Sveriges Kommuner och Regioner

PROMEMORIA

2021-08-15

Laglighetsprövning av Zenicor 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.

1 Zenicor-EKG är en CE-märkt medicinteknisk och molntjänstbaserad produkt som utvecklas och tillhandahålls av det svenska företaget Zenicor Medical Systems AB (Zenicor). Zenicor-EKG kan mäta hjärtat elektriska aktivitet via två avledare. Zenicor-EKG kräver inte en surfplatta eller en smartphone. Den har en inbyggd kommunikationslösning för att skicka registrerade värden till Zenicors lagringslösning för att där göras tillgängliga för vårdgivare. Analys av data och detektering av avvikelser sker på Zenicors it-plattform. Zenicor-EKG marknadsförs bara mot vårdgivare.

2 Läkarsystemet är Zenicors tjänst för vårdgivare. Läkarsystemet innefattar lagring och behandling av insända EKG, analys-, process- och tolkningsstöd för snabbare och säkrare diagnostisering samt användargränssnitt för presentation av EKG för vårdgivare. Läkarsystemet är installerat på en central server tillsammans med EKG-databasen och går att nå från valfri internetansluten enhet utan föregående installation. Även Läkarsystemet är en CE-märkt medicinteknisk produkt.

3 Av de grundläggande dataskyddsprinciperna i dataskyddsförordningen framgår att den personuppgiftsansvarige bl.a. ska säkerställa att behandlade personuppgifter är korrekta och relevanta (artikel 5.1). Vidare ställs krav på att personuppgiftsansvariga alltid beaktar inbyggt dataskydd (Privacy by design) vid utformning av system och tjänster så att de är ”…utformade för ett effektivt genomförande av dataskyddsprinciper…” (artikel 25.1). Det finns inga sådana mekanismer eller något inbyggt skydd i apparaten Zenicor-EKG-2 som förhindrar en felaktig behandling av personuppgifter genom att en annan person än patienten använder apparaten. Risken för felaktig behandling av personuppgifter får emellertid betraktas som låg.

Innehållsförteckning

1 Bakgrund

1.1 Störningar i hjärtats elektriska styrsystem kan vara kontinuerliga, men även uppträda intermittent, med korta eller längre mellanrum mellan episoderna av oregelbunden hjärtrytm. Patienterna kan märka dessa störningar i hjärtrytmen som hjärtklappningar eller mindre ork. Symptomgivande förmaksflimmer är den vanligaste rubbningen i hjärtrytmen och förekommer hos ca 3 - 4 procent av befolkningen.[1] Ytterligare 3 procent av befolkningen har ett intermittent och tyst (asymptomatisk) förmaksflimmer som inte diagnostiserats eller givit symptom.[2]

1.2 Att registrera den elektriska aktiviteten från hjärtat i samband med rytmstörningar som varar kort tid och uppträder sällan är en utmaning för hälso- och sjukvården. Om en individ själv kan registrera den elektriska aktiviteten vid oregelbunden hjärtrytm är det en fördel. Av intresse för sådan registrering är de produkter som brukar benämnas tum-EKG eller hjärtmonitor, varav vissa riktar sig till konsumentmarknaden.

1.3 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 2014 ett kunskapsunderlag med en hälsoekonomisk utvärdering gällande primärpreventiv screening av förmaksflimmer med tum-EKG. 2016 publicerade myndigheten ett nytt kunskapsunderlag för samma produktsegment.

1.4 I november 2019 godkände TLV den första digitala produkten för behandling av astma inom ramen för subventionen för barn med okontrollerad astma.

1.5 Medicintekniska produktrådet (MTP-rådet) vid Sveriges Kommuner och Regioner (SKR), en samverkan mellan regionerna på det medicintekniska området, har beslutat att utvärdera ny teknik för egenmonitorering av förmaksflimmer. Rådet har begärt av TLV att göra en hälsoekonomisk värdering av ett antal produkter innan rådet ger en rekommendation till regionerna om val av produkt eller produkter. TLV gjorde 2020 en s.k. temaspaning inom hjärt- och kärlområdet, som gav uppslag till de produkter som MTP-rådet funnit intressanta att gå vidare med. Det handlar om produkter där en patient själv ska kunna registrera sitt EKG och överföra det till sin vårdgivare.

1.6 MTP-rådet har nominerat följande produkter för en hälsoekonomisk bedömning:
- Coala Heart Monitor Pro
- CardioMem CM 100 XT och PhysioMem PM 100
- KardiaMobile och KardiaPro
- Zenicor-EKG

[1] Socialstyrelsen och Statens beredning för medicinsk och social utvärdering, Screening för förmaksflimmer med tum-EKG i syfte att förebygga stroke, 2017.
[2] Tandvårds- och läkemedelsförmånsverket, Kunskapsunderlag - Hälsoekonomisk utvärdering gällande primärpreventiv screening av förmaksflimmer med tum-EK, 2016.

1.7 I TLV:s uppdrag ingår inte att granska frågor om dataskydd och andra integritetsfrågor. I stället utreds sådana frågor av MTP-rådet. I denna promemoria som upprättats på uppdrag av MTP-rådet utreds en av de nominerade produkterna, *Zenicor-EKG.*

1.8 *Zenicor-EKG* är en CE-märkt medicinteknisk och molntjänstbaserad produkt som utvecklas och tillhandahålls av det svenska företaget Zenicor Medical Systems AB (Zenicor). Zenicor-EKG kan mäta hjärtat elektriska aktivitet via två avledare. Zenicor-EKG kräver inte en surfplatta eller en smartphone. Den har en inbyggd kommunikationslösning baserad på mobilt nätverk (2/5G) för att skicka registrerade värden till Zenicor lagringslösning för att där göras tillgängliga för vårdgivare. Analys av data och detektering av avvikelser sker på Zenicors it-plattform. Zenicor-EKG marknadsförs bara mot vårdgivare. Patienten får ingen återkoppling från Zenicor-EKG och stödjer därmed inte egenvård. Alla EKG granskas enbart av vårdgivare via Läkarsystemet.

1.9 *Läkarsystemet* är Zenicors tjänst för vårdgivare. Som framhållits erbjuds Zenicor-EKG inte på konsumentmarknaden utan är en utpräglad tjänst för vårdgivare för att utreda patienter med kända eller misstänkta hjärtsjukdomar. Läkarsystemet innefattar lagring och behandling av insända EKG, analys-, process- och tolkningsstöd för snabbare och säkrare diagnostisering samt användargränssnitt för presentation av EKG för vårdgivare. Läkarsystemet är installerat på en central server tillsammans med EKG-databasen och går att nå från valfri internetansluten enhet utan föregående installation. Även Läkarsystemet är en CE-märkt medicinteknisk produkt.

2 Uppdrag och frågeställningar

2.1 MTP-rådet har begärt en laglighetsprövning av Zenicor-EKG. Laglighetsprövningen är avgränsad till själva behandlingen och skyddet av personuppgifter i Zenicor-EKG och Läkarsystemet 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 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.

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. Utlämnande av uppgift i en patientjournal inom och 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 Vilken registerförfattning är tillämplig på Zenicor-EKG respektive Läkarsystemet?

4.1 Som redovisats är Zenicor-EKG ett verktyg enbart för vårdgivare för att möjliggöra en enkel och effektiv diagnostisering av förmaksflimmer och andra hjärtarytmier. Zenicor tillhandahåller en komplett systemlösning optimerad för att hälso- och sjukvården ska kunna utföra utredningar där patienten under längre perioder, flera gånger dagligen, och vid symtom registrerar EKG och överför dem till Zenicors lagringslösning där EKG

presenteras för vårdgivare via internet. Läkarsystemet är Zenicors digitala tjänst för vårdgivare för att monitorera patienter och analysera EKG.

4.2 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 hjärtmonitorering 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.

4.3 Ett tum-EKG 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.

4.4 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 4.6.

4.5 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 konto hos tillverkaren där data kan sparas och analyseras.

4.6 Zenicor-EKG används varken för egenvård eller egenmonitorering. Produkten används enbart i enlighet med en ordination av läkare. Zenicor-EKG används således inom ramen för hälso- och sjukvård av en vårdgivare (distanssjukvård). PDL är tillämplig på behandlingen av personuppgifter i Zenicor-EKG och Läkarsystemet.

5 Vem är personuppgiftsansvarig?

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

5.2 Vid användning av Zenicor-EKG och Läkarsystemet för distanssjukvård är patientansvarig vårdgivare personuppgiftsansvarig. Vårdgivaren är även personuppgiftsansvarig för sina medarbetares konton i Läkarsystemet.

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 Zenicor-EKG och Läkarsystemet innefattar således en tillåten behandling enligt PDL, såvida behandlingen är nödvändig för ändamålet och de grundläggande dataskyddsprinciperna i dataskyddsförordningen beaktas (se avsnitt 7). Något samtycke krävs alltså inte av patienten för att en vårdgivare ska få behandla dennes personuppgifter inom ramen för distanssjukvård på det sätt som sker genom Zenicor-EKG och Läkarsystemet.

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, t.ex. en vårdgivare, 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

[3] SOU 2017:66 s. 227.

och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med förordningen. De åtgärder som vidtas ska ses över och uppdateras vid behov (artikel 24.1). Ett sätt för den personuppgiftsansvarige att visa att denne fullgör sina skyldigheter är att tillämpa godkända uppförandekoder eller godkända certifieringsmekanismer (artikel 24.3).

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

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

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, t.ex. en vårdgivare, 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 för tredjelandsöverföring. Rekommendationerna är ett svar på EU-domstolens dom i Schrems II.[4]

11 Sanktionsavgifter

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

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

12 Zenicor-EKG och Läkarsystemet

12.1 Zenicor är leverantör av apparaten Zenicor-EKG-2 och den digitala tjänsten Läkarsystemet (Zenicor-EKG Back-end System). Båda produkterna är CE-märkta medicintekniska produkter. De dokumenterade användningsområdena är sekundärpreventiv screening hos strokepatienter, primärpreventiv screening i riskgrupper, arytmiutredning på vuxna patienter med symtom och arytmiutredning på barnpatienter (0-18 år).

12.2 Zenicor-EKG tillåter patienter att mäta och registrera EKG när som helst och var som helst. Zenicor använder algoritmer för att analysera hjärtrytm. Analys av data och detektering av avvikelser sker i Zenicors it-plattform.

12.3 Enligt Zenicor har hela EKG-plattformen byggts med säkerhet i åtanke.[5] Plattformen bygger på Amazon Web Services (AWS) infrastrukturer (se vidare avsnitt 13). Vidare tillämpar Zenicor enligt egen uppgift en Hold-Your-Own-Key-lösning (HYOK).[6] Det innebär att patientuppgifter krypteras och dekrypteras av Zenicor och att enbart Zenicor förfogar över krypteringsnyckeln. AWS lagrar således enbart krypterade uppgifter, vilka krypterats av Zenicor på uppdrag av kunden. AWS förfogar inte själv över någon krypteringsnyckel eller andra medel för att få tillgång till vårdgivares patientuppgifter i klartext. I Zenicor-EKG back-end kopplas apparatens (Zenicor-EKG) serienummer till en patient.

[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] Technical Overview Zenicor EKG System.
[6] Mejlkonversation med Zenicor.

12.4 Apparaten Zenicor-EKG-2 lagrar således inga personuppgifter (namn, ID eller annan identifierbar information) och ger inte heller någon återkoppling till patient rörande mätningens resultat annat än en bekräftelse på att mätning genomförts respektive skickats till Zenicors it-plattform Läkarsystemet. Således kommuniceras ingen individrelaterad information till patient, och EKG-apparaten i sig innehåller ingen information som kan kopplas till en specifik patient. Någon autentisering sker dock inte av patienten när denne använder Zenicor-EKG. Patienten informeras om att apparaten är strikt personlig och får inte lånas ut till någon annan person.

12.5 Zenicor framhåller att deras tjänsteplattform har byggts med integritet i åtanke. Amazon betraktas av Zenicor som betrodd molntjänstleverantör. Amazon har en serie av säkerhetscertifieringar inklusive:

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

12.6 Data i AWS lagras i Frankfurt, Tyskland. Observera att Zenicor inte tillhandahåller någon inloggning eller tjänst till patienter (se figur 1). Enbart vårdgivare förfogar över en webbtjänst för att ta del av mätvärden för specifika patienter. En användare av Läkarsystemet måste ha ett konto.

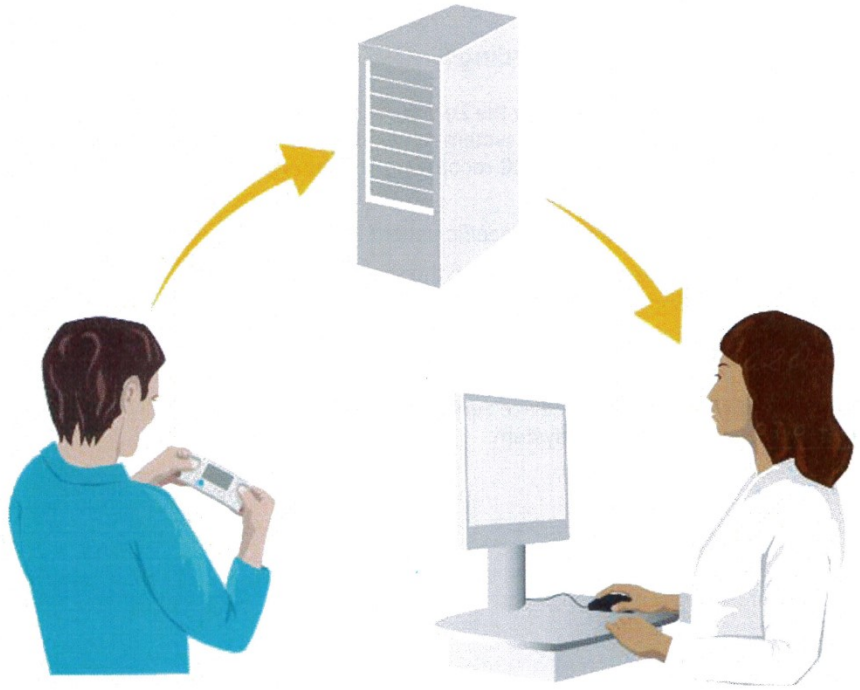

Fig. 1. Dataflöden mellan Zenicor-EKG och Läkarsystemet..

12.7 Av Zenicors integritetspolicy framgår att bolaget behandlar personuppgifter enbart inom EU/EES. I de fall som personuppgifter behandlas utanför EU/EES säkerhetsställer

Zenicor att anlitade leverantörer lever upp till samma säkerhetsskyddsnivå som tillämpas i EU/EES.[7]

12.8 Enligt uppgift använder Zenicor s.k. sessionskakor för att hålla inloggningsinformation om vårdgivares medarbetare så länge som användaren är inloggad. Kakan tas bort vid utloggning och således finns ingen kaka kvar i användarens dator efter utloggning.

12.9 Invånare erbjuds ingen inloggning till Zenicors it-tjänster. Endast vårdgivare har behörighet till Zenicors EKG Back-end (Läkarsystemet). Varje vårdgivare avgör själva nivå på autentisering. Enfaktorsautentisering (användarnamn och lösenord) är baslösningen. Zenicor rekommenderar dock alla kunder att använda sig av någon av de tvåfaktorlösningar som bolaget erbjuder. Tvåfaktorsautentisering erbjuds i dagsläget i form av Yubikey, SITHS och/eller TOTP. Zenicor kan på uppdrag av vårdgivare ställa in att tvåfaktorsautentisering blir tvingande på varje anslutet användarkonto tillhörigt vårdgivaren. Zenicors egen personal identifierar sig alltid med tvåfaktorsautentisering i egen it-plattform.

12.10 Vårdgivare ansvarar själva för att dokumentera väsentliga iakttagelser och fynd i eget vårdinformationssystem. Läkarsystemet erbjuder utskrift av pdf-rapporter som kan skrivas ut eller laddas ner av vårdgivaren för att sparas i dedikerat system.

13 Tredjepartsapplikationer och tredjepartsleverantörer i Zenicor-EKG

13.1 Som redovisas i avsnitt 12 anlitar Zenicor den amerikanska underleverantören AWS för infrastrukturen till EKG-databasen. Zenicor monitorerar, underhåller och uppdaterar databasen. Som många andra amerikanska leverantörer erbjuder AWS lagring av data i Europa.

13.2 Lagring i AWS sker på bolagets datacenter i Frankfurt, Tyskland. Av AWS integritetspolicy[8] 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*.”

13.3 I AWS kan kunden, dvs. Zenicor, välja region där data ska tekniskt lagras.[9] 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*

[7] Integritetspolicy (MM149) och Specifikation över behandling av personuppgifter (avtalsbilaga i Zenicors kundavtal).
[8] https://aws.amazon.com/privacy/
[9] https://aws.amazon.com/compliance/data-privacy-faq/?nc=sn&loc=4

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

13.4 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[10]: "*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*."

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 (Zenicor 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

[10] https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/

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 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 vårdgivare, 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 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.

14.8 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.

14.9 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.

14.10 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[11]).

[11] 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.

14.11 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.

14.12 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.

14.13 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).

14.14 Standardavtalsklausuler är en lämplig skyddsåtgärd som kan läggas till grund för överföring av personuppgifter till tredjeland om det i mottagarens land finns ett grundläggande rättighetsskydd och en möjlighet att göra detta skydd gällande inför domstol eller annan oberoende instans. EU-domstolens konstateranden i målet mellan Facebook Ireland och Schrems avseende rättsläget i USA vad gäller inskränkningar av grundläggande rättigheter och tillgången till effektiva rättsmedel och oberoende prövning (Schrems II) äger enligt it-driftsutredningen giltighet även i förhållande till övriga grunder för överföring av personuppgifter till USA enligt dataskyddsförordningen, eftersom kravet på skyddsnivå är detsamma oavsett vilken grund för överföringen som tillämpas (s. 228 f.). Utredningen har mot denna bakgrund svårt att se att det i en situation som gäller tredjelandsöverföring vid utkontraktering av it-drift finns några ytterligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen i Schrems II bedömer finns i amerikansk lagstiftning. En sådan åtgärd dock skulle vara krypterad överföring och teknisk lagring där myndigheten enbart förfogar över krypteringsnyckeln.[12]

[12] Se EDPB:s rekommendationer om tredjelandsöverföring, bilaga 2, Användarfall nr 1.

14.15 Kommissionen har i juni presenterat nya standardavtalsklausuler. Kravet kvarstår dock för att kunna använda standardavtalsklausulerna att det tredjelandet ska ha en adekvat skyddsnivå i lagstiftningen som motsvarar dataskyddsförordningen och som omfattar landets myndigheter samt effektiva rättsmedel för EU-medborgare att utöva medborgerliga rättigheter.

14.16 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.

14.17 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 artikel 48. 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.[13]

14.18 Den personuppgiftsansvarige har enligt it-driftsutredningen 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.

14.19 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

14.20 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.

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

14.21 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 uppgifterna i Zenicor-EKG och Läkarsystemet ett godtagbart skydd?

Bedömning: Av de grundläggande dataskyddsprinciperna i dataskyddsförordningen framgår att den personuppgiftsansvarige bl.a. ska säkerställa att behandlade personuppgifter är korrekta och relevanta (artikel 5.1). Vidare ställs krav på att personuppgiftsansvariga alltid beaktar inbyggt dataskydd (Privacy by design) vid utformning av system och tjänster så att de är ”…utformade för ett effektivt genomförande av dataskyddsprinciper…” (artikel 25.1). Det finns inga sådana mekanismer eller något inbyggt skydd i apparaten Zenicor-EKG-2 som förhindrar en felaktig behandling av personuppgifter genom att en annan person än patienten använder apparaten. Risken för felaktig behandling av personuppgifter får emellertid betraktas som låg.

15.1 Föreliggande laglighetsprövningen av Zenicor-EKG och Läkarsystemet är enligt uppdrag avgränsad till själva behandlingen och skyddet av personuppgifter i produkterna och tredjepartsapplikationer. Uppdraget är att redovisa om personuppgiftsbehandlingen i produkterna är förenlig med gällande rätt.

15.2 Som konstaterats har vårdgivare en rätt att behandla personuppgifter, inklusive känsliga sådana, för distanssjukvård, 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 Det erinras att vad gäller bestämmelserna om tredjelandsöverföring ska de beaktas av både personuppgiftsansvariga och personuppgiftsbiträden.

15.5 Zenicor är ett svenskt bolag. Zenicor anlitar underleverantören AWS för applikationsförvaltning och lagring av hälsorelaterade personuppgifter. Lagring av data sker i Tyskland. Lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter är tillämplig på Zenicors medarbetare. De omfattas således av en straffsanktionerad tystnadsplikt. Lagen ger således ett godtagbart skydd för enskildas hälsorelaterade personuppgifter, om något av bolagen hanterar personuppgifter. Däremot är lagen om tystnadsplikt för tjänsteleverantörer inte tillämplig på AWS medarbetare utomlands och dess utländska underleverantörer eftersom data förvaltas i annat land än Sverige.

15.6 AWS är ett amerikanskt företag som, såvitt kan bedömas, enligt egna källor och avtalsvillkor inte utesluter att de kan behöva överföra personuppgifter till USA och andra tredje länder och med ansvarsfriskrivningar för utlämnanden av uppgifter enligt bl.a. Cloud Act (se avsnitt 13 och 14). Kommissionens nya standardavtalsvillkor ”släcker” inte på något sätt en sådant brott mot bestämmelserna om tredjelandsöverföring eftersom USA enligt EU-domstolen saknar en adekvat skyddsnivå och effektiva rättsmedel för EU-medborgare vad gäller behandlingen av deras personuppgifter hos amerikanska myndigheter. Även it-driftsutredningen har bedömt att kommissionens tidigare standardavtalsklausuler inte ”släcker” de brister på adekvat skyddsnivå för EU-medborgares personuppgifter och avsaknaden av effektiva rättsmedel och transparens i USA (se avsnitt 14).

15.7 Zenicor har emellertid en lösning på plats som innebär att patientuppgifter lagras i krypterad form i AWS:s servrar och databasapplikationer och att endast Zenicor förfogar över krypteringsnyckeln, inte AWS. Enligt uppgift läser Zenicor in krypterad data lagrat hos AWS i Zenicor EKG Back-end System (i arbetsminnet). Där dekrypteras den så att applikationen kan utföra analyser och presentera resultat för respektive inloggad användare. All överföring av data (AWS till/från arbetsminne; applikation till/från klient; etc.) är krypterad. Efter bearbetning av data rensas arbetsminnet. Det är alltså inte fråga om någon permanent mellanlagring av okrypterad data i Zenicors back-end, utan data dekrypteras "i realtid" för hantering. All lagring och trafik mellan Zenicor och AWS sker således i krypterad form där Zenicor dekrypterar respektive krypterar uppgifter i sitt back-end på uppdrag av den personuppgiftsansvariga vårdgivaren.[14]

15.8 Den Europeiska dataskyddsstyrelsen (EDPB) fastställde i juni 2021 rekommendationer för tredjelandsöverföring med anledning av Schrems II-domen.[15] EDPB anger i skäl 3 till rekommendationerna att ”… in the absence of an EU adequacy decision, a controller or

[14] Mejlkonversation med Zenicor

[15] 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

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.

15.9 I bilaga 2 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 en "dataexportör" använder en "värdtjänstleverantör" i ett tredjeland för att lagra personuppgifter, t.ex. för säkerhetskopieringsändamål. EDPB skriver (fritt översatt till svenska) följande: Om

1. personuppgifterna behandlas med stark kryptering före överföring och identiteten av importören är verifierad,
2. krypteringsalgoritmen och dess parametrar (t.ex. nyckellängd etc.), överensstämmer med den senaste krypteringstekniken och kan anses vara robust mot kryptoanalyser som utförs av myndigheter i mottagarlandet med hänsyn till tillgängliga resurser och tekniska funktioner (t.ex. datorkraft för brute-force attacker),
3. krypteringens styrka och nyckellängd tar hänsyn till den specifika tidsperioden under vilken sekretessen för de krypterade personuppgifterna måste bevaras,
4. krypteringsalgoritmen implementeras korrekt och med korrekt underhållen programvara utan kända sårbarheter vars överensstämmelse med algoritmens specifikation har verifierats, t.ex. genom certifiering,
5. nycklarna hanteras på ett tillförlitligt sätt (genereras, administreras, lagras, om det är relevant, kopplat till en avsedd mottagares identitet, och återkallas), och
6. nycklarna enbart är under kontroll av dataexportören eller av en aktör som anlitas av dataexportören inom EU/EES eller under en jurisdiktion som erbjuder en väsentligen likvärdig nivå av skydd som garanteras inom EU/EES,

så anser EDPB att den utförda krypteringen innebär en effektiv kompletterande åtgärd och att tredjelandsöverföringen är tillåten enligt dataskyddsförordningen, trots brist på en adekvat skyddsnivå för européers personuppgifter i mottagarlandet.

15.10 Zenicors HYOK-lösning, om den är rätt implementerad och innefattar för ändamålet en effektiv nyckelängd och algoritm, bedöms eliminera helt risken för amerikanska myndigheter att kunna ta del av svenska patienters hälsorelaterade uppgifter i klartext, om dessa skulle begära ut uppgifter tillhörande svenska vårdgivare från AWS med yppandeförbud gentemot AWS.

15.11 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 att åtkomst till patientuppgifter föregås av stark autentisering. Zenicor erbjuder

inloggningslösningar baserade på stark autentisering, dvs. tvåfaktorsautentisering, bl.a. SITHS. Zenicor levererar således en lösning som lever upp till gällande författningskrav på identifiering inom en vårdgivares verksamhet.

15.12 Zenicor använder sessionscookies i Läkarsystemet för att hålla inloggningsinformation om vårdgivares medarbetare så länge som användaren är inloggad i systemet. Det är Zenicors egen kaka. Den är enligt uppgift från Zenicor alltså helt knuten till bolagets tjänstedomän (DNS) och ej åtkomlig för eller tillhandahållen av tredje part. Den är inte heller åtkomlig för script som körs i användares webbläsare. Kakan innefattar dessutom bara information om vårdgivarens organisation – inte individuella uppgifter. Organisationsuppgifter omfattas inte av dataskyddsförordningens bestämmelser med undantag för enskilda firmor baserade på egennamn. Den risken får betraktas som liten eftersom Zenicor används inom den slutna vården och i huvudsak av regioner och större kommunala bolag, men skulle egennamn förekomma har Zenicor rätt att behandla sådana personuppgifter i rollen som personuppgiftsbiträde.

15.13 Beträffande EKG-apparaten, dvs. Zenicor-EKG, väcks frågan i vilken utsträckning dataskyddsförordningen och PDL är tillämplig på den behandling av uppgifter i densamma. När en patient ska tilldelas apparaten registrerar vårdgivaren apparatens serienummer på patienten i Läkarsystemet. Kopplingen mellan patient och apparat finns således i Zenicors back-end. Apparaten innehåller inga namn eller personnummer. Apparaten har ingen inloggningsmekanism. Överföringen av rådata sker via ett inbyggt modem för mobilt nätverk (2/5G). Dock sparar apparaten rådata från mättillfällen som av någon anledning inte kunnat överföras till Zenicors EKG-databas. Såvitt förstås kan dock denna rådata inte åtkommas av användaren eller någon annan.

15.14 Det råder ingen tvekan om att eventuellt sparad rådata i apparaten utgör personuppgifter per definition enligt dataskyddsförordningen. Socialstyrelsens föreskriver i sina föreskrifter och allmänna råd till PDL (HSLF-FS 2016:40) ett krav på stark autentisering vid åtkomst till patientuppgifter över öppna nät. Det är inte aktuellt i detta fall eftersom vare sig användaren eller någon annan inte har åtkomst till rådata i apparaten. För övrigt sker i detta fall ingen åtkomst över öppet nät. Vårdgivaren är emellertid personuppgiftsansvarig för behandlingen av personuppgifterna i apparaten och för skyddet av uppgifterna vid överföringen, även om det sker i en teleoperatörs nät. Teleoperatörens ansvar regleras i lagen om elektronisk kommunikation.

15.15 Ur ett patientsäkerhetsperspektiv finns det anledning att resa vissa tvivel över apparaten. En vårdgivare kan inte veta om någon annan person använder apparaten Zenicor-EKG-2. Därmed finns en risk att vårdgivaren baserar sina diagnoser för en specifik patient (den som tilldelats apparaten) på helt felaktiga premisser. Patientsäkerhetsaspekter ligger utanför ramen för detta utredningsuppdrag, men däremot inte dataskyddsregleringen.

15.16 Av de grundläggande dataskyddsprinciperna i dataskyddsförordningen framgår att den personuppgiftsansvarige bl.a. ska säkerställa att behandlade personuppgifter är korrekta och relevanta (artikel 5.1). Vidare ställs krav på att personuppgiftsansvariga alltid beaktar inbyggt dataskydd (Privacy by design) vid utformning av system och tjänster så

att de är ”…utformade för ett effektivt genomförande av dataskyddsprinciper…” (artikel 25.1). **Det saknas ett inbyggt skydd för felaktig behandling av personuppgifter i Zenicor-EKG-2**. Det är vårdgivarna i rollen som personuppgiftsansvariga som ska säkerställa inbyggt dataskydd som lever upp till kraven i de grundläggande dataskyddsprinciperna. Risken får felaktig behandling av personuppgifter får emellertid betraktas som låg.

På uppdrag av MTP-rådet

Manólis Nymark