyle Libre-sensorer upprättas under NFC-kommunikation med en LibreLink-app eller avläsare.

12.5 Abbott framhåller att hela LibreView-plattformen har byggts med integritet i åtanke. EU-medborgare och medborgare inom ESS garanteras av Abbott en rätt att få utöva sina rättigheter enligt dataskyddsförordningen. Abbott garanterar även andra användare över hela världen samma rättigheter. Amazon betraktas av Abbott som en betrodd molntjänstleverantörer. Amazon har en serie av säkerhetscertifieringar inklusive:

- ISO 27001 Ledningssystem för informationssäkerhet
- PCI-överensstämmelse (nivå 1)

[6] Libre View Professional User EU/UK Data Processing Agreement September 2021.

- AICPA och SOC
- HIPAA

12.6 Abbott använder användaravtalet (EULA) som rättslig grund för behandling av personuppgifter för ändamålen 1) behandling av personuppgifter i tjänsten och 2) marknadsföring eller reklamkommunikation. Användare kan när som helst motsätta sig ändamål 2) genom att klicka på "avsluta prenumerationen" i Abbotts e-postuppdateringar.

12.7 FreeStyle LibreLink-appen sparar ovillkorligen användarens glukosvärden i molnet, dvs. i LibreView datahanteringssystem. En användare kan således inte begränsa överföring av data från appen till molnet. Från och med version 3 av appen kommer dock en användare att kunna välja huruvida värden ska sparas i molnet eller lokalt i appen. Abbotts avläsare sparar däremot inte glukosvärden i molnet utan enbart i läsaren. Användare som laddar upp data från avläsaren till sitt eget LibreView-konto, eller Vårdgivare som laddar upp data från avläsaren till sitt LibreView-klinikkonto, där data kan kopplas till en patientprofil eller laddas upp som en engångsrapport sparas tillfälligt i 24 timmar.

12.8 Inloggning i LibreLink-appen sker utan någon stark autentisering. Användares åtkomst till egen data i LibreView datahanteringssystem (www.libreview.com) som registrerats av appen sker dock med stark autentisering genom engångslösenord via sms eller e-post. Åtkomst kan än så länge inte ske med Bank-ID eller annat elektroniskt ID. Även vårdgivare loggar in på sitt klinik-konto i LibreView datahanteringssystem med stark autentisering. De kan dock inte nyttja SITHS-kort eller annat slag av e-legitimation. I LibreView-kontot, liksom i appen, kan en användare ta del av glukosvärden över tid såsom dagliga mönster, tid i målvärdesområde, medelvärde för glukos. I www.libreview.com kan användaren även skriva ut rapporter i pdf-format.

12.9 En användare kan dela sina glukosvärden med en vårdgivare via LibreLinkUp-appen. LibreLinkUp-appen är egentligen avsedd för en användare att kunna dela sina glukosvärden med andra personer. En enskild person kan i sin LibreLink-app dela sina data med upp till 25 personer, både anhöriga och enskilda yrkesutövare inom hälso- och sjukvården, såvida dessa förfogar över en LibreLinkUp-app. Tillgång till LibreLinkUp-appen förutsätter en inbjudan av en användare via LibreLink-appen. Samma användarvillkor och personuppgiftspolicy gäller för användare av LibreLinkUp-appen som för LibreLink appanvändare. En LibreLinkUp-användare måste teckna ett konto för att kunna nyttja appen.

12.10 Användare av Freestyle Libre-sensorn och LibreLink-appen kan även dela sina elektroniska glukosvärden med en vårdgivare som har ett LibreView klinik-konto i LibreView datahanteringssystemet och där skapat en patientprofil för användaren. Av Abbotts användarvillkor för vårdgivare framgår följande: “*The LibreView Data Management System allows patients with LibreView Data Management System accounts to share their glucose readings with you, and it also allows you to connect your patients' Meters, Readers and the FreeStyle App to your computer and upload their glucose*

readings into a patient profile that you have created."[7] Vårdgivares åtkomst till en invånares LibreView-konto sker genom s.k. direktåtkomst.

12.11 En vårdgivare kan därutöver enligt Abbotts användarvillkor för vårdgivare skapa ett LibreView-konto åt en patient.[8] Det är dock inte vårdgivaren som i sådana fall tilldelar patienten lösenord; det skapar patienten själv. En vårdgivare kan således både förskriva en FreeStyle Libre-sensor och skapa ett LibreView-konto för att få elektronisk tillgång till patientens glukosvärden. Enligt Abbott är vårdgivaren vid en direktåtkomst till respektive ett upprättande av patientkonto personuppgiftsansvarig för behandlingen av personuppgifter i LibreView-kontot, och Abbott hanterar personuppgifterna i rollen som personuppgiftsbiträde. Det framgår av Abbotts användarvillkor för vårdgivare: "*When your patient has created a LibreView Data Management System account and grants you access to that account, or where you set up a LibreView Data Management System account for your patient, Abbott (through the LibreView Data Management System) will be processing both your and your patient's personal data as a 'processor' on your behalf as a healthcare provider where you process your patient information to protect their vital interests as determined in your sole discretion as their healthcare provider*."[9]

12.12 Hur patienten ska förfara om denne vill använda FreeStyle Libre-sensorn efter avslutad distanssjukvård, t.ex. för egenvård eller för självhjälp, och vem som är personuppgiftsansvarig för genererade glukosdata efter avslutad sjukvård framgår inte av vare sig Abbots användarvillkor för vårdgivare, personuppgiftspolicy[10] för användare av LibreLink-appen respektive LibreLinkUp-appen eller annan tillhandahållen information från Abbott.

12.13 Abbott använder sig av kommissionens standardavtalsklausuler vid överföring av personuppgifter från EU till USA. Det innebär att Abbott åtar sig att respektera de rättigheter som EU-medborgare kommer i åtnjutande av enligt dataskyddsförordningen.

12.14 Av Abbotts personuppgiftspolicy[11] för användare av LibreLink-appen respektive LibreLinkUp-appen framgår att om användaren begär support av Abbott och delar sina felsökningsuppgifter (däribland hälsorelaterad information), överförs dessa uppgifter till USA i den mån det är nödvändigt för att bolaget ska kunna ge teknisk support och utföra bredare analys för att upptäcka systemproblem och den lokala supporten i Europa inte kan lösa frågan. Ansvarig för felsökning och annan support är Abbott i USA. Sådan överföring av användarens uppgifter till USA sker enligt Abbotts personuppgiftspolicy endast när det krävs, från fall till fall, och sker i enlighet med stöd av undantaget för tredjelandsöverföring i dataskyddsförordningen, artikel 49.1 b, eftersom överföringarna är begränsade till de som är nödvändiga för att bolaget ska kunna fullfölja sitt avtal med

[7] Libre View Professional User EU/UK Data Processing Agreement September 2021.
[8] Se Libre View Professional User EU/UK Data Processing Agreement September 2021: "When your patient has created a LibreView Data Management System account and grants you access to that account, or where you set up a LibreView Data Management System account for your patient, […].
[9] Libre View Professional User EU/UK Data Processing Agreement September 2021
[10] Abbotts sekretessmeddelande för användning av LibreView datahanteringssystem, november 2021.
[11] Abbotts sekretessmeddelande för användning av LibreView datahanteringssystem, november 2021.

användaren för tillhandahållandet av ett individuellt användarkonto i LibreView datahanteringssystem.

12.15 När en användare delar din personliga och hälsorelaterade information med en person som denne bjuder in att använda LibreLinkUp-appen, använder Abbott molntjänsten Firebase Cloud Messaging för att skicka underhålls- och avbrottsmeddelanden från LibreView-datahanteringssystemkonto till de personer som är anslutna till användaren via LibreLinkUp. Abbott informerar om att dessa meddelanden kan överföras via USA. Meddelandena är emellertid standardiserade underhålls- och avbrottsmeddelanden baserade på land och språk. Såvitt förstås överförs inga person- eller hälsorelaterade uppgifter till användarna av LibreLinkUp-konton.

12.16 När en användare loggar för första gången in på sitt konto i LibreView datahanteringssystem, efterfrågar tjänsten samtycke av användaren för att låta Abbott använda glukosdata utan koppling till användaren för ändamålet framtida forskning. Av informationen som lämnas i samband härmed samt av Abbotts personuppgiftspolicy för LibreLink- och LibreLinkUp-appanvändare[12] framgår att ”*avidentifierade, pseudonymiserade, sammanställda och/eller anonymiserade data [överförs] till USA, som inte identifierar dig med namn, i syfte att utföra forskning som beskrivs i avsnittet Forskning ovan.” Abbott framhåller i policyn att bolaget använder termerna ”avidentifiera” och ”pseudonymisera” som utbytbara.* Framställningen återkommer till frågan om forskning i avsnitt 15.

12.17 I Abbots användarvillkor för vårdgivare[13] framgår att bolaget äger en rätt att använda avidentifierade eller pseudonymiserade data som tillhör vårdgivaren för framtida forskning, liksom för utveckling av tjänsten: “*Abbott does not claim ownership of your personal data. […] Abbott may create, access, retain, use or disclose to third-party researchers, aggregated, anonymized, de-identified (or pseudonymized to the extent permitted by your law) data derived from the LibreView Data Management System for the purposes of research, to evaluate how the LibreView Data Management System is provided, to evaluate its use and its various components and equipment, to evaluate performance or impact on clinical staff or across clinics, to enhance the functioning of the LibreView Data Management System and the FreeStyle Libre sensors, to validate LibreView Data Management System upgrades, or for product development and quality and safety of medical devices. You agree that the license herein permits Abbott to take any such actions. Where personal information is provided to third-party suppliers to assist us with the provision of the LibreView Data Management System, they are required to keep personal information confidential and secure and may only use personal information to the minimum extent necessary*.”

12.18 Av personuppgiftspolicyn[14] framgår vidare att Abbott *”överför dina personuppgifter (i avidentifierat, pseudonymiserat, sammanställt och/eller anonymiserat format där det är möjligt) för att uppfylla våra juridiska skyldigheter”*. Med juridiska skyldigheter avses

[12] Abbotts sekretessmeddelande för användning av LibreView datahanteringssystem, november 2021.
[13] Libre View Professional User EU/UK Data Processing Agreement September 2021.
[14] Abbotts sekretessmeddelande för användning av LibreView datahanteringssystem, november 2021.

regulatoriska krav i USA krav avseende medicintekniska produkter, t.ex. avvikelser i produktens prestanda eller säkerhet. Abbott förklarar att överföringen av felsökningsdata (inklusive hälsorelaterade data) till USA sker med stöd av det specifika undantaget i dataskyddsförordningen, artikel 49.1 d, eftersom det är i allmänhetens intresse att Abbott uppfyller sina juridiska skyldigheter.

12.19 I personuppgiftspolicyn[15] erinrar Abbott tydligt användare av LibreLink-appen respektive LibreLinkUp-appen att USA inte förfogar över dataskydd- eller sekretessförfattningar som motsvarar dataskyddsförordningen och nationella integritetsbestämmelser inom EU/EES. Abbott framhåller emellertid att bolaget vidtar lämpliga avtalsmässiga, tekniska och organisatoriska skyddsåtgärder och kompletterande åtgärder för att skydda användarnas personuppgifter och att ytterligare skydd för att fortsätta att skydda personuppgifter kan tillkomma.

12.20 Av Abbotts personuppgiftspolicy[16] framgår att bolaget kan röja den information som samlas in från användare för att följa lagen, ett rättsligt förfarande, domstolsbeslut eller annan rättslig process i ett annat land än Sverige, t.ex. som svar på ett domstolsbeslut eller en stämning. Av policyn framgår vidare att Abbott som huvudregel informerar användare om rättsliga processer som söker tillgång till dennes information, såsom domstolsbeslut eller stämningar, såvida bolaget inte är förbjuden enligt lag att göra det.

12.21 Av Abbotts användarvillkor för vårdgivare[17] framgår att Abbott, såvida inte det är förbjudet enligt dataskyddsförordningens eller annan nationell reglering, informera skriftligen yrkesutövare så snart som det är praktiskt möjligt om ett rättsligt förfarande, domstolsbeslut eller annan rättslig process, som syftar till att få tillgång till eller röjande av personuppgifter som registrerats av yrkesutövare i LibreView datahanteringssystemet.

12.22 Personuppgiftsbiträdesavtalet som finns bilagt till användarvillkoren för vårdgivare[18] kompletteras av kommissionens standardavtalsklausuler[19] för tredjelandsöverföring, modul två-villkor (Personuppgiftsansvarig till personuppgiftsbiträde). Enligt punkt 15 a 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 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.

12.23 Enligt personuppgiftspolicyn för LibreLink- respektive LibreLinkUp-appanvändare använder Abbott kakor, som Google Analytics och Invisible reCAPTCHA. Dessa

[15] Abbotts sekretessmeddelande för användning av LibreView datahanteringssystem, november 2021.
[16] Abbotts sekretessmeddelande för användning av LibreView datahanteringssystem, november 2021.
[17] Libre View Professional User EU/UK Data Processing Agreement September 2021.
[18] Libre View Professional User EU/UK Data Processing Agreement September 2021
[19] Comission implementing decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

används för att hjälpa bolaget att förbättra sin service, prestanda, användarupplevelser samt för att känna igen botar. Enligt Abbott samlas följande information om användarna: domännamn, typ av webbläsare och operativsystem, IP-adress samt felsöknings- och analysdata. Abbot informerar om att bolaget kan kombinera denna automatiskt insamlade information med annan information som bolaget har om användaren. LibreView använder följande typer av cookies:

- Kakor som krävs för att Abbott ska kunna förvalta och säkerställa åtkomsten till LibreView datahanteringssystem och för att känna igen användaren när denne loggar in på sitt konto i datahanteringssystem.
- Funktions- och säkerhetskakor för att visa rätt datum och tid för användarens användarsessioner och för att hjälpa oss att skydda LibreViews integritet och hålla LibreView säkert.
- Kakor för att analysera LibreLink- och LibreLinkUp-appens prestanda. Abbott använder för detta syfte Google Analytics för att samla in prestandaövervakningsdata för apparna. Abbott menar att det sker i ett aggregerat och avidentifierat format. Prestandaövervakningsdata kan inkludera appversion, land, OS-nivå, enhet, radio- och operatörsinformation. Informationen innehåller inte Freestyle Libre-sensorns serienummer eller några andra personuppgifter, däribland hälsorelaterad information.

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

13 Tredjepartsapplikationer och tredjepartsleverantörer i Freestyle Libre CGM-system

13.1 Som redovisas i avsnitt 12 driftas Abbotts backend för LibreLink-appen, LibreView datahanteringssystem (wwwlibreview.com) och LibreLinkUp-appen av det amerikanska bolaget Amazon Web Service (AWS). Som många andra amerikanska leverantörer erbjuder AWS lagring av data i Europa. När det gäller support m.m. tillhandahålls det av Abbott från USA.

13.2 Som också redovisas i avsnitt 12 överför Abbott både användares och hälso- och sjukvårdspersonals personuppgifter till bl.a. USA för bl.a. ändamålen support, regulatoriska krav för medicintekniska produkter och framtida forskning. I huvudsak rör det sig om pseudonymiserade uppgifter. Vid support kan även individbaserade uppgifter överföras. Någon absolut garanti för att européers personuppgifter stannar i Europa ges inte av Abbott.

13.3 Abbott förklarar i sina användarvillkor för vårdgivare att bolaget stödjer sin tredjelandsöverföring till USA av personuppgifter om verksamhet och personal på kommissionens standardavtalsklausuler. Beträffande tredjelandsöverföring av invånares personuppgifter till USA stödjer sig Abbott på bestämmelserna om undantagssituationer i särskilda situationer i dataskyddsförordningen, artikel 49.

13.4 Lagring i AWS sker på det bolagets datacenter i Dublin, Irland. AWS agerar här i rollen som personuppgiftsbiträde åt Abbott. Av AWS integritetspolicy[20] framgår bl.a. under rubriken ”Location of Personal Information” följande: “*Amazon Web Services, Inc. is located in the United States, and our affiliated companies are located throughout the world. Depending on the scope of your interactions with AWS Offerings, your personal information may be stored in or accessed from multiple countries, including the United States. Whenever we transfer personal information to other jurisdictions, we will ensure that the information is transferred in accordance with this Privacy Notice and as permitted by applicable data protection laws*.”

13.5 I AWS kan kunden, dvs. Abbott, välja region där data ska tekniskt lagras.[21] AWS skriver: “*We will not move or replicate your content outside of your chosen AWS Region(s) without your consent, except in each case as necessary to comply with the law or a binding order of a governmental body*. AWS skriver vidare följande: “*We will not disclose customer content unless we're required to do so to comply with the law or a binding order of a government body. If a governmental body sends AWS a demand for customer content, we will attempt to redirect the governmental body to request that data directly from the customer. If compelled to disclose customer content to a government body, we will give customers reasonable notice of the demand to allow the customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so*.”

13.6 AWS informerar att tredjelandsöverföringen till USA inte sker med stöd av kommissionens beslut om skölden för privatlivet (Privacy Shield, se avsnitt 14). Under rubriken EU-US Privacy Shield anför AWS följande[22]: “*Since the Court of Justice of the European Union has validated the use of Standard Contractual Clauses (SCCs) as a mechanism for transferring data outside the European Union, our customers can continue to rely on the SCCs included in the AWS GDPR Data Processing Addendum if they choose to transfer their data outside the European Union in compliance with GDPR. The AWS GDPR Data Processing Addendum with Standard Contractual Clauses is part of the AWS Service Terms and is available automatically for all customers transferring personal data from the EU to any of the AWS regions around the world, including in the US*.”

13.7 Abbott tillämpar enligt egen uppgift en Hold-Your-Own-Key-lösning (HYOK).[23] Det innebär att patientuppgifter krypteras och dekrypteras av det irländska dotterbolaget Abbott Ltd. på Irland och att enbart dotterbolaget förfogar över krypteringsnyckeln. AWS lagrar således enbart krypterade uppgifter, vilka krypterats av Abbott. AWS förfogar inte själv över någon krypteringsnyckel eller andra medel för att få tillgång till vårdgivares patientuppgifter eller privata användares egeninsamlade personuppgifter i klartext.

[20] https://aws.amazon.com/privacy/
[21] https://aws.amazon.com/compliance/data-privacy-faq/?nc=sn&loc=4
[22] https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/
[23] Mejlkonversation med Abbott.

13.8 Abbott använder Google Analytics, Invisible reCAPTCHA samt inloggnings-, funktions- och säkerhetsprogramvaror i sina appar och på www.libreview.com, vilka kräver kakor. Enligt Abbott samlas följande information om användarna: domännamn, typ av webbläsare och operativsystem, IP-adress samt felsöknings- och analysdata. Såvitt kunnat utrönas ansvarar Abbott ensam för inloggnings-, funktions- och säkerhetskakorna. Överföring av personuppgifter till USA kan inte uteslutas. Invisible reCAPTCHA används för att förhindra åtkomst till konton av botar. Google Analytics används för att föra statistik över användningen av tjänsten. Tjänsterna tillhandahålls av en och samma amerikanska leverantörer, Google. Överföring av personuppgifter till USA eller till annat tredjeland via Abbotts underleverantör Google 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, 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 (Abbott 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[24]).

[24] 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.

- 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.

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

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

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

14.16 En lämplig skyddsåtgärd som står till buds är Kommissionens standardavtalsvillkor för tredjelandsöverföring i syfte att binda t.ex. leverantör att effektuera rättsmedel för registrerade motsvarande de som finns i dataskyddsförordningen. Sådana villkor är inbäddade i Abbotts avtalsvillkor för vårdgivare.[25] Amerikanska myndigheter är emellertid inte bundna av standardavtalsvillkoren, vilket innebär en risk för otillåten behandling i strid med dataskyddsförordningen om uppgifter hamnar i myndigheternas förvar. En annan teknisk skyddsåtgärd skulle vara krypterad överföring och teknisk lagring där myndigheten, dvs. den personuppgiftsansvarige enbart förfogar över krypteringsnyckeln och inte tjänsteleverantören.

14.17 Kommissionen har i juni 2021 presenterat nya standardavtalsklausuler. Kravet kvarstår dock enligt Schrems II-domen för att kunna använda standardavtalsklausulerna att det

[25] Libre View Professional User EU/UK Data Processing Agreement September 2021

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.[26]

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.

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

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.

15 Har personuppgifter i FreeStyle LibreLink och LibreLinkUp samt LibreView datahanteringssystem ett godtagbart skydd?

Bedömning: Avtalspart för Abbotts tjänster är Abbott Diabetes Care Inc. i USA (Abbott). Abbott anlitar leverantörerna AWS för drift av sina tjänster. Teknisk support m.m. tillhandahålls av Abbott själv från EU och USA. Drift av Abbotts data sker på Irland, men i vissa fall överförs personuppgifter till USA för ändamålen support (Abbott) samt kvalitets- och säkerhetsövervakning av medicintekniska produkter (myndigheter). Överföringen är reglerad i Abbots villkor för tjänsterna, både i villkoren för enskilda privata användare respektive vårdgivare. Överföringarna bedöms utgöra en tillåten tredjelandsöverföring.

Abbott och AWS är emellertid amerikanska företag som, såvitt kan bedömas, enligt avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Abbotts och AWS avtal innehåller bl.a. ansvarsfriskrivningar för det fallet att de skulle tvingas av amerikansk myndighet eller domstol att lämna ut uppgifter enligt bl.a. FISA 702 eller Cloud Act. Det finns således en risk, trots föredömliga organisatoriska och tekniska åtgärder från Abbotts sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Abbott får dock betraktas som mycket låg med hänsyn till bolagets kärnverksamhet (diabetesmonitorering) samt att det irländska dotterbolaget Abbott Ltd. 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.

Abbotts avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver kompletteras med skriftliga instruktion från vårdgivaren till bolaget om en rätt att överföra personuppgifter dels till Abbott i USA för nödvändig support och underhåll, dels till tillsynsmyndighet i bl.a. USA för ändamålet kvalitets- och säkerhetsövervakning

inom området medicintekniska produkter. Abbotts kan i dessa fall inte stödja sig på artikel 49.1 i dataskyddsförordningen för överföringen av personuppgifter som en vårdgivare är personuppgiftsansvarig för eftersom kommissionens standardavtalsvillkor används som rättsligt stöd enligt artikel 46 och därmed exkluderar användning av undantagssituationerna för överföring enligt artikel 49.1. Abbott har meddelat att bolaget inte ser några hinder för att lägga till berörda instruktioner i personuppgiftsbiträdesavtal med vårdgivare.

Den av Abbott valda juridiska lösningen för LibreView datahanteringssystemet ger upphov till otydliga ansvarsförhållanden för personuppgiftsbehandlingen när en vårdgivare inför en tidsbegränsad vårdepisod (distanssjukvård) antingen skapar ett LibreLink-konto åt en patient alternativt får direktåtkomst till en patients LibreLink-konto, som denne skapat själv. I det förstnämnda fallet är det oklart vem som är personuppgiftsansvarig för LibreLink-kontot efter avslutad vårdepisod. I det senare fallet är det också oklart om en vårdgivare får ett utsträckt personuppgiftsansvar för all glukosdata i kontot genom direktåtkomsten. En osäkerhetsfaktor i sammanhanget är om PDL förbjuder en vårdgivare att bereda sig direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Abbott) eller om lagen tillåter direktåtkomst eftersom den ligger utanför PDL:s tillämpningsområde. Rättsläget är alltså oklart. Genom tydligare information i avtalsvillkoren för enskilda användare respektive vårdgivare torde Abbott kunna reducera väsentligen de risker som föreligger för registrerade vid ett otydligt personuppgiftsansvar på beskrivet sätt. Det är inte uteslutet att det finns ett visst ”spelrum” i brist på vägledning i lagstiftningen för både Abbott och vårdgivare att reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke och att använda sig av direktåtkomst. Abbott har meddelat att bolaget avser att förtydliga för enskilda användare och vårdgivare om Abbotts respektive vårdgivares personuppgiftsansvar vid distanssjukvård i integritetspolicys, personuppgiftsbiträdesavtal och användarvillkor. Abbott har vidare meddelat att bolaget överväger en framtida lösning som gör det möjligt för vårdgivare att genom API:er begära att få ta del av uppgifter från en enskild användares LibreLink-konto och överföra dem till vårdgivarens eget vårdinformationssystem, dvs. genom en fråga-svar-lösning.

Abbotts avtalsvillkor med vårdgivare, innebärande att en offentlig vårdgivare, t.ex. en region, ska anses ha överlåtit kontrollen, och därmed ägandeskapet, över patientuppgifter till Abbott, tillika personuppgiftsbiträde, när bolaget gör felsökningar, ger support, tillhandahåller tjänsten eller bedriver forskning (”research”), kan vara i strid med de grundläggande dataskyddsprinciperna i dataskyddsförordningen. Det är inte skäligt att en leverantör ger sig själv sådana långtgående anspråk på personuppgifter hos en personuppgiftsansvarig, varför avtalsvillkoren kan vara i strid med principen om korrekthet i artikel 5.1 a i dataskyddsförordningen. Det är helt enkelt inte branschpraxis eller sedvana att ett personuppgiftsbiträde gör anspråk på att vara personuppgiftsansvarig över en kunds personuppgifter eller data för nu nämnda ändamål. Abbott rekommenderas att se över avtalsvillkoren för vårdgivare.

Beträffande vårdgivares inloggning till sitt klinik-konto på LibreView datahanteringssystem lever Abbott upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd. Beträffande sedan en enskild persons inloggning till sitt konto på www.libreview.com lever Abbott också upp till kraven på stark autentisering. Beträffande slutligen LibreLink- respektive LibreLinkUp-apparna omfattas dessa förvisso inte av Socialstyrelsens föreskrifter. Något krav på stark autentisering i författning finns inte. Rekommendationen är dock att enskilds inloggning till hälsodata i apparna bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i LibreView datahanteringssystem ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.

Tredjepartstjänsten Google Analytics och Google Invisible reCAPTCHA innebär en risk för otillåten behandling av personuppgifter. Risken får betraktas som hög. Med beaktande av den senaste utvecklingen och de beslut som dataskyddsmyndigheterna har fattat och förväntas fatta inom en snar framtid i detta avseende, har Abbott meddelat att bolaget utvärderar och följer noggrant utvecklingen i samband med användningen av kakor och liknande verktyg i samband med apparna LibreLink och LibreLinkUp

15.1 Föreliggande laglighetsprövningen av FreeStyle LibreLink och LibreLinkUp samt LibreView datahanteringssystem är enligt uppdrag avgränsad till själva behandlingen och skyddet av personuppgifter i apparna och tredjepartsapplikationer. Uppdraget är att redovisa om personuppgiftsbehandlingen i produkten är förenlig med gällande rätt.

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

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

15.4 Abbott är ett amerikansk bolag. Bolaget har ett fast verksamhetsställe i Sverige genom Abbott Scandinavia AB. Avtalspart för Abbotts tjänster är emellertid Abbott Diabetes

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

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

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

Tystnadsplikt

15.7 Personalen verksamma i Abbotts verksamhet i USA omfattas inte av en lagreglerad och straffsanktionerad tystnadsplikt enligt lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. Lagen gäller i praktiken bara för aktörer vars medarbetare är fysiskt verksamma i Sverige. Tystnadsplikt för bolagen och dess medarbetare måste i stället avtalsregleras. En sådan avtalad tystnadsplikt finns reglerad i både Abbots personuppgiftspolicy för användare av LibreLink-appen och LibreView, november 2021, och avtalsvillkoren med vårdgivare.[27] Några disciplinära eller andra sanktioner mot enskild medarbetare hos Abbott som bryter tystnadsplikten, t.ex. i form av löneavdrag, avskedande, vite eller skadestånd, verkar inte existera. Det innebär generellt sett ett svagare skydd än en lagstiftad, straffsanktionerad tystnadsplikt på individnivå som kan rendera böter eller fängelse.

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

15.9 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

[27] Libre View Professional User EU/UK Data Processing Agreement September 2021.

Irland för anställda hos molntjänstleverantörer som har verksamhet i det landet. I Sverige renderar brott mot en lagstadgad tystnadsplikt upp till ett års fängelse, vilket är ett lägre straff än den irländska straffpåföljden. Irland får därmed anses har ett fullgott skydd mot obehörigt röjande av personuppgifter hos personuppgiftsbiträden verksamma på Irland. I detta fall AWS personal på Irland.

Överföringar av personuppgifter till USA och andra länder

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

15.11 Beträffande först överföringen av enskilda användares personuppgifter till USA, dvs. enskilda personer som använder Freestyle Libre-sensorn, LibreLink-appen och LibreLinkUp-appen för eget bruk (självhjälp eller egenvård), sker en överföring om användaren begär support av Abbott och delar sina felsökningsuppgifter (däribland hälsorelaterad information) samt i den mån det är nödvändigt för att bolaget ska kunna ge teknisk support och utföra bredare analys för att upptäcka systemproblem. Ansvarig för felsökning och annan support är Abbott. i USA. Sådan överföring sker enligt Abbott i enlighet med stöd av undantaget för tredjelandsöverföring, artikel 49.1 b i dataskyddsförordningen, eftersom överföringarna är begränsade till de som är nödvändiga för att bolaget ska kunna fullfölja sitt avtal med användaren för tillhandahållandet av ett individuellt användarkonto i LibreView datahanteringssystem. De databaser som Abbott använder är konfigurerade för att övervaka och skicka säkerhetsvarningar vid överföringar av höga volymer data från LibreView datahanteringssystem. Data är även krypterade i vila och under överföring genom användning av krypteringsnycklar som hanteras på ett säkert sätt.

15.12 Abbott har vidare en lösning på plats som innebär att enskilda användares personuppgifter lagras i krypterad form i AWS:s servrar och databasapplikationer och att endast Abbott förfogar över krypteringsnyckeln, inte AWS. Enligt uppgift läser ett irländskt dotterbolag, Abbott, Ltd., in krypterade data lagrat hos AWS i dotterbolagets back-end system. Där dekrypteras den så att Abbotts applikationer kan utföra analyser och presentera resultat för respektive inloggad användare. All överföring av data är krypterad. All lagring och trafik mellan Abbott Ltd. och AWS sker således i krypterad form där Abbott, Ltd. dekrypterar respektive krypterar uppgifter i sitt back-end.

15.13 Artikel 49.1 b i dataskyddsförordningen får anses utgöra en legitim grund för tredjelandsöverföring av konsumentbaserade personuppgifter för avsett syfte. Överföring är dessutom enligt Abbotts villkor under konsumentens kontroll genom att denne ska godkänna överföringen. Från och med version 3 av LibreLink-appen kan också en

användare välja huruvida värden ska sparas i molnet eller tillfälligt i appen. Av Schrems II-domen framgår för övrigt att domen om ett underkännande av Privacy Shield inte på något sätt underkänner överföring av personuppgifter till tredjeland med stöd av de särskilda undantagen i artikel 49 i dataskyddsförordningen, vilken artikel är tillämplig om det saknas ett beslut om adekvata skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46).

15.14 Av personuppgiftspolicyn för enskilda användare framgår vidare att Abbott överför registrerades personuppgifter för att uppfylla bolagets juridiska skyldigheter. Med juridiska skyldigheter avses bl.a. regulatoriska krav i USA krav avseende medicintekniska produkter, t.ex. avvikelser i produktens prestanda eller säkerhet. Abbott förklarar att överföringen av felsökningsdata (inklusive hälsorelaterade data) till USA sker med stöd av det specifika undantaget i dataskyddsförordningen, artikel 49.1 d, eftersom det är i allmänhetens intresse att Abbott uppfyller sina juridiska skyldigheter.

15.15 De uppgifter som överförs i dessa sammanhang är pseudonymiserade personuppgifter, såsom ”Complaint ID”, serienummer på produkten, kön och ålder.[28]. Andra identifierare såsom namn eller e-mailadress har tagits bort innan sådan behandling och behandlas inte för dessa ändamål med ”undantag för enstaka fall där Abbott enligt lag är skyldig att ange namnet på den person som lämnat in en incidentrapport till Abbott.”[29] Överföringen av uppgifter för att efterleva regulatoriska krav inom området medicintekniska produkter avser således i huvudsak ”personuppgifter” enligt dataskyddsförordningen.

15.16 I artikel 49.1 d klargörs det att allmänintresset ska vara erkänt i EU-rätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av. Det aktuella allmänintresset måste alltså ha ett rättsligt stöd, ett stöd i tillämplig rättsordning. Den rättsliga grunden för behandlingen av personuppgifterna måste därmed vara någon av de som avses i artikel 6.1 c eller e i dataskyddsförordningen, dvs. en rättslig förpliktelse, en arbetsuppgift av allmänt intresse eller myndighetsutövning som har stöd i rättsordningen. Det krävs alltså inte att själva överföringen eller behandlingen i övrigt av personuppgifterna har rättsligt stöd utan att den rättsliga förpliktelse, arbetsuppgift eller myndighetsutövning som överföringen är nödvändig för har ett rättsligt stöd.

15.17 Det finns ingen anledning att betvivla Abbotts påstående att de omfattas i USA av regulatoriska krav som innefattar en skyldighet att rapportera personuppgifter till amerikanska myndigheter. I huvudsak rör det sig om pseudonymiserade uppgifter, vilket minskar betydligt risken för integritetsförluster för enskilda användare. I enstaka fall sker en överföring av individuppgifter. Förbudet för tredjelandsöverföring i artikel 48 i dataskyddsförordningen[30] bedöms inte vara tillämplig eftersom de skyldigheter rörande regulatoriska krav som Abbott åberopar följer av hemlandets lagstiftning och inte av

[28] Svar från Abbott till en region den 11 mars 2021.
[29] Svar från Abbott till en region den 11 mars 2021.
[30] Artikel 48: ”Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.”

domstolsbeslut eller beslut från myndigheter. Tredjelandsöverföringen får därmed anses tillåten.

15.18 Annorlunda förhåller det sig med Abbotts åberopande av artikel 49.1 c i dataskyddsförordningen i bolagets personuppgiftsbiträdesavtal[31] med vårdgivare. Abbott åberopar denna bestämmelse i dataskyddsförordningen för att överföra personuppgifter till USA i syfte att genomföra support, underhåll och uppdateringar av sina tjänster, om det är absolut nödvändigt, dvs. om supporten i Europa inte kan lösa frågan. Av artikel 49.1 c framgår att en tredjelandsöverföring är tillåten om överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse, dvs. ett avtal mellan vårdgivare (personuppgiftsansvarig) och annan juridisk person (Abbott).

15.19 Artikel 49.1 är emellertid bara tillämplig om det saknas ett beslut om adekvat skyddsnivå (artikel 45) eller lämpliga skyddsåtgärder (artikel 46). Vid avtalsslut med vårdgivare och som komplement till personuppgiftsbiträdesavtalet använder sig Abbott emellertid av kommissionens standardavtalsvillkor. Det är en skyddsåtgärd som är uttryckligen angiven i artikel 46. Abbott kan således inte stödja sig på någon av bestämmelserna i artikel 49.1 eftersom artikel 46 är ”aktiverad”. Därutöver gäller inte led c åtgärder som vidtas av offentliga myndigheter (i detta fall regioner) som ett led i utövandet av deras offentliga befogenheter (artikel 49.3 i dataskyddsförordningen). Därför är det aktuella villkoret i Abbotts avtalsvillkor för vårdgivare i strid med dataskyddsförordningen. I stället ska Abbotts utlämnande av kundens (vårdgivarens) personuppgifter, oavsett om det rör sig om patienter eller medarbetare, utformas som en instruktion från vårdgivaren att Abbott får överföra sådana uppgifter till USA för ändamålet support, underhåll och uppdateringar av tjänsterna. Det framgår av kommissionens standardavtalsvillkor, modul 3, punkt 8.1, som kompletterar Abbotts personuppgiftsbiträdesavtal med en vårdgivare. En sådan instruktion saknas i dagsläget. . Abbott har meddelat att bolaget inte ser några hinder för att lägga till berörda instruktioner i personuppgiftsbiträdesavtal med vårdgivare.

15.20 Abbott har vidare ha ett behov av att överföra personuppgifter tillhörande vårdgivaren i pseudonymiserad form till myndighet i USA på grund av regulatoriska krav. En tillverkare av medicintekniska produkter, såsom Abbott, har som regel ett ansvar för produktföljning som ska rapporteras till tillsynsmyndigheten, t.ex. incidenter med produkten. Det rör sig här om rapportering av personuppgifter i pseudonymiserad form. Villkoren för en sådan överföring regleras närmare i kommissionens standardavtalsvillkor, modul 2, punkt 8.8, som kompletterar Abbotts personuppgiftsbiträdesavtal med en vårdgivare.

[31] Libre View Professional User EU/UK Data Processing Agreement September 2021. EU/UK DPA, punkt 9: International transfers: LibreView Data Management System servers for the European Economic Area ("EEA") and the UK users are located in the EEA. Abbott is located in the United States of America, a third country for the purposes of GDPR. Professional User understands that for Abbott to provide customer support, maintenance and updates to the LibreView Data Management System ("Maintenance Services"), it will sometimes be necessary to transfer Personal Data, including via remote access into the LibreView servers, from the EEA to Abbott or its Subprocessors pursuant to GDPR Article 49(1)(c).

15.21 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.[32] 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.

15.22 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".

15.23 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 Abbott 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

[32] 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.

Abbotts avtalsvillkor om LibreView datahanteringssystem och att bolaget säkerställer att det finns en skriftlig instruktion från vårdgivaren till bolaget om att denna överföring får ske till tillsynsmyndighet i bl.a. USA för ändamålet regulatoriska krav inom produktsegmentet medicintekniska. En sådan instruktion saknas och behöver tillföras Abbotts avtalsvillkor.

15.24 Kommissionens standardavtalsvillkor för tredjelandsöverföring är en skyddsåtgärd i sig för tredjelandsöverföring i syfte att binda t.ex. leverantör att effektuera rättsmedel för registrerade motsvarande de som finns i dataskyddsförordningen. Sådana villkor är inbäddade i Abbotts avtalsvillkor för vårdgivare.[33] Som framhållits är amerikanska myndigheter emellertid inte bundna av standardavtalsvillkoren, vilket innebär en risk för otillåten behandling i strid med dataskyddsförordningen om uppgifter hamnar i myndigheternas förvar. Ytterligare skyddsåtgärder krävs för att förhindra det. Den Europeiska dataskyddsstyrelsen (EDPB) fastställde därför i juni 2021 rekommendationer för tredjelandsöverföring med anledning av Schrems II-domen.[34] EDPB anger i skäl 3 till rekommendationerna att ”… in the absence of an EU adequacy decision, a controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject”. Rekommendationen måste beaktas av både personuppgiftsansvariga och biträden.

15.25 En sådan teknisk skyddsåtgärd skulle vara krypterad överföring och teknisk lagring där myndigheten, dvs. den personuppgiftsansvarige enbart förfogar över krypteringsnyckeln och inte tjänsteleverantören. I bilaga 2 i de nämnda rekommendationerna från EDPB beskrivs olika fallsituationer avseende tredjelandsöverföring som bedöms som antingen tillåtna eller inte. Bl.a. ges exempel på ”adekvata skyddsåtgärder” för att kompensera bristen på ett kommisionsgodkännande eller en adekvat skyddsnivå för skyddet av personuppgifter i tredjeland som motsvarar dataskyddsförordningen. I fallsituation 1 beskrivs en situation där nycklarna enbart är under kontroll av dataexportören eller av en aktör som anlitas av dataexportören inom EU/EES. Vad som beskrivs är en s.k. Hold Your Own Key-lösning (HYOK). Abbott använder sig av en sådan lösning för utkontrakteringen av drift av glukosdata till AWS. Det är ett dotterbolag på Irland, Abbott Ltd., som i rollen som personuppgiftsbiträde åt Abbott, Inc, (och underbiträde åt svenska vårdgivare), enbart förfogar över en krypteringsnyckel för data som är krypterad hos AWS.

15.26 Abbott menar vidare att de personuppgifter som finns i LibreView datahanteringssystem inte 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 LibreView är relaterade till kunders glukosvärden. Abbott hävdar att bolaget aldrig har fått någon övervakningsbegäran från USA och förväntar sig inte heller att få någon sådan begäran i

[33] Libre View Professional User EU/UK Data Processing Agreement September 2021
[34] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021.

framtiden.[35] Abbott använder därtill end-to-end kryptering i syfte att skydda överföringar av data och kunddata.

15.27 Endast leverantörer av elektroniska kommunikationstjänster (electronic communication service providers) omfattas av övervakningsåtgärder som sker med stöd av Section 702 FISA, vilket inbegriper telekomoperatörer (telecommunication carriers), tjänsteleverantörer som tillhandahåller olika kommunikationstjänster (t.ex. tjänster för kommunikation över internet, ECS) och molntjänstleverantörer som tillhandhåller sådana tjänster ”till allmänheten” (remote computing services, RCS). Till skillnad från leverantörer av fjärrdatortjänster (RCS) behöver en ECS inte tillhandahålla tjänster till allmänheten; att ge eventuella användare – såsom företagets egna anställda – möjlighet att skicka eller ta emot kommunikation är tillräckligt.[36] Det går därför inte att utesluta att Abbott kan komma att omfattas av övervakningsprogram enligt Section 702 FISA på grund av att bolaget tillhandahåller tjänster ”till allmänheten”.

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

15.29 Det saknar i sammanhanget betydelse att Abbott åtar sig enligt avtal att ”challenge legally binding orders from any U.S. governmental agency that conflict with Abbott’s obligations”. Abbott har friskrivit sig från ansvar om att underrätta en vårdgivare om en begäran eller ett beslut från amerikansk myndighet eller domstol ”to the extend not prohibited by…any applicable law”, t.ex. amerikansk rätt. **Det finns således en kvarstående risk, trots föredömliga organisatoriska och tekniska åtgärder från Abbotts sida för en otillåten behandling av personuppgifter i bolagets tjänster. Risken att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Abbott får dock betraktas som mycket låg med hänsyn till bolagets kärnverksamhet (diabetesmonitorering) samt att Abbott 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.**

[35] Svar till en region den 11 mars 2021.
[36] Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, Prof. Stephen I. Vladeck, den 15 november 2021 till de tyska dataskyddsmyndigheterna (DSK). Se även amerikanska justitiedepartemenets PM, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, https://www.justice.gov/file/442111/download

Personuppgiftsansvaret i trepartsförhållandet vårdgivare, Abbott och enskild användare

15.30 Abbott har skapat en lösning som inte har en helt tydlig separation mellan behandlingen av enskildas hälsokonton och vårdgivares konton i LibreView datahanteringssystem. I avtalsvillkoren för vårdgivare[37] skriver Abbott bl.a. följande (mina understrykningar):

"*The LibreView Data Management System allows patients with LibreView Data Management System accounts to share their glucose readings with you, and it also allows you to connect your patients' Meters, Readers and the FreeStyle App to your computer and upload their glucose readings into a patient profile that you have created*."

"If you have patients who do not have a LibreView Data Management System account which would enable you to view their glucose readings, it also allows you to create a patient profile whereby you may connect your patients' Meters to your computer, upload their glucose readings into the patient profile that you created for them, and share that information with Abbott."

"Patient profiles: After you have created a LibreView Data Management System account, you will be permitted to create patient profiles. When creating a patient profile, you will be required to manually enter some personal information for example their name and date of birth. Within their patient profile, you will be able to manually upload their Meter readings to the LibreView Data Management System."

"Where your patient has independently created a LibreView Data Management System account, either for their own use or for the use of a child or other person for whom they provide care, Abbott will be the data controller and will comply with applicable local data protection and privacy laws."

"Notice. When your patient has created a LibreView Data Management System account and grants you access to that account, or where you set up a LibreView Data Management System account for your patient, Abbott (through the LibreView Data Management System) will be processing both your and your patient's personal data as a 'processor' on your behalf as a healthcare provider where you process your patient information to protect their vital interests as determined in your sole discretion as their healthcare provider."

"When it provides the LibreView Data Management System, Abbott processes the Personal Data of the following categories of Data Subjects as a Processor on behalf of Professional User:
a. Professional User's employees; and
b. Patients enrolled to the LibreView Data Management System by Professional User except where patients have separately registered for a LibreView account through the LibreView website."

[37] Libre View Professional User EU/UK Data Processing Agreement September 2021

15.31 I ett svar till en region[38] förtydligar Abbott när en vårdgivare är att anse som personuppgiftsansvariga för behandlingar av personuppgifter i LibreView datahanteringssystem:

- När en patient har skapat ett användarkonto i LibreView-systemet och ger vårdgivaren tillgång till användarkontot för att vårdgivaren ska kunna behandla personuppgifterna däri i syfte att ge vård.
- När vårdgivaren skapar ett konto för en patient.
- När vårdgivaren kopplar en patients mätare eller avläsare till LibreView-systemet i syfte att ge vård och patienten inte har ett eget användarkonto i LibreView-systemet.

15.32 I *konsumentläget* råder det ingen tvekan om att Abbott är personuppgiftsansvarig för behandlingen av den enskildes personuppgifter. Individen (konsumenten) har stor rådighet över sina data och kan t.ex. exportera data till en annan leverantör och/eller helt sonika be att Abbott raderar dem. I *patientläget* råder andra rättsliga förhållanden när vårdgivaren är personuppgiftsansvarig. Patientdatalagen är tillämplig. Patientens rådighet över sina data är mer begränsad.

15.33 Oklarheten i Abbotts lösning avser personuppgiftsansvaret i en situation när en vårdgivare upprättar ett LibreLink-konto åt en patient inom ramen för en tidsbegränsad vårdepisod, dvs. distanssjukvård i form av egenmonitorering. Den fråga som väcks är vem som är personuppgiftsansvarig för patientens konto och insamlade uppgifter efter att vårdepisoden har upphört. Om en patient nekas fortsatt förskrivning av gratis sensor och i stället införskaffar sådan själv, fortsätter han eller hon att använda samma konto. Är det då Abbott eller vårdgivaren som är personuppgiftsansvarig? Det har inte gått att utreda på ett tillfredsställande sätt baserat på Abbotts personuppgiftspolicy och avtalsvillkor för vårdgivare.

15.34 En annan oklarhet är vårdgivarens direktåtkomst till en enskild persons redan tidigare upprättade konto i rollen som konsument (självhjälp). För vilka personuppgifter i kontot blir vårdgivaren personuppgiftsansvarig för? Bara de data som samlas in och sparas av den registrerade via sensorn under vårdepisoden? Eller alla tidigare historiska data som den enskilde samlat in på egen hand inom ramen för självhjälp?

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

[38] Den 11 mars 2021.

15.36 Av 5 kap. 4 § PDL framgår förvisso att en vårdgivares ”utlämnande genom direktåtkomst” till personuppgifter är tillåten endast i den utsträckning som anges i lag eller förordning. Här rör det sig inte om ett utlämnande av personuppgifter utan om en *insamling* av personuppgifter av en vårdgivare från en enskild persons konto hos en annan aktör. Å andra sidan framgår det av 2 kap. 6 § PDL att vårdgivares personuppgiftsansvar omfattar även sådan behandling av personuppgifter som vårdgivaren, eller den myndighet i en region eller en kommun som är personuppgiftsansvarig, utför när vårdgivaren eller myndigheten genom direktåtkomst i ett enskilt fall *bereder sig tillgång till* personuppgifter om en patient hos en annan *vårdgivare eller annan myndighet i samma region eller kommun*.” Det väcker frågan om en vårdgivare därmed är förbjuden att bereda sig direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Abbott) eller om det är fritt fram eftersom direktåtkomsten ligger utanför PDL:s tillämpningsområde. Om en vårdgivare är förbjuden enligt PDL att bereda sig direktåtkomst till ett LibreLink-konto, kan vårdgivare inte heller med stöd av patientens samtycke få direktåtkomst till dennes personuppgifter i konto eftersom direktåtkomst är uttömmande reglerat i PDL. Genom en potentiell teknisk åtkomst blir vidare uppgifterna i kontot enligt svensk rätt att betrakta som inkomna och förvarade allmänna handlingar hos en myndighet, t.ex. en hälso- och sjukvårdsnämnd i en region (2 kap. 6 § tryckfrihetsförordningen).[39]

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

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

15.39 En form av elektroniskt informationsutbyte som är vanlig mellan myndigheter är fråga-svar-funktioner. Högsta förvaltningsdomstolen (HDF) har i den s.k. Lefi-onlinedomen (HFD 2015 ref. 61) ansett att gränsdragningen mellan vad som är direktåtkomst och annat utlämnande på medium för automatiserad behandling beror på om den aktuella uppgiften kan anses förvarad hos den mottagande myndigheten enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen. Avgörande är således om uppgiften är tillgänglig för

[39] 2 kap. 6 § tryckfrihetsförordningen: En upptagning som avses i 3 § anses förvarad hos en myndighet, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt.

myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. HFD:s dom kan tolkas så att den tekniska utformningen av en myndighets system för utlämnande av uppgifter kan bli avgörande för om utlämnandet ska anses som direktåtkomst eller som annat utlämnande på medium för automatiserad behandling. I domen fann HDF mottagande myndighets åtkomst till uppgifter hos den utlämnande myndigheten genom ett system som utformats med en fråga-svar-funktionalitet inte utgjorde direktåtkomst. På motsvarande sätt fungerar Inera AB:s tjänstekontrakt i de nationella tjänsterna som bolaget förvaltar, t.ex. i Nationell Patientöversikt (NPÖ).

15.40 Den av Abbott valda juridiska lösningen för LibreView datahanteringssystem ger upphov till otydliga ansvarsförhållanden för personuppgiftsbehandlingen när en vårdgivare inför en tidsbegränsad vårdepisod (distanssjukvård) skapar ett LibreLink-konto åt en patient samt får direktåtkomst till en enskild persons hälsokonto, som den enskilde skapat själv. I det förstnämnda fallet är det oklart vem som är personuppgiftsansvarig för LibreLink-kontot efter avslutad vårdepisod. I det senare fallet är det också oklart om en vårdgivare får ett utsträckt personuppgiftsansvar för all glukosdata i kontot genom direktåtkomsten. En osäkerhetsfaktor i sammanhanget är den potentiell tekniska åtkomsten som innebär att uppgifterna i kontot anses som förvarade allmänna handlingar hos en offentlig vårdgivare. En annan osäkerhetsfaktor är om PDL förbjuder en vårdgivare att bereda sig direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Abbott) eller om lagen tillåter sådan direktåtkomst eftersom den ligger utanför PDL:s tillämpningsområde och inte alls är reglerad.

15.41 Rättsläget är således oklart. Genom tydligare information i avtalsvillkoren för enskilda användare respektive vårdgivare torde Abbott kunna reducera väsentligen de risker som föreligger för registrerade vid ett otydligt personuppgiftsansvar på beskrivet sätt och att använda sig av direktåtkomst. Det är inte uteslutet att det finns ett visst ”spelrum” i brist på vägledning i lagstiftningen för både Abbott och vårdgivare att reglera personuppgiftsansvaret i de situationer som beskrivs i föregående stycke. Abbott har meddelat att bolaget avser att förtydliga för enskilda användare och vårdgivare om Abbotts respektive vårdgivares personuppgiftsansvar vid distanssjukvård i integritetspolicys, personuppgiftsbiträdesavtal och användarvillkor.

15.42 Andra alternativ, som ska betraktas som rekommendationer, är att vid distanssjukvård, dvs. hälso- och sjukvård per definition i hälso- och sjukvårdslagen, bara erbjuda avläsare vars data vårdgivare laddar upp till eget konto i LibreView datahanteringssystem och sedan delar via direktåtkomst till patienten och i övrigt avtalsmässigt avgränsa vårdgivares användning av LibreLink-appen och LibreLink-konto till egenvård inom ramen för ett egenvårdsbeslut, eller självhjälp, varvid användaren kan dela sina egenhändigt insamlade glukosvärden med en vårdgivare i LibreView datahanteringssystem för egenvårdsuppföljning genom s.k. ADB-utlämnande, inte genom direktåtkomst. Abbott har meddelat att bolaget överväger en framtida lösning som gör det möjligt för vårdgivare att genom API:er begära att få ta del av uppgifter från en enskild användares LibreLink-konto och överföra dem till vårdgivarens eget vårdinformationssystem, dvs. genom en fråga-svar-lösning.

Abbotts avtalsvillkor för vårdgivares användning av LibreView datahanteringssystem

15.43 Av Abbotts avtalsvillkor för vårdgivare[40] framgår bl.a. följande:

> *"Where Abbott uses identifiable patient data that you [vårdgivare] enter into the LibreView Data Management System for the purposes of improving treatment guidance for patients utilizing Abbott's Meters, system troubleshooting, system and/or customer support, research or reporting, or to comply with Abbott's legal obligations, including in relation to quality and safety of medical devices, Abbott will be the data controller and will comply with applicable local data protection and privacy laws;"*
>
> Och vidare:
>
> *"Abbott does not claim ownership of your [vårdgivare] personal data that you transmit or submit to the LibreView Data Management System. By disclosing your personal information to Abbott, you grant it a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish and translate such data for the purpose of providing you with the LibreView Data Management System. Abbott may create, access, retain, use or disclose to third-party researchers, aggregated, anonymized, de-identified (or pseudonymized to the extent permitted by your law) data derived from the LibreView Data Management System for the purposes of research, to evaluate how the LibreView Data Management System is provided, to evaluate its use and its various components and equipment, to evaluate performance or impact on clinical staff or across clinics, to enhance the functioning of the LibreView Data Management System and the FreeStyle Libre sensors, to validate LibreView Data Management System upgrades, or for product development and quality and safety of medical devices. You agree that the license herein permits Abbott to take any such actions. Where personal information is provided to third-party suppliers to assist us with the provision of the LibreView Data Management System, they are required to keep personal information confidential and secure and may only use personal information to the minimum extent necessary."*

15.44 Avtalsvillkoren för vårdgivares nyttjande av LibreView datahanteringssystem är långtgående till Abbotts fördel vad gäller användning av ”personal data”, om än i pseudonymiserad eller avidentifierad form. Det finns inga hinder rättsligt sett för Abbott att uppställa sådana långtgående villkor, men ur ett myndighetsperspektiv väcker det farhågor att en offentlig aktör såsom t.ex. en region avhänder sig kontrollen över sina personuppgifter i sådan omfattning. Det kan rubba tilliten till den offentliga förvaltningen. Utöver det väcker villkoren frågan vad som avses med ”personal data” – menas vårdgivarens medarbetares personuppgifter eller patientuppgifter? Det behöver tydliggöras i avtalsvillkoren.

[40] Libre View Professional User EU/UK Data Processing Agreement September 2021

15.45 I ett hänseende förfogar Abbott över patientdata – ”identifiable patient data” i rollen som personuppgiftsansvarig, om vårdgivaren använder bolagets tjänster för behandlingsrekommendationer, felsökning, support, forskning (”research”) samt kvalitets- och säkerhetskrav för medicintekniska produkter och andra rättsliga förpliktelser. De ändamål som Abbott emellertid åberopar till grund för att överta äganderätten till en vårdgivares patientuppgifter, för det måste rimligen vara innebörden av ett personuppgiftsansvar – att man faktiskt bestämmer över personuppgifter – är tveksamma. Felsökning och support utgör inte berättigade skäl för en offentlig vårdgivare att röja (lämna ut) patientuppgifter till en leverantör, än mindre för att tillhandahålla tjänsten. Däremot finns det berättigade skäl för en offentlig vårdgivare att medge eller godta leverantörens behov av patientuppgifter för att fullgöra en rättslig förpliktelse.

15.46 Abbotts avtalsvillkor med vårdgivare, innebärande att en offentlig vårdgivare, t.ex. en region, ska anses ha överlåtit kontrollen, och därmed ägandeskapet, över patientuppgifter till Abbott, tillika personuppgiftsbiträde, när bolaget gör felsökningar, ger support, tillhandahåller tjänsten eller bedriver forskning (”research”), kan vara i strid med de grundläggande dataskyddsprinciperna i dataskyddsförordningen. **Det är inte skäligt att en leverantör ger sig själv sådana långtgående anspråk på personuppgifter hos en personuppgiftsansvarig, varför avtalsvillkoren kan vara i strid med principen om korrekthet i artikel 5.1 a i dataskyddsförordningen**. Det är helt enkelt inte branschpraxis eller sedvana att ett personuppgiftsbiträde gör anspråk på att vara personuppgiftsansvarig över en kunds personuppgifter eller data för nu nämnda ändamål. Abbott rekommenderas att se över avtalsvillkoren för vårdgivare.

Enskild användares delning av data med andra via LibreLinkUp-appen

15.47 En enskild person kan i sin LibreLink-app dela sina data med upp till 20 personer, t.ex. anhöriga, såvida dessa förfogar över en LibreLinkUp-app. Det finns inga rättsliga hinder för en sådan datadelning med anhöriga inom ramen för en enskild användares nyttjande av ett hälsokonto i rollen som konsument och där Abbot är personuppgiftsansvarig. Beträffande delning med en vårdgivare genom LibreLinkUp-appen, se under rubriken *Personuppgiftsansvaret i trepartsförhållanden vårdgivare* i detta avsnitt.

Autentisering av användare

15.48 Inloggning i LibreLink-appen sker utan någon autentisering, bortsett från PIN-kod till den mobila enheten. Användares åtkomst till egen data i LibreView datahanteringssystem (www.libreview.com) som registrerats av appen sker dock med stark autentisering genom engångslösenord via sms eller e-post. Åtkomst kan än så länge inte ske med Bank-ID eller annat elektroniskt ID. Vårdgivare däremot loggar in på sitt klinik-konto i LibreView datahanteringssystem med stark autentisering. Det sker genom engångslösenord via sms eller e-post. De kan emellertid inte nyttja SITHS-kort eller annat slag av e-legitimation.

15.49 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.

15.50 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).

15.51 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”.

15.52 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.

15.53 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.

15.54 **Beträffande vårdgivares inloggning till sitt klinik-konto på LibreView datahanteringssystem lever Abbott upp till kravet på stark autentisering i Socialstyrelsens föreskrifter och allmänna råd.** Beträffande sedan en enskild persons inloggning till sitt konto på www.libreview.com lever Abbott också upp till kraven på stark autentisering. Beträffande slutligen LibreLink- respektive LibreLinkUp-apparna omfattas dessa förvisso inte av Socialstyrelsens föreskrifter. Något krav på stark autentisering i författning finns inte. **Rekommendationen är dock att enskilds inloggning till hälsodata i apparna bör ske med stark autentisering (tvåfaktorsautentisering) för att nå en adekvat skyddsnivå med hänsyn till arten av uppgifter i kontot. Om enskilda användare däremot ska medges direktåtkomst till vårdgivares data i LibreView datahanteringssystem ska apparna ha funktionalitet för stark autentisering; det följer av Socialstyrelsens föreskrifter.**

Forskning

15.55 Abbott inhämtar ett uttryckligt samtycke för forskning på en användares personuppgifter när denne tecknar ett LibreLink-konto. Det är ett frivilligt samtycke och inte ett villkor för att använda tjänsten.

15.56 Av Abbots personuppgiftspolicy[41] framgår att en enskild användare samtycker till att bolaget får använda användarens glukosdata för forskning. Policyn specificerar dock inte vad för slags forskning det rör sig om eller vilka som ska bedriva forskningen. Vad som framgår är att Abbott hävdar att bolaget enbart kommer att använda sig anonymiserade data och bara nyttja uppgifter om födelseår, nationalitet och produktanvändning, såsom användarens avläsning av sensorn, användarens avläsning av värden i appen, gränsvärden för individens glukosvärden m.m. Andra identifierare såsom namn eller e-mailadress har tagits bort innan sådan behandling och behandlas inte för framtida forskning. Det rör sig således om anonymiserade uppgifter.

15.57 Under avsnittet ”Forskning” i personuppgiftspolicyn för enskilda användare finns en länk till pågående forskningsstudier benämnd ” Scientific Research Projects”. Av handlingen framgår att Abbott bedriver tre forskningsstudier. Yttterligare kontaktuppgifter finns i handlingen för den som vill ha ytterligare information.

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

[41] Abbotts sekretessmeddelande för användning av LibreView datahanteringssystem, november 2021.

15.59 Av principen om ändamålsbegränsning i dataskyddsförordningen (artikel 5.1 b) framgår emellertid att all behandling av personuppgifter ska ha ett ändamål. Ändamål ska vara ”särskilda, uttryckligt angivna och berättigade”. Det kravet på ändamål gäller även behandling av personuppgifter för forskning. Det finns alltså inte utrymme i dataskyddsregelverket att skapa uppgiftssamlingar för framtida forskningsbehov eller framtida forskningsfrågor, inte ens med stöd av en enskilds samtycke eftersom samtycket inte kan ”släcka” de grundläggande dataskyddsprinciperna. Samma begränsningar råder för den som behandlar personuppgifter i syfte att skapa anonymiserade uppgifter för samma ändamål.

15.60 LibreView datahanteringssystem bedöms emellertid innefatta en tillåten personuppgiftsbehandling för ändamålet forskning såvida användaren väljer att samtycka till densamma. Av skäl 33 i dataskyddsförordningen framgår för övrigt en inskränkning vad gäller kravet på samtycke för forskning. Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för forskning, när vedertagna etiska standarder för forskning iakttas.

Kakor och tredjepartsaktörer

15.61 Abbott använder Google Analytics, Invisible reCAPTCHA samt inloggnings-, funktions- och säkerhetsprogramvaror i sina appar och på www.libreview.com, vilka kräver kakor. Enligt Abbott samlas följande information om användarna: domännamn, typ av webbläsare och operativsystem, IP-adress samt felsöknings- och analysdata. Såvitt kunnat utrönas ansvarar Abbott ensam för inloggnings-, funktions- och säkerhetskakorna. Kakorna bedöms som nödvändiga för tjänstens funktionalitet. Eventuella personuppgifter som överförs till USA via dessa kakor är Abbott mottagare av. Överföringen har stöd i artikel 49.1 b i dataskyddsförordningen.

15.62 reCAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) är en säkerhetsåtgärd som kontrollerar att användaren kan ange ett manuellt svar. En CAPTCHA skyddar användaren mot skräppost och lösenordskrytpering genom att den utför ett enkelt test som visar att du är en människa och inte en dator som försöker att komma åt ett lösenordsskyddat konto. Google Analytics används av Abbott för prestandaövervakning av LibreLink- och LibreLinkUp-apparna. Abbott menar att det sker i ett aggregerat och avidentifierat format. Prestandaövervakningsdata kan inkludera appversion, land, OS-nivå, enhet, radio- och operatörsinformation. Informationen innehåller inte Freestyle Libre-sensorns serienummer eller några andra personuppgifter, däribland hälsorelaterad information.

15.63 Överföring av personuppgifter till USA eller till annat tredjeland via Abbotts underleverantör Google kan dock inte uteslutas. Både Google Analytics och reCAPTCHA registrerar IP-nummer hos användare av appar. Via Google Analytics och reCAPTCHA kan Google sannolikt hänföra IP-nummer från en enskild privat användares LibreLink-app eller dator vid inloggning i LibreLink-konto i www.libreview.com till eventuellt Google-konto som användaren också använder.

Google kan därmed identifiera individen och rikta direktreklam om vårdrelaterade tjänster eftersom LibreLink-appen är en hälsoapp. Förutom att det inte är etiskt försvarbart för berörda personuppgiftsansvariga - vårdgivare – som vill använda Abbotts tjänster för diabetesvård så finns 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[42] 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 Google reCAPTCHA innebär därmed en risk för otillåten behandling av personuppgifter**. **Risken får betraktas som hög**.

15.64 Abbott har meddelat att bolaget till följd av nyligen fattade myndighetsbeslut noggrant utvärderar och följer utvecklingen när det gäller användningen av kakor och andra tredjepartsverktyg i samband med apparna LibreLink och LibreLinkUp.

På uppdrag av SKR

Manólis Nymark

[42] Datenschutzbehörde den 22 december 2021, D155.027, 2021-0.586.257.

Bilaga 1

1 Bakgrund

Den 2 februari 2022 mottog Abbott ett utkast till promemoria med titeln *Laglighetsprövning av FreeStyle Libre CGM-system* avseende dataskydd och annat integritetsskydd" ("**promemorian**"). Abbott och författaren till memot har därefter utväxlat kommentarer och uppdaterade versioner av promemorian samt kommentarer samt haft diskussion med författaren den 11 mars 2022.

Abbott noterar och uppskattar de ansträngningar som har vidtagits för att gå igenom och beskriva Abbotts tjänster avseende Freestyle Libre-systemet samt justeringar och förtydliganden som har gjorts efter diskussion och Abbotts kommentarer. Abbott vill i detta dokument dock lämna ett par övergripande kommentarer och synpunkter på innehållet i promemorian.

Kommentarerna nedan utgör Abbotts bedömningar och utgör inte rådgivning till annan.

2 Överföring av personuppgifter till USA

2.1 Bedömningar och/eller påståenden i promemorian (punkterna 3-4 i sammanfattningen)

> 3. Avtalspart för Abbotts CGM-tjänster är Abbott Diabetes Care Inc. i USA (Abbott). Abbott anlitar leverantörerna Amazon Web Services (AWS) för drift av sina tjänster. Teknisk support m.m. tillhandahålls av Abbott själv från EU och USA. Drift av Abbotts data sker på Irland, men i vissa fall överförs personuppgifter till USA för ändamålen support (Abbott) samt kvalitets- och säkerhetsövervakning av medicintekniska produkter (myndigheter). Överföringen är reglerad i Abbots villkor för tjänsterna, både i villkoren för enskilda privata användare respektive vårdgivare. Överföringarna bedöms utgöra en tillåten tredjelandsöverföring.
>
> 4. Abbott och AWS är emellertid amerikanska företag som, såvitt kan bedömas, enligt avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder om så påfordras av myndigheter och domstolar i dessa länder. Abbotts och AWS avtal innehåller bl.a. ansvarsfriskrivningar för det fallet att de skulle tvingas av amerikansk myndighet eller domstol att lämna ut uppgifter enligt bl.a. FISA 702 eller Cloud Act. Det finns således en risk, trots föredömliga organisatoriska och tekniska åtgärder från Abbotts sida, för en otillåten behandling av personuppgifter. Risken för att amerikanska myndigheter vill ta del av kunduppgifter förvarade hos Abbott får dock betraktas som mycket låg med hänsyn till bolagets kärnverksamhet (diabetesmonitorering) samt att det irländska dotterbolaget Abbott Ltd. 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.

2.2 Abbotts kommentar

Abbott delar bedömningen att överföringarna är att betrakta som tillåtna tredjelandsöverföringar och att risken för att amerikanska myndigheter vill ta del av Abbotts kunduppgifter kan betraktas som mycket låg.

Abbott har aldrig fått någon begäran från amerikanska myndigheter för nationell säkerhet (eng*: U.S. government national security agencies*) om åtkomst till personuppgifter som finns i LibreView datahanteringssystem och förväntar sig inte heller att få en sådan begäran. Avseende risken för en begäran enligt FISA 702 bör det noteras att FISA tillämpas på "*electronic communications service*

*provide*rs". Dessa inkluderar både "*providers of electronic communications services*" och "*providers of remote computing services*".

Abbott har inhämtat rådgivning från externa lokala legala experter som har kommit fram till att Abbott **varken** är att betrakta som en "*provider of electronic communications services*" i relation till LibreView **eller** en "*provider of remote computing services*". Detta beror på att LibreView inte underlättar någon form av kommunikation mellan individer. FISA 702 bör således inte kunna användas för begäran till Abbott avseende personuppgifter som behandlas i LibreView.

Personuppgifter som behandlas i LibreView datahanteringssystem är krypterade vid överföring och i vila, vilket ger ytterligare tekniska skyddsåtgärder så om någon särskild överföring av personuppgifter skulle bli uppsnappad av amerikanska nationella säkerhetsmyndigheter skulle uppgifterna vara oläsliga. Det enda sättet för en spionerande myndighet att läsa informationen som överförs skulle vara att bryta krypteringen eller att använda krypteringsnyckeln. Krypteringsnycklarna innehas endast av Abbott *på Irland*.

För mer information rörande denna bedömning, vänligen se Abbott Diabetes Care Freestyle Libre Data Transfer Assessment for Customers of LibreView ("**LibreView TIA**"). LibreView TIA är tillgänglig vid förfrågan.

Som närmare beskrivs i LibreView TIA kan tjänsterna som tillhandahålls av underbiträdet AWS på Irland vara föremål för ett föreläggande enligt Cloud Act. Det bör dock observeras att krypteringsnycklarna endast innehas av Abbott på Irland och således är personuppgifterna inte tillgängliga för AWS i okrypterad form. Dessutom skulle GDPR gälla för en sådan begäran enligt principen om internationell hövlighet (Eng. *the principle of international comity*) och varje sådan begäran skulle kunna överklagas i domstol av leverantören av elektroniska kommunikationstjänster. Både GDPR och Cloud Act ger möjlighet till rättslig prövning.

Slutligen kan det noteras att Schrems II-domen inte innehöll någon bedömning av huruvida Cloud Act är en sådan lagstiftning som, om ens tillämplig, skulle betraktas som "problematisk lagstiftning".

3 Uppdateringar av villkor

3.1 Bedömningar och/eller påståenden i promemorian (punkt 5 i sammanfattningen)

> 5. Abbotts avtalsvillkor och personuppgiftsbiträdesavtal med vårdgivare behöver dock kompletteras med skriftliga instruktion från vårdgivaren till bolaget om en rätt att överföra personuppgifter dels till Abbott i USA för nödvändig support och underhåll, dels till tillsynsmyndighet i bl.a. USA för ändamålet kvalitets- och säkerhetsövervakning inom området medicintekniska produkter. Abbott kan i dessa fall inte stödja sig på artikel 49.1 i dataskyddsförordningen för överföringen av personuppgifter som en vårdgivare är personuppgiftsansvarig för eftersom kommissionens standardavtalsvillkor används som rättsligt stöd enligt artikel 46 och därmed exkluderar användning av undantagssituationerna för tredjelandsöverföring enligt artikel 49.1. Abbott har meddelat att bolaget inte ser några hinder för att lägga till berörda instruktioner i personuppgiftsbiträdesavtal med vårdgivare.

3.2 Abbotts kommentar

Abbott erbjuder Sveriges Regioner och andra offentliga verksamheter i Sverige att ingå separata personuppgiftsbiträdesavtal baserat på SKR:s personuppgiftsbiträdesmall ("**SKR-mallen**"). Abbott ser inga problem med att lägga till den begärda tilläggsinformationen till instruktionerna i sådana personuppgiftsbiträdesavtal för att ytterligare förtydliga instruktionerna i detta avseende.

För tydlighetens skull bör det dock poängteras att Abbott inte delar bedömningen att användningen av kommissionens standardavtalsklausuler ("**SCCs**") som rättslig grund enligt artikel 46 i GDPR utesluter användningen av undantaget för tredjelandsöverföring enligt artikel 49 (1). Enligt Abbotts bedömning kan

man använda olika överföringsmekanismer för enskilda behandlingar. Eftersom de aktuella överföringarna är tillfälliga snarare än systematiska kan sådana överföringar legitimeras av undantaget enligt artikel 49.(1) i GPDR.

Abbott har dock gått med begäran från Professionella Användare att ingå SCCs som en del av Abbotts ansvar som personuppgiftsbiträde enligt artikel 28 i GDPR för att bistå sina personuppgiftsansvariga kunder.

4 Klargörande av roller samt direktåtkomst

4.1 Bedömningar och/eller påståenden i promemorian (punkt 6-7 i sammanfattningen)

6. Den av Abbott valda juridiska lösningen för LibreView datahanteringssystemet bedöms ge upphov till otydliga ansvarsförhållanden för personuppgiftsbehandlingen när en vårdgivare inför en tidsbegränsad vårdepisod (distanssjukvård) antingen skapar ett LibreLink-konto åt en patient alternativt får direktåtkomst till en patients LibreLink-konto, som denne skapat själv. I det förstnämnda fallet är det oklart vem som är personuppgiftsansvarig för LibreLink-kontot efter avslutad vårdepisod. I det senare fallet är det också oklart om en vårdgivare får ett utsträckt personuppgiftsansvar för all glukosdata i kontot genom direktåtkomsten. En osäkerhetsfaktor i sammanhanget är den potentiell tekniska åtkomsten som innebär att uppgifterna i kontot anses som förvarade allmänna handlingar hos en offentlig vårdgivare. En annan osäkerhetsfaktor är om PDL förbjuder en vårdgivare att bereda sig direktåtkomst till hälsorelaterade uppgifter hos en annan aktör (Abbott) eller om lagen tillåter sådan direktåtkomst eftersom den ligger utanför PDL:s tillämpningsområde och inte alls är reglerad.

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

Abbott har meddelat att bolaget avser att förtydliga för enskilda användare och vårdgivare om Abbotts respektive vårdgivares personuppgiftsansvar vid distanssjukvård i integritetspolicys, personuppgiftsbiträdesavtal och användarvillkor. Abbott har vidare meddelat att bolaget överväger en framtida lösning som gör det möjligt för vårdgivare att genom API:er begära att få ta del av uppgifter från en enskild användares LibreLink-konto och överföra dem till vårdgivarens eget vårdinformationssystem, dvs. genom en fråga-svar-lösning.

4.2 Abbotts kommentar

Abbott har noggrant utvärderat och inkluderat information om olika roller under användningen av LibreViews datahanteringssystem i sina användarvillkor och sekretessmeddelanden. Abbott välkomnar de diskussioner Abbott har haft i samband med denna promemoria och kommer att fortsätta arbetet med att förtydliga informationen och rollfördelningen i samband med tillhandahållande av LibreView i Sverige.

Ytterligare information om parternas roller och behandling kan också ingå i de instruktioner som överenskommes i personuppgiftsbiträdesavtalet baserat på SKR-mallen som erbjuds regionen och anda offentliga verksamheter i Sverige.

Abbott noterar att svenska lagstiftning inte har förutsett tjänster för distansmonitorering inom vården varför rättsläget i denna del är oklart och behöver förtydligas och uppdateras. I avvaktan på sådan uppdatering och klargörande önskar Abbott att komplettera promemorian med följande överväganden som Abbott gjort i denna fråga.

<u>Om roller och fördelning av personuppgiftsansvar</u>

En av de oklarheter som har identifierats är huruvida all data i ett LibreView-konto automatiskt omfattas av Professionella Användares personuppgiftsansvar i samband med att en enskild användare ger tillgång till sitt LibreView-konto inom ramen för vårdgivares tillhandahållande av hälso- och sjukvård enligt definitionen i den svenska hälso- och sjukvårdslagen. Abbott anser att det, mot bakgrund av uttalanden som gjorts i förarbetena till PDL i detta avseende (se Prop. 2007/08 s. 62), finns visst stöd för att en vårdgivare enbart är personuppgiftsansvarig för de personuppgifter som vårdpersonalen *faktiskt får tillgång till* i patientens LibreView-konto under den tid sådan tillgång ges inom ramen för bedrivande av hälso- och sjukvård. Detta innebär att man kan argumentera för att vårdgivaren inte automatiskt ska betraktas som personuppgiftsansvarig för alla uppgifter på patientens LibreView-konto eller eventuella uppgifter som läggs till i kontot efter upphörande av distanssjukvård eller annan hälso- och sjukvård som tillhandahålls av vårdgivaren eller när en användare på annat sätt väljer att avsluta sådan åtkomst.

Som påpekats i Användningsvillkoren för Sjukvårdspersonal ska LibreViews datahanteringssystem och LibreView-kontot inte användas för långtidslagring av information och vårdgivaren bör därför efter distanssjukvårdsperioden säkerställa att nödvändig information laddas ner och förvaras någon annanstans efter behov.

Efter en distanssjukvårdsperiod behöver vårdpersonalen inte längre ha tillgång till patientens LibreView-konto. Sådan åtkomst kan således avbrytas av patienten och vårdgivaren kommer inte längre att ha tillgång till patientens uppgifter. Uppgifterna i patientens LibreView-konto skulle sedan finnas kvar i kontot tills ytterligare åtgärder vidtas. Om patienten önskar fortsätta använda sitt konto efter att distanssjukvårdsvårdperioden har löpt ut kommer Abbott därefter att fortsätta att vara personuppgiftsansvarig för sådan behandling.

Om ett konto har varit inaktivt i mer än sex månader kan Abbott, som beskrivs närmare i användningsvillkoren och sekretessmeddelandet, radera det inaktiva kontot.

Om ytterligare information om en viss behandlingsåtgärd krävs diskuterar Abbott gärna detta ytterligare med respektive vårdgivare och kan även tillhandahålla ytterligare information om de behandlingar som diskuteras och de säkerhetsåtgärder som vidtagits i samband med efterlevnad av data- och integritetsskyddsregler. Det skulle även kunna förtydligas i den information som tillhandahålls av vårdgivaren före användningen av distanssjukvården eller annan åtkomst till uppgifter i patientens LibreView-konto, att Abbott är personuppgiftsansvarig för personuppgifterna i patientens LibreView-konto efter att distanssjukvård eller hälsovård har upphört.

Om direktåtkomst m.m.

Med hänsyn till den oro som framförts om att vårdgivaren har sk "direktåtkomst" till patientens personliga LibreView-konto under tiden för tillhandahållande av distanssjukvård eller annan sjukvård enligt definitionen i den svenska hälso- och sjukvårdslagen, skulle Abbott vilja förtydligaföljande. Abbott är en tjänsteleverantör och tillhandahåller LibreView-datahanteringssystemet till både sjukvårdspersonal ("**Professionella Användare**") och patienten. Abbotts tjänster används i denna specifika situation av patienten som ett verktyg för informationsdelning mellan Professionella Användare och patienten och informationen delas inte juridiskt sett mellan vare sig två vårdgivare eller mellan Abbott (en privat enhet) och en vårdgivare, vilken skulle omfattas av begränsningarna för direktåtkomst enligt PDL. Frågan som återstår blir därmed att avgöra om direktåtkomst mellan en patient och en vårdgivare är att anses som otillåten enligt PDL.

Även om rättsläget är oklart även i denna del anser Abbott att det finns argument som talar för att patientens delning av sin data direkt till sin vårdgivare inte ska omfattas av PDL innan sådan delning faktiskt skett. Dvs den data som patienten delar är innan sådan delning sker inte patientdata som omfattas av PDL. Det finns följaktligen enligt Abbotts bedömning ingen direkt tillgång/utlämnande av patientdata till externa mottagare som skulle falla under bestämmelserna om direktåtkomstbegränsningar i PDL och därför anses vara laglig/olaglig.

Abbott delar dock uppfattningen om att det vore bra om lagstiftaren i Sverige förtydligar detta i uppdateringar av lag eller föreskrift för att undvika dessa oklarheter och förenkla användningen av de produkter för distansmonitorering som Abbott och andra aktörer tillhandahåller. Förhoppningsvis kan en

sådan uppdatering ske åtminstone senast i samband med svensk implementering av den av EU föreslagna Dataakten, vilken enligt nuvarande version särskilt har som syfte att förstärka en användares rätt att dela med sig av sin data.

I avvaktan på klargörande eller uppdaterad lagstiftning i denna del finns, såsom ovan nämnts möjlighet att utveckla och använda ett partner-API som kan överföra uppgifter från LibreView till klinikens hälsoplattform, till exempel till patientjournalen (eng: *the patient journal or electronical medical record*). Abbott vill dock särskilt upplysa om att en sådan API-lösning kräver relativt omfattande insatser från aktuella vårdgivare samt Abbott, varvid en realistisk förväntansbild bör vara att en sådan lösning tar ca 2-3 år att få på plats.

Avslutningsvis vill Abbott nämna att om Professionella Användare, samtidigt som de tillhandahåller hälso- och sjukvård enligt hälso- och sjukvårdslagen, inte vill få tillgång till information via patientens LibreView-konto, är det möjligt för Professionella Användare att inte erbjuda patienterna ett sådan delningsalternativ, och istället endast dela uppgifter genom att ladda ner dem direkt från avläsaren till de Professionella Användarnas egen dator eller till ett tillfälligt konto i LibreViews datahanteringssystem där uppgifterna sparas temporärt i 24 timmar. Detta innebär dock att patienten inte kommer att kunna dela uppgifter på distans utan måste istället besöka de Professionella Användarna för att dela information.

5 Överlåtelse av kontroll över personuppgifter

5.1 Bedömningar och/eller påståenden i promemorian (punkt 8 i sammanfattningen)

> 8. Abbotts avtalsvillkor med vårdgivare, innebärande att en offentlig vårdgivare, t.ex. en region, ska anses ha överlåtit kontrollen, och därmed ägandeskapet, över patientuppgifter till Abbott, tillika personuppgiftsbiträde, när bolaget gör felsökningar, ger support, tillhandahåller tjänsten eller bedriver forskning ("research"), kan vara i strid med de grundläggande dataskyddsprinciperna i dataskyddsförordningen. Det är inte skäligt att en leverantör ger sig själv sådana långtgående anspråk på personuppgifter hos en personuppgiftsansvarig, varför avtalsvillkoren kan vara i strid med principen om korrekthet i artikel 5.1 a i dataskyddsförordningen. Det är helt enkelt inte branschpraxis eller sedvana att ett personuppgiftsbiträde gör anspråk på att vara personuppgiftsansvarig över en kunds personuppgifter eller data för nu nämnda ändamål. Abbott rekommenderas att se över avtalsvillkoren för vårdgivare.

5.2 Abbotts kommentar

Abbott delar inte bedömningen att avtalsvillkoren medför att vårdgivare ska anses ha överfört kontrollen i strid med bestämmelserna i GDPR eller avtalsvillkoren skulle vara i strid med grundläggande dataskyddsprinciperna i GDPR. Abbotts tjänster används av verksamheter i flertalet länder inom EU som också har att efterleva de grundläggande kraven och principerna i GDPR.

Abbott välkomnar dock förslag från användare om nödvändiga förtydliganden och påminner om möjligheten för offentliga verksamheter i Sverige att ingå separata personuppgiftsbiträdesavtal baserade på SKR-mallen .

Det anges även uttryckligen i avsnitt 14 i Användningsvillkor för Sjukvårdspersonal att Abbott inte gör något anspråk på äganderätt till personuppgifter som Professionella Användare överför eller skickar till LibreViews datahanteringssystem. Abbott är även transparant avseende den behandling som sker i forskningssyfte i sekretessmeddelandet som innehåller en länk med mer information om forskningsprojekten. Vänligen se: https://freestyleserver.com/Payloads/ifu/2020/q4/DOC43602-001_rev-A.pdf.

6 Begränsad användning av tredjepartstjänster

6.1 Bedömningar och/eller påståenden i promemorian (punkt 10 i sammanfattningen)

10. Tredjepartstjänsten Google Analytics och Google reCAPTCHA innebär en risk för otillåten behandling av personuppgifter. Risken får betraktas som hög. Med beaktande av den senaste utvecklingen och de beslut som dataskyddsmyndigheterna har fattat och förväntas fatta inom en snar framtid i detta avseende, har Abbott meddelat att bolaget utvärderar och följer noggrant utvecklingen i samband med användningen av kakor och liknande verktyg i samband med apparna LibreLink och LibreLinkUp

6.2 Abbotts kommentar

Abbott följer som ovan nämnts noga utvecklingen och besluten om användningen av Google Analytics. Abbott följer även noga den process som nu pågår inom EU för att fatta ett nytt kommissionsbeslut om godkänt ramverk för överföringar mellan EU respektive USA mot bakgrund av den nyligen annonserade överenskommelsen därom mellan EU och USA.

Eftersom Abbott lägger stor vikt vid integritet och efterlevnad av GDPR analyserar Abbott för närvarande trots detta även de senaste franska och österrikiska besluten och inväntar de ytterligare 99 besluten som väntas komma i detta avseende för att utvärdera användningen av Google Analytics-verktygen i samband med tillhandahållandet av datahanteringssystemet LibreView.

Som en del av att Abbott uppfyller sina lagstadgade skyldigheter måste Abbott övervaka appens prestanda. För sådan översyn är Google Analytics Crashlytics-verktyget nödvändigt för ändamålet. När det gäller andra Google Analytics-verktyg som inte krävs för ovanstående syfte, ska användningen av sådana verktyg konfigureras på ett sätt som säkerställer att sådana verktyg endast används efter ett giltigt medgivande från användaren.

reCAPTCHA-verktyget används också för säkerhetsändamål och samlar in mycket begränsade personuppgifter om en användare, om ens några. Vänligen notera att de pågående utredningarna rörande användningen av Google Analytics efter Schrems II-domen (dvs. de 101 Google Analytics-klagomålet från NOYB) inte omfattar någon granskning av reCAPTCHA-verktyget.

Addendum 2022-04-07: Abbott har implementerat TrustArc i LibreView, vilket gör att användare nu har möjlighet att hantera val av cookies och kan avvisa alla funktionella cookies, som Google Analytics.

7 Generell kommentar avseende refererade uttalanden från it-driftsutredningen

Abbott har noterat de uttalanden som gjorts i IT-driftsutredningen (SOU 2021:1) avseende tolkning av GDPR. Eftersom GDPR är en EU-förordning som ska tolkas enhetligt i hela unionen är det dock svårt att bedöma den rättsliga betydelsen och värdet av uttalanden relaterade till tolkningen av GDPR som görs i utredningar som IT-driftsutredningen.

Detta blir ännu svårare i synnerhet när sådana uttalanden gjordes i samband med outsourcing av drift och inte molntjänster samt inte har resulterat i några ytterligare åtgärder från den svenska lagstiftarens sida när det gäller nya eller föreslagna nya lagar med anknytning till sådana uttalanden. Abbott kommer naturligtvis att fortsätta att följa den rättsliga utvecklingen i detta avseende.