MOLNTJÄNSTER

och deras roll i utvecklingen mot en god och nära vård

Juridisk nulägesrapport december 2021, framtagen inom Innovationsmotorerna, ett projekt finansierat av Medtech4Health, en gemensam satsning av Vinnova, Formas och Energimyndigheten

SWEDISH Medtech

Medtech 4Health

Molntjänster och deras roll i utvecklingen mot en god och nära vård

Som vi alla vet, inte minst efter erfarenheter under Coronapandemin, är digitaliseringen av det svenska vård- och omsorgssystemet avgörande för en fortsatt högkvalitativ, personcentrerad, jämlik och hållbar vård och omsorg. Teknikutvecklingen går framåt i rasande takt och på medicinteknik-området tas ny diagnostik och nya behandlingsmetoder fram som effektiviserar hälso- och sjukvården, snabbar upp arbetsflöden och förenklar arbetet för personal och tillvaron för patienter.

Digitaliseringen är en förutsättning för att möjliggöra en ökad egenvård, att möta mål uppsatta av regeringen i Vision eHälsa[1] samt att satsningar ska kunna genomföras för en god och nära vård, baserat på utredningen med samma namn (SOU 2020:19[2]). Satsningar kommer bland annat från överenskommelsen som SKR och regeringen träffat[3] för att under 2021 vidareutveckla ”…hälso- och sjukvården för att patienten får en god, nära och samordnad vård som stärker hälsan”.

Digitaliseringen innebär dock en rad juridiska utmaningar. Inom hälso- och sjukvården kräver den nära vården behandling av känslig information. Lagringen av denna information sker ofta via moln-tjänster, vilka därför spelar en allt större roll i svensk hälso- och sjukvård. När en myndighet eller vårdorganisation i en region ska påbörja användandet av en molntjänst eller en produkt som inbegriper en molntjänst, måste hänsyn tas till olika lagbestämmelser. Lagar, förordningar, policys och riktlinjer tas fram, utvecklas och förändras allt eftersom tekniken utvecklas. Det medför att lagstiftaren ofta hamnar på efterkälken då det är svårt att hinna förstå eller förutse utvecklingen hos viss teknologi. Mycket händer på molntjänstområdet just nu och i väntan på att praxis ska utvecklas kan tolkningen av lagstiftningen skilja sig mellan olika aktörer, såväl hos myndigheter som hos regionala jurister.

Det har under en längre tid förelegat osäkerhet kring möjligheterna att upphandla molntjänster i offentlig sektor. Osäkerhet och avsaknad av tydlig juridisk vägledning gör att hälso- och sjukvården riskerar att gå miste om viktiga effektiviseringsvinster och utveckling av hälso- och sjukvården till gagn för både patienter och personal. Denna rapport, framtagen inom ramen för det nationella projektet Innovationsmotorer[4], finansierat av Vinnova, vill ge en ögonblicksbild av det juridiska läget i Sverige idag vad gäller molntjänster. Den vänder sig till dig som vill veta mer om vad de hinder som står i vägen för implementering av eHälsolösningar som använder sig av molntjänster i Sverige idag. *Rapporten är allmän i sin natur och syftar till att ge generell information, den har inte för avsikt att vara en heltäckande kartläggning av det rådande rättsläget. Rapporten är inte avsedd att vara eller ska tolkas och förlitas på som en juridisk bedömning eller rekommendation om en specifik fråga eller ett specifikt fall.*

[1] ehalsa2025.se/
[2] www.regeringen.se/495be8/contentassets/320f37078d854712ab89e8185466817b/god-och-nara-vard-en-reform-for-ett-hallbart-halso--och-sjukvardssystem-sou_2020_19_webb.pdf
[3] skr.se/skr/halsasjukvard/utvecklingavverksamhet/naravard/overenskommelseomengodochnaravard.28402.html
[4] https://www.swedishmedtech.se/sidor/innovationsmotorer.aspx

Innehållsförteckning

1 UTVECKLINGEN MOT EN DIGITALISERAD VÅRD OCH OMSORG 4

2 VAD ÄR EN MOLNTJÄNST? 5

3 ANSVAR OCH UTMANINGAR VID ANVÄNDNING AV MOLNTJÄNST 5

4 ARTIKEL 9 I DATASKYDDSFÖRORDNINGEN (GDPR) 7

5 OFFENTLIGHETS- OCH SEKRETESSLAGEN OCH MOLNTJÄNSTER 7

6 PRAXIS, UTTALANDEN, VÄGLEDNINGAR OCH LAGAR 8

6.1 JO-BESLUT 2014 OUTSOURCING AV JOURNALFÖRING INOM VÅRDEN 8
6.2 ESAM RÄTTSLIGT UTTALANDE 2015 9
6.3 CLOUD ACT, 2018 9
6.4 ESAMS RÄTTSLIGA UTTALANDE OM RÖJANDE OCH MOLNTJÄNSTER, 2018 9
6.5 ESAM KOMPLETTERANDE PROMEMORIA, SEPTEMBER 2019 10
6.6 ESAM OUTSOURCING 2.0 EN VÄGLEDNING OM SEKRETESS OCH DATASKYDD FRÅN 2019 10

7 NY LAG OM TYSTNADSPLIKT FÖR PRIVATA TJÄNSTELEVERANTÖRER, 2021 11

8 UTREDNING OM UTKONTRAKTERING, 2021 12

9 TREDJELANDSÖVERFÖRINGAR 16

9.1 SCHREMS II-MÅLET 16
9.2 NÄRMARE OM US CLOUD ACT 17
9.3 STANDARDAVTALSKLAUSULER FÖR ÖVERFÖRING TILL TREDJE LAND 18
9.4 SAMMANFATTANDE KOMMENTAR 19

10 OLIKA AKTÖRERS VÄGLEDNINGAR 20

10.1 SKR TILLHANDAHÅLLER ÖVERGRIPANDE VÄGLEDNING 20
10.2 INTEGRITETSSKYDDSMYNDIGHETEN 20
10.3 EUROPEISKA DATASKYDDSSTYRELSEN 21

11 ENSKILDA BEDÖMNINGAR I REGIONERNA 21

11.1 REGION STOCKHOLM 22
11.2 REGION ÖSTERGÖTLAND 22
11.3 REGION HALLAND 22
11.4 REGION SKÅNE 22
11.5 VÄSTRA GÖTALANDSREGIONEN 24

12 DET OSÄKRA RÄTTSLÄGETS EFFEKT PÅ MEDTECHINDUSTRIN OCH HÄLSO- OCH SJUKVÅRDEN 25

12.1 BESKRIVANDE CASE 26

13 AVSLUTANDE KOMMENTARER 27

14 BILAGOR 29

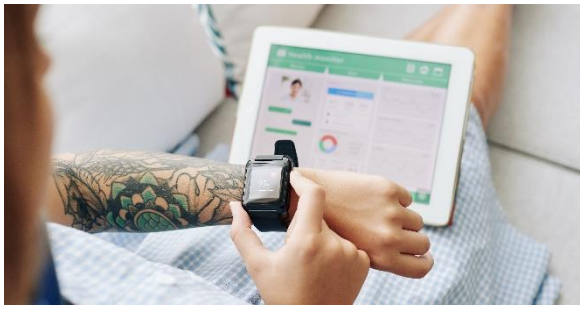
14.1 TILLVERKARENS/LEVERANTÖRENS ANSVAR 29
14.2 ANDRA AKTÖRERS ARBETE OCH INTRESSANTA LÄNKAR 29
14.3 NÅGRA BEGREPP OCH DEFINITIONER 29

1 Utvecklingen mot en digitaliserad vård och omsorg

Distansmonitorering möjliggör för patienter att själva regelbundet med hjälp av olika typer av medicintekniska produkter och tjänster mäta olika vitalparametrar och automatiskt och kontinuerligt kommunicera dem till sjukvården[5]. Detta skapar stora flöden av hälsodata från patienterna till vården och kräver säker och smidig infrastruktur för dataöverföring och -lagring.

Socialstyrelsen har i sitt uppdrag att följa omställningen till en mer nära vård i regioner och kommuner[6] slagit fast att såväl regioners som kommuners hälso- och sjukvård varit mycket ansträngd under Coronapandemin. Deras uppföljning visar det som tydligt framgått, nämligen att utvecklingen har gått mycket fort på digitaliseringsområdet, särskilt vad gäller i kontakten mellan patienter och vård. Pandemin har påtagligt visat på behov av och möjligheter med digitalisering inom vård och omsorg. Enligt utredningen *Framtidens teknik i omsorgens tjänst* (SOU 2020:14[7]) har användandet av välfärdsteknik ökat i den kommunala hälso- och sjukvården, men inte i den utsträckning som man idag har behov av. Två av de sex huvudsakliga hinder för ett breddinförande som utredningen lägger fram är osäkerhet kring de juridiska förutsättningarna.

Verktyg för egenvård, distansmonitorering och kommunikation finns tillgängliga, alla med olika typer av plattformar, upplägg och ersättningsmodeller. Befintliga produkter, med anpassningar för patient och vårdpersonal, kan redan nu skalas upp för hela Sverige och har kapacitet att hantera många fler patienter än vad som görs i dagsläget. Patienter som ingår i digitala behandlingsprogram för till exempel psykisk ohälsa eller astma kan fortsätta sina behandlingar oberoende av en hårt pressad fysisk vård. Digitala verktyg möjliggör både att vårdprofessioner kan arbeta hemifrån, och att patienter kan isolera sig vid behov. Man skyddar givetvis också de som inte kan undvika fysiska besök i vården.



Ett annat exempel är teknik som möjliggör för tjänsteleverantörer av medicintekniska produkter att effektivt övervaka en produkts prestanda liksom att utföra underhåll och säkerställa kontinuitet. Fjärrsupport gör det möjligt för servicepersonal att tidigt upptäcka och korrigera potentiella hårdvaru- och/eller mjukvaruproblem. Särskilt effektivt kan detta vara när ett problem inträffar under ett patientingrepp och vårdgivaren behöver omedelbar assistans. Support och service-information kan tillhandahållas oavsett plats eller tid på dygnet och i situationer när exempelvis besök på plats i vården är kostsamt eller opraktiskt, såsom under en pandemi. För att detta ska fungera kan data behöva delas utanför vårdorganisationen.

Dagens och framtidens hälso- och sjukvård är med andra ord helt beroende av att data kan delas sömlöst. Här verkar idag molntjänster vara avgörande. På samma sätt som att data måste kunna överföras mellan länder för forskning och utveckling och övervakning av produktsäkerhet krävs det, för att kunna bedriva hälso- och sjukvård, även att data kan överföras till tredje land. I det följande redogörs för vad en molntjänst är, vilka lagar som styr användandet av en molntjänst samt några viktiga myndigheters syn på och rekommendationer vad gäller användning av molntjänster.

[5] Ett illustrativt exempel på sid 26 i detta dokument: www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

[6] skr.se/skr/halsasjukvard/utvecklingavverksamhet/naravard/uppfoljningnaravard.46736.html

[7] www.regeringen.se/494156/contentassets/576aa4588db340b0ad052537ae90511d/framtidens-teknik-i-omsorgens-tjanst-sou-2020_14.pdf

2 Vad är en molntjänst?

Molntjänster är tjänster som tillhandahålls över internet. Det finns olika definitioner framtagna av tex NIST[8] och av SIS[9]. Det kan handla om lagring, datorkapacitet och programvara, allt från lagring av personalinformation till att artificiell intelligens (AI) behandlar patientdata för beslutsstöd. De mest vedertagna benämningarna på olika typer av molntjänster är *Software as a service*, SaaS (mjukvara), *Plattform as a service*, PaaS (plattform) och *Infrastructure as a service*, IaaS (infrastruktur)[10]. Det finns också olika typer av molninfrastrukturer: privata, publika, partnermoln och hybridmoln[11]. Fördelarna med molntjänster är både ekonomiska och praktiska då lagringsutrymme kan anpassas efter behov utan att investeringar i egna servrar måste göras, liksom att den lagrade informationen kan nås av användarna på ett enkelt sätt. Ökad säkerhet och minskade behov av egen it-personal brukar lyftas fram som andra fördelar.

Hur data ska lagras och användas på ett säkert sätt är en högaktuell fråga. Det är av yttersta vikt att klarlägga de legala förutsättningarna för användning av molntjänster. Molntjänster har många fördelar för vården men användningen kan också medföra risker. Genom ett systematiskt och ändamålsenligt informationssäkerhetsarbete ska data effektivt kunna nyttjas samtidigt som de skyddas från att hamna i orätta händer. Riskerna att använda molntjänster för känsliga personuppgifter kan minskas genom att vidta olika organisatoriska och tekniska åtgärder. Vid hantering av patientdata är tillgången till obehörig data en oerhört känslig punkt. Leverantörer av molntjänster erbjuder därför olika säkerhetsåtgärder, till exempel loggning av vem som har tillgång till data och kryptering.

3 Ansvar och utmaningar vid användning av molntjänst

Av 2 kap. 6 § Patientdatalagen (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 som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Den som använder en molntjänst för behandling av personuppgifter är personuppgiftsansvarig[12] även om den utförs av en molntjänstleverantör eller dess underleverantörer. När regionen upphandlar en medicinteknisk produkt är alltså regionen personuppgiftsansvarig för den behandling av person-uppgifter som sker kopplat till produkten och för syften som inbegriper hälso- och sjukvård i de fall vårdgivaren ska bestämma ändamålet för behandlingen. Leverantören och dess underleverantörer som anlitas för behandlingen är *personuppgiftsbiträden*. Personuppgiftsbiträdet behandlar personuppgifter ”för den personuppgiftsansvariges räkning”.

[8] csrc.nist.gov/publications/detail/sp/800-145/final

[9] SIS översättning av ISO-standarden definierar begreppet molnbaserade datortjänster som “koncept för nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser med automatisk åtkomst och administration på begäran”, se www.sis.se/api/document/preview/104900/

[10] Se sid 2: nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[11] Se sid 3: nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

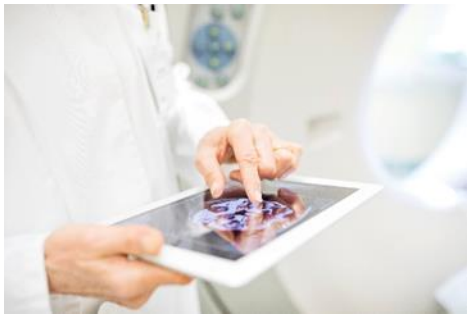
[12] www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

Regionen ansvarar för att hanteringen av information i en molntjänst följer tillämplig lagstiftning. En stor utmaning i dagsläget i samband med användning av molntjänster inom det offentliga är att bedöma under vilka förutsättningar detta är förenligt med nationell rätt och EU-rätt. Under de senaste åren har flera nya regelverk, som alla måste beaktas vid användning av molntjänster, trätt i kraft liksom uppdaterats. Dataskyddsförordningen (GDPR) och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) trädde i kraft 2018, det gjorde likaså lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS). EU-kommissionen presenterade i december 2020 ett förslag på ett nytt NIS-direktiv, kallat NIS 2. Andra tillämpliga lagar kan vara patientdatalagen (PDL), offentlighets- och sekretesslagen (OSL), Säkerhetsskyddslagen (SSL) och tystnadspliktslagen[13]. Frågor rörande upphandling, arkivhantering, upphovs- och avtalsrätt aktualiseras också ofta.

Därtill finns det flera länder utanför EU/EES-området, så kallade tredje länder, vars lagstiftning under vissa förutsättningar ger deras myndigheter rätt att ta del av uppgifter hos leverantörer under sin jurisdiktion. Ett exempel, som vi tittar närmare på i den här rapporten, är den amerikanska lagstiftningen CLOUD Act. Lagstiftningen i tredje land kan leda till att det uppstår konflikter med annan motstridig lagstiftning när en molntjänst tillhandahålls av en leverantör som står under jurisdiktion i ett tredjeland.

Utöver lagstiftning finns också till exempel utlåtanden, uttalanden och praxis att beakta. Det är den personuppgiftsansvarige som ska genomföra en risk- och sårbarhetsanalys, göra bedömningen om den aktuella behandlingen är laglig och vidta nödvändiga säkerhetsåtgärder för användning av molntjänsten. Ju större integritetsrisker, desto högre är kraven på säkerhetsåtgärder.

Ett personuppgiftsbiträdesavtal[14] som säkerställer de juridiska förutsättningarna genom specifika krav behöver tecknas med molntjänstleverantören där den personuppgiftsansvarige bestämmer hur personuppgifterna i molntjänsten ska behandlas samt vilka instruktioner personuppgiftsbiträdet ska följa. Av GDPR art 28 framgår att det av ett personuppgiftsbiträdesavtal bland annat ska framgå att biträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige (detta gäller även för överföringar till ett tredje land). Enligt avtalet ska tillförsäkras att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt. Personuppgiftsbiträdet ska vidta alla de tekniska och organisatoriska åtgärder som krävs enligt GDPR för att säkerställa en lämplig säkerhetsnivå. Det ska också av avtalet framgå att personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att se till att vissa i GPDR angivna skyldigheter avseende bland annat säkerhet uppfylls.



13 Tystnadspliktslagen lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter

14 https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/personuppgiftsbitradesavtal/

4 Artikel 9 i dataskyddsförordningen (GDPR)

I artikel 9 i GDPR regleras behandling av särskilda kategorier av personuppgifter. Enligt artikel 9.1 ska behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning vara förbjuden.

I artikel 9.2 finns ett antal undantag till förbudet i artikel 9.1. Enligt artikel 9.2h gäller inte förbudet om behandlingen av personuppgifterna är nödvändig av skäl som hör samman med bland annat förebyggande hälso- och sjukvård och tillhandahållandet av hälso- och sjukvård.

För att undantaget i artikel 9.2h ska vara tillämpligt krävs att villkoren om tystnadsplikt i artikel 9.3 är uppfyllda. Av artikel 9.3 framgår att personuppgifter som avses i artikel 9.1 får behandlas för de ändamål som avses i artikel 9.2 h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ. Under avsnitt 11.4.1 återkommer vi till artikel 9 i GDPR.

5 Offentlighets- och sekretesslagen och molntjänster

Offentlighets- och sekretesslagen (OSL) påverkar myndigheters möjlighet att använda molntjänster. Enligt 25 kap. 1 § OSL gäller sekretess inom hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Frågan om en vårdgivare kan lämna ut sekretessbelagda uppgifter till ett personuppgiftsbiträde eller till personal hos biträdet ska prövas på vanligt sätt enligt OSL. Vid användning av en molntjänst måste göras en noggrann analys av om ett utlämnande till molntjänstleverantören kan ske enligt relevanta sekretessbestämmelser. En skade-bedömning ska göras i varje enskilt fall där man bland annat tittar på hur molntjänsten ska användas, vilken typ av sekretessbelagda uppgifter som omfattas av ett visst utlämnande, hur uppgifterna skyddas hos molntjänstleverantören, d.v.s. hur de skyddas mot obehörig åtkomst, obehörig användning och spridning, samt i vilket land lagring sker och var underleverantören har sitt säte. OSL och dess påverkan på myndigheters möjlighet att använda molntjänster behandlas närmare under avsnitt 7.

6 Praxis, uttalanden, vägledningar och lagar

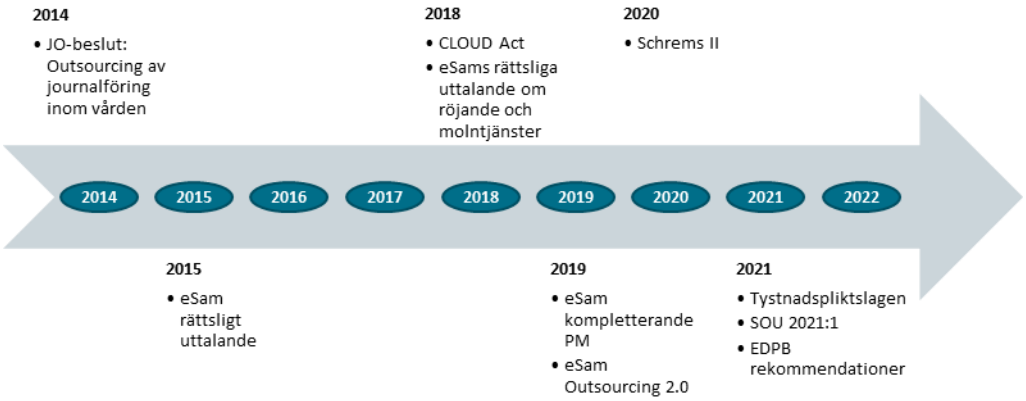
Debatten om huruvida offentliga myndigheters användning av molntjänster står i strid med OSL och annan lagstiftning, har pågått under lång tid, åtminstone sedan 2014 då Justitieombudsmannen (JO) kritiserade vårdgivare (se nedan). I följande stycken resoneras i kronologisk ordning kring några av de händelser som lett fram till det rådande osäkra rättsläget vad gäller förutsättningarna för offentlig sektor att upphandla privata molntjänstleverantörer.

6.1 JO-beslut 2014 Outsourcing av journalföring inom vården

I Justitieombudsmannens (JO:s) beslut den 9 september 2014 (dnr. 3032–2011)[15] riktades allvarlig kritik mot vårdgivare för att man ingått avtal om journalföring med ett företag trots att detta inte varit förenligt med reglerna om sekretess inom hälso- och sjukvården. Omständigheterna i ärendet var att läkarsekreterare hos företaget på distans lyssnade av inlästa läkardiktat som sedan skrevs in i patienters journaler. Uppgifterna lagrades aldrig utanför regionernas it-system. JO konstaterade att läkarsekreterarna hos företaget inte omfattas av den tystnadsplikt enligt OSL som gäller för vårdgivarens egen personal (en straffsanktionerad tystnadsplikt). Läkarsekreterarna hade en avtalsreglerad tystnadsplikt i förhållande till arbetsgivaren (d.v.s. företaget). Enligt JO bedömdes denna ”alternativa” tystnadsplikt för läkarsekreterarna inte tillräcklig för att anse att ett utlämnande kan ske utan att det innebär men (skada) för den som skyddas av sekretessen.

Vid bedömningen har – mot bakgrund av att de uppgifter som behandlas enligt avtalen är av mycket integritetskänsligt slag – vikt lagts bland annat vid att vårdgivarens egen personal kan dömas för brott mot tystnadsplikt om en sekretessbelagd uppgift felaktigt röjs, medan så inte är fallet när det gäller läkarsekreterare som är anställda i företaget. Ett utlämnande har inte heller haft stöd i någon sekretessbrytande bestämmelse.

Kommentar: JO:s bedömning utgår från omständigheterna i det aktuella ärendet. Man bör vara försiktig med att dra alltför långtgående slutsatser utifrån JO:s beslut då användningen av molntjänster typiskt sett inte innebär att anställda hos molntjänstleverantören tar del av kundernas uppgifter på det sätt som skett i det aktuella ärendet. Även om det finns anställda hos molntjänstleverantören som rent tekniskt kan komma åt uppgifterna finns det ofta instruktioner och tekniska åtgärder som begränsar denna åtkomst. Skillnaderna i detta hänseende kan påverka bedömningen. En anställd hos en leverantör som obehörigen skaffar sig tillgång till lagrade uppgifter kan även dömas för dataintrång. Sedan årsskiftet gäller också tystnadspliktslagen enligt vilka anställda hos en privat molntjänstleverantör, som hanterar sekretessbelagda uppgifter, kan åläggas en straffsanktionerad tystnadsplikt, se närmare avsnitt 7.



[15] www.jo.se/PageFiles/4794/3032-2011.pdf

6.2 eSam rättsligt uttalande 2015

I ett rättsligt uttalande[16] som publicerades i december 2015 bedömdes att uppgifter inte ska anses röjda i offentlighets- och sekretesslagens mening, trots att de gjorts tekniskt tillgängliga för en tjänsteleverantör, om tjänsteleverantören enligt avtal inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker. eSam[17] tittade här alltså på huruvida ett röjande sker, inte om vissa uppgifter är sekretessbelagda i förhållande till leverantören. Uttalandet omfattar inte molntjänster som erbjuds av företag som har datacenter i många länder och där informationen kan finnas i flera länder samt kan flyttas mellan olika jurisdiktioner. Sedan det här uttalandet gjordes har eSam i senare uttalandet bytt uppfattning till att det inte är osannolikt att ett röjande sker när en utländsk molntjänstleverantör anlitas, se nedan.

6.3 CLOUD Act, 2018

2018 antog USA CLOUD Act (Clarifying Lawful Overseas Use of Data Act), vilken är en lag som ger amerikanska rättsvårdande och brottsbekämpande myndigheter möjlighet att, från molntjänst-leverantörer som lyder under amerikansk jurisdiktion, under vissa förutsättningar begära ut data. Information skulle teoretiskt kunna begäras ut även om uppgifterna finns på servrar utanför USA. Se nedan för mer information om CLOUD Act.

6.4 eSams rättsliga uttalande om röjande och molntjänster, 2018

Efter att CLOUD Act antagits tog eSams juridiska expertgrupp fram ytterligare ett rättslig uttalande den 23 oktober 2018 (VER 2018:57)[18] om behandling av sekretessreglerade uppgifter i samband med användningen av vissa typer av molntjänster. Uttalandet följdes av ytterligare ett uttalande 2019 och det kompletterades med en uppdaterad vägledning[19].

eSam gör följande bedömning i sitt uttalande från 2018: Det rättsliga uttalandet från 2015 rörde inte sådana molntjänster som erbjuds av företag med servrar i olika länder, vilket kan innebära att informationen kan finnas sparad i flera länder och snabbt flyttas mellan olika jurisdiktioner samt vara åtkomlig över nät. Internationell rättshjälp är den väg en stat normalt har att gå enligt folkrätten för att få ta del av elektronisk bevisning från andra stater vad gäller innehåll i molnkonton och liknande. Det innebär att den stat som behöver information från en server i en annan stat måste begära hjälp av den andra statens myndigheter för att få ut informationen. Ett intensivt regelarbete pågår dock i många stater, vilket gör rättsläget osäkert.

Det förekommer att företag enligt den rättsordning som gäller i ett annat land är skyldiga att under vissa omständigheter lämna information till en myndighet i det landet utan att frågan hanteras genom internationellt samarbete mellan berörda stater. Som exempel anger eSam den reglering som innebär att amerikanska myndigheter ska ges tillgång även till data som lagras utomlands och att amerikanska tjänsteleverantörer av det skälet inte kan vägra att lämna ut sådana data. Sekretess-reglerade uppgifter kan enligt denna reglering komma att lämnas ut även om själva lagringen sker inom EU:s gränser.

---

[16] "Röjandebegreppet enligt offentlighets- och sekretesslagen", 17 december 2015.
[17] eSamverkansprogrammet (eSam) är ett medlemsdrivet program för samverkan mellan 27 myndigheter och Sveriges Regioner och Kommuner (SKR).
[18] https://www.esamverka.se/download/18.1d126bc174ad1e6c39cac3/1542007824143/eSam%20-%20Ra%CC%88ttsligt%20uttalande%20om%20ro%CC%88jande%20och%20molntj%C3%A4nster.pdf
[19] "Kompletterande information om molntjänster", 20 september 2019, "Outsourcing 2.0 – En vägledning om sekretess och dataskydd", december 2019.

Enligt eSam får sekretessreglerade uppgifter anses vara röjda (enligt OSL) om de lämnas till ett företag som omfattas av en förpliktelse av beskrivet slag. Det finns dessutom företag som erbjuder molntjänster där ägarförhållandena eller den geografiska placeringen av de tekniska hjälpmedlen är sådana att det finns skäl att ifrågasatta skyddet för mänskliga rättigheter, bland annat skyddet för privatlivet, eller skyddet för det allmännas intressen, till exempel skyddet för rikets säkerhet. Även här bör enligt eSam en försiktig bedömning göras. Ger omständigheterna anledning att befara att mänskliga rättigheter eller nationens intressen inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts får dessa uppgifter anses vara röjda eftersom det inte längre är osannolikt att de lämnas till utomstående.

Kommentar: Kritik har riktats mot eSams uttalande från 2018, se mer om detta nedan.

6.5 eSam kompletterande promemoria, september 2019

På grund av att det rättsliga uttalandet den 23 oktober 2018 om röjande och molntjänster (VER 2018:57) ifrågasatts har eSam lämnat kompletterande information i en promemoria i september 2019[20]. Man hänvisar till den bedömning som eSams juridiska expertgrupp gjorde i det rättsliga uttalandet 2015 (se ovan) och tydliggör att det inte räcker med en sannolikhetsbedömning av om ett röjande kan komma att ske. Först måste den rättsliga regleringen av parternas mellanhavande ha utformats på ett hållbart sätt så att en juridiskt bindande och sanktionerad avtalssekretess föreligger. Dessutom får leverantören av tjänsten inte vara bunden av regler i främmande rätt om att lämna ut uppgifter utan en föregående sekretessprövning eller annan laglig grund enligt svensk rätt för ett utlämnande. Dessa kompletteringar har inte inneburit att expertgruppens ändrat sina tidigare uttalanden.

6.6 eSam Outsourcing 2.0 En vägledning om sekretess och dataskydd från 2019

Vägledningen innehåller bland annat avsnitt om sekretess och dataskydd i samband med outsourcing av funktioner som annars skulle skötas i offentlig verksamhets egen regi. Vidare följer eSam upp det rättsliga uttalande om röjande av sekretessreglerade uppgifter och molntjänster från oktober 2018 (VER 2018:57). *Sammanfattningsvis står eSam fast vid sin bedömning och den grundläggande uppfattningen är att CLOUD Act innebär en risk för att uppgifter kan lämnas vidare till amerikanska myndigheter, och att denna risk innebär att uppgifterna ska betraktas som röjda till dessa myndigheter.*

Kommentar: Om man ska försöka sammanfatta eSams ståndpunkt i uttalandena ovan är de att ett utlämnande till en tjänsteleverantör som omfattas av CLOUD Act innebär att uppgifterna får anses vara röjda till utländsk myndighet. Detta då det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående. eSams uppfattning om gällande rätt har kritiserats från flera håll[21]. Rättsläget kring frågan om röjande enligt OSL är osäkert trots att det har behandlats i olika rätts-utlåtanden och utredningar (bland annat it-driftsutredningen, se nedan). Efter eSams rättsliga uttalanden var det många myndigheter som bedömde att det förelåg juridiska hinder att använda sig av molntjänstleverantörer som omfattas av CLOUD Act, en bedömning som naturligtvis påverkat digitaliseringen av offentlig sektor/hälso- och sjukvård negativt.

[20] eSam, Kompletterande information om molntjänster: www.esamverka.se/download/18.1d126bc174ad1e6c39caf4/1568977769756/Kompletterande%20information%20om%20molnfr%C3%A5gan%202019-09.pdf

[21] https://www.regeringen.se/48efac/contentassets/10a3aff9f8b847b48b35036d0907439e/saker-och-kostnadseffektiv-it-drift--rattsliga-forutsattningar-for-utkontraktering-sou_2021_1

7 Ny lag om tystnadsplikt för privata tjänsteleverantörer, 2021

I januari 2021 trädde tystnadspliktslagen, lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, i kraft[22]. Lagen ska skydda så att personers känsliga uppgifter om till exempel hälsa inte röjs till obehöriga. Lagen är tillämplig när en myndighet[23], genom utkontraktering uppdrar åt en tjänsteleverantör (exempelvis en molntjänstleverantör) att endast tekniskt bearbeta eller tekniskt lagra uppgifter. Syftet är att uppgifter från en myndighet som hanteras av en tjänsteleverantör ska få ett sekretesskydd likvärdigt med det som gäller när en annan myndighet tillhandahåller en sådan tjänst. Med andra ord möjliggörs det för offentlig sektor att röja sekretesskyddade uppgifter till tjänsteleverantörer i situationer då det tidigare inte varit tillåtet[24]. Lagen är tillämplig på tjänsteleverantörer i Sverige, d.v.s. anställda i svenska verksamheter som anlitas för ”teknisk bearbetning eller teknisk lagring” av de sekretesskyddade uppgifterna [25]. Den som bryter mot bestämmelsen riskerar att göra sig skyldig till brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken[26]. Tystnadsplikten omfattar även personal hos tjänsteleverantörers underleverantörer. I avsnittet 11.4.1 berörs bestämmelsen närmare. Vilka tjänster som ryms inom begreppen exemplifieras i propositionen[27]:

”Vilka slag av åtgärder som kan omfattas av teknisk bearbetning eller teknisk lagring behöver tolkas i förhållande till dagens digitala informationshantering och den fortgående tekniska utvecklingen. En tjänsteleverantör kan exempelvis ha i uppdrag att införa, förvalta, utveckla och så småningom avveckla en tjänst åt en myndighet. Tjänsteleverantören kan under dessa olika faser behöva vidta en mängd olika åtgärder som innefattar teknisk bearbetning eller teknisk lagring av uppgifter för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som har avtalats mellan parterna. Sådana åtgärder kan röra sig om förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration mot andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Det kan också röra sig om säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering. Vid avveckling av en tjänst kan myndighetens information behöva migreras eller exporteras tillbaka till myndigheten eller till en annan tjänsteleverantör.”

---

[22] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2020914-om-tystnadsplikt-vid_sfs-2020-914

[23] 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.

[24] Bakgrunden till lagens tillkomst är att OSL inte innehåller någon allmän bestämmelse om tystnadsplikt för en utomstående fysisk eller juridisk person som tar del av en sekretessbelagd uppgift. Eftersom molntjänstleverantörer tidigare inte omfattats av den straffsanktionerade tystnadsplikten i 20 kap. 3 § brottsbalken var det upp till myndigheten och den privata leverantören att själva avtala om tystnadsplikt vid en utkontraktering. Det har ansetts oklart om en sådan avtalsreglerad tystnadsplikt varit tillräckligt för att ett utlämnande till en molntjänstleverantör ska kunna ske, särskilt efter att det i JO:s beslut (se avsnitt ovan) uttalades att en särskild viktig aspekt vid skade- och menbedömningen är huruvida den utomstående mottagaren omfattas av en tystnadsplikt som är straffsanktionerad. Enligt JO stod det inte klart att ett utlämnande av de sekretessbelagda uppgifterna som var av integritetskänslig art kunde ske utan men för den enskilde eller närstående till denne, och därför saknades rättsligt stöd för att lämna ut uppgifterna. Inte heller kunde någon av de sekretessbrytande bestämmelserna i 10 kap. OSL medge ett utlämnande.

[25] Begreppen teknisk bearbetning och teknisk lagring är hämtade från tryckfrihetsförordningen.

[26] Vård- och omsorgspersonal i Sverige omfattas redan av en lagstadgad straffsanktionerad tystnadsplikt som kan ge böter eller fängelse upp till 1 år, se OSL 2 kap. 1 § för allmän verksamhet och Patientsäkerhetslagen 6 kap. 12–16 §§ för privat hälso- och sjukvård.

[27] https://www.regeringen.se/4a522b/contentassets/8c634aa11b01455f80af380ccbfddc83/tystnadsplikt-vid-utkontraktering-av-teknisk-bearbetning-eller-lagring-av-uppgifter-prop-201920201

En fråga, som bland andra Integritetsskyddsmyndigheten (IMY) tittat på, är räckvidden av den lagstadgade tystnadsplikten[28]. En förutsättning för tillämpning av den sekretessbrytande grunden är nämligen att it-leverantörens och/eller underleverantörers personal också kan dömas för brott mot tystnadsplikten. För brott som begås utanför Sverige har svensk domstol endast domsrätt för fall där den som begått brottet är svensk medborgare eller har hemvist i Sverige. Se mer om detta under avsnitt 11.4.1.1. Rättsläget är oklart men detta skulle eventuellt kunna innebära att myndigheten inte kan nyttja exempelvis en amerikansk leverantör vars personal inte är hemmahörande i Sverige.

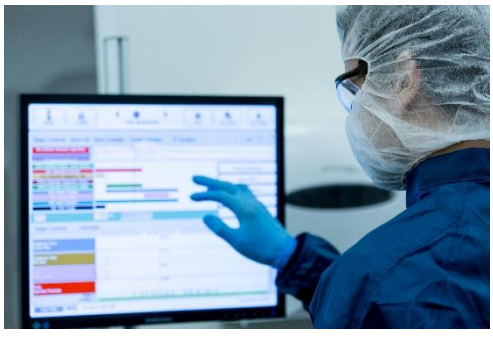
I en situation där en svensk myndighet anlitar en utländsk tjänsteleverantör verksam utanför Sveriges gränser och kompenserar bristen på straffrättsligt skydd för sekretessbelagda personuppgifter med att i stället ingå ett sekretessavtal med leverantören är det oklart om det är tillräckligt som skydd för sekretessbelagda personuppgifter. Ett alternativ skulle eventuellt kunna vara att det i landet där leverantören bedriver sin verksamhet finns lagstiftning med bestämmelser om tystnadsplikt för tjänsteleverantörer som sanktioneras med böter eller fängelse vid överträdelse. Enligt artikel 28 i GDPR kan sådan utländsk straffsanktionerad tystnadsplikt vägas in vid bedömningen om leverantören kan ge ”tillräckliga garantier för dataskydd”.

Trots att det i GDPR uppställs krav på såväl att personuppgiftsansvarig och personuppgiftsbiträde ska skydda personuppgifterna som på tydliga instruktioner i personuppgiftsbiträdesavtal till leverantören om hur personuppgifterna får behandlas, samt krav på tystnadsplikt, så måste bestämmelserna kring tystnadsplikt i OSL iakttas.

8 Utredning om utkontraktering, 2021

I delbetänkandet ”Säker och kostnadseffektiv it-drift - rättsliga förutsättningar för utkontraktering” (SOU 2021:1, ”it-driftsutredningen”) behandlas den rådande osäkerheten kring förutsättningarna för offentlig sektor att upphandla it-tjänster hos privata leverantörer. Utredningen analyserar bland annat rättsliga förutsättningar för statliga myndigheter, kommuner och regioner att med bibehållen säkerhet utkontraktera it-drift till privata leverantörer. Att offentlig sektor följer med i den tekniska och digitala utvecklingen är av vikt av säkerhets-, kostnads- och effektivitetsskäl och utredningen framhåller att statliga myndigheter, kommuner och regioner har behov av att utkontraktera it-drift som omfattar sekretessreglerade uppgifter. Detta eftersom lösningar för it-drift nästan uteslutande tillhandahålls av privata bolag.

Utredningen konstaterar att utkontraktering av it-drift som medför att sekretessbelagda uppgifter tillgängliggörs till leverantören är att se som ett röjande enligt OSL, detta oavsett om uppgifterna har krypterats eller pseudonymiserats, och oavsett om leverantören (t.ex. en molntjänstleverantör) är bunden av CLOUD Act eller inte[29]. Att exempelvis binda it-leverantören till sekretess genom avtal innebär inte att uppgifterna är skyddade på så vis att röjandet kan anses vara tillåtet. Det är endast om det föreligger en lagstadgad sekretessbrytande grund som uppgifterna får röjas. Avtal utgör idag inte en sådan grund i OSL. Utredningen föreslår därför att det införs en ny bestämmelse i 10 kap OSL med följande rubrik och lydelse:



[28] Samrådsyttrande DI-2021-2983 s. 14.
[29] Delbetänkandet, s.277.

Utkontraktering av teknisk bearbetning eller lagring av uppgifter

2 a§ *Sekretess hindrar inte att en uppgift lämnas ut till ett företag eller annan enskild eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de uppgifter som lämnas ut för den utlämnande myndighetens räkning.*

En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Det andra stycket ovan innebär alltså att ett utlämnande villkoras med att myndigheten först gör en intresseavvägning, och då kommer fram till att sekretessintresset inte överväger intresset av en utkontraktering. Enligt it-driftsutredningen behövs en sekretessbrytande bestämmelse dels för att förenkla den skadeprövning som myndigheten ska göra innan ett utlämnande, dels bedömer man att ett utlämnande mot sekretessförbehåll endast kan ske i undantagsfall vid utkontraktering. Ytterligare en anledning är att det finns begränsade möjligheter för myndigheterna att utkontraktera it-drift om utkontrakteringen omfattar uppgifter som träffas av absolut sekretess.

It-driftsutredningen anser, *till skillnad från eSam*, att myndigheter inte röjer uppgifter för en utländsk myndighet på otillåtet vis, om de lämnar ut uppgifter till leverantörer som omfattas av CLOUD Act, bara för att en sådan leverantör kan behöva lämna uppgifterna vidare till amerikanska myndigheter. CLOUD Act har ingen betydelse för om uppgifter ska anses ha röjts enligt OSL då uppgifterna ska anses röjda redan när de överförts till en molntjänstleverantör. Enligt eSam står dock detta i strid med specifikt 8 kap. 3 § OSL, enligt vilken råder ett förbud för myndigheter att i vissa fall röja uppgifter för utländska myndigheter. It-driftsutredningens bedömning är dock att en överföring till USA sker först i samband med att uppgifterna i fråga rent faktiskt överförs till myndigheter eller annan mottagare i USA[30]. Som huvudregel förbjuder OSL myndigheter att röja uppgifter för utländska myndigheter. Men att en leverantör, som fått uppgifter till sig av en svensk myndighet, eventuellt lämnar uppgifter vidare till en utländsk myndighet innebär inte att den svenska myndigheten har röjt uppgifterna för den utländska myndigheten - den svenska myndigheten har röjt uppgifterna endast för leverantören. Enligt utredningen bryter således inte en myndighet mot 8 kap 3 § genom att lämna ut uppgifter till en tjänsteleverantör som är bunden av CLOUD Act eller någon annan liknande reglering[31]. Givetvis måste annan lagstiftning såsom GDPR fortfarande beaktas när personuppgifter överförs. Utredningen menar att det inte har någon betydelse om uppgiften är krypterad eller pseudonymiserad för om personuppgiften ska anses överförd till tredje land genom att behandlas genom utrustning i tredjeland.

Kommentar: Om it-driftsutredningens förslag går igenom (lagen förväntas träda i kraft i januari 2022) torde myndigheter kunna använda en molntjänstleverantör för uppdrag att utföra teknisk bearbetning eller teknisk lagring för samtliga typer av sekretessbelagda uppgifter, även absolut sekretess, i enlighet med OSL. En intresseavvägning måste dock göras av myndigheten, där intresset för utkontraktering ska väga tyngre än intresset som skyddas av sekretess, för att det ska vara möjligt.

[30] Delbetänkandet s. 215.
[31] Delbetänkandet s. 271–272.

Enligt utredningen sker, som också nämnts ovan, ett röjande oavsett om uppgifterna är krypterade eller pseudonymiserade. Detta då det enligt utredningen i dagsläget saknas kända tekniska säkerhetsåtgärder som gör det omöjligt för en tjänsteleverantör att ta del av uppgifterna[32]. Kryptering och pseudonymisering kan dock ha betydelse i myndigheternas övergripande bedömning avseende om ett utlämnande av personuppgifter till en molntjänstleverantör kan orsaka skada (skadeprövningen). Likaså lyfts i utredningen att kryptering och liknande åtgärder ska beaktas i den intresseavvägning som ska göras av myndigheten.

Utredningen gör inte någon uttrycklig skillnad på utländska (amerikanska med hänsyn till CLOUD Act och europeiska) och svenska molntjänstleverantörer. Men vid myndighetens intresseavvägning avseende om utkontraktering är möjlig, ska en bedömning av hur starkt sekretesskyddet är hos leverantören, göras[33]. I en FAQ framtagen av Synch Advokat AB[34] lyfts att det även är möjligt att argumentera för att risken för att obehörig ges åtkomst till uppgifterna ska ges betydelse vid bedömningen. Vidare argumenteras för i FAQ:n[35] att, även om utredningen inte uttryckligen tar upp det, man kan tänka sig två omständigheter till varför det faktum att leverantören är amerikansk får betydelse inom intresseavvägningen:

1. *Den nya lagstadgade tystnadsplikten[36] som talar för att uppgifter kan utkontrakteras, träffar sannolikt inte amerikanska leverantörer lika effektivt som den träffar leverantörer som uteslutande har anställda inom EU. Detta eftersom det kan tänkas att brottet mot tystnadsplikten begås av anställda utanför EU, och att det är osäkert i vad mån svensk domstol då har jurisdiktion[37]. Det är alltså oklart om det går att lagföra anställda hos utländska tjänsteleverantörer för samtliga brott mot den straffsanktionerade tystnadsplikten.*

2. *CLOUD Act medför potentiellt en risk för att enskildas personuppgifter lämnas ut till utländska myndigheter och därigenom överförs till USA. Denna potentiella risk kan medföra att utkontrakteringen innebär större risker för de enskildas personuppgifter, vilket skulle kunna tillmätas betydelse vid intresseavvägningen enligt den föreslagna bestämmelsen.*

Vidare argumenterar författarna till FAQ:n att det ska noteras att dessa omständigheter är två av flera omständigheter som skulle kunna läggas i vågskålen vid den intresseavvägning myndigheter ska genomföra enligt den föreslagna bestämmelsen[38]. En leverantör kan förvisso ha anställda utanför EU, där det är oklart om lagen om tystnadsplikt vid utkontraktering är effektiv mot, men samma leverantör kan ha vidtagit organisatoriska åtgärder som gör att dessa anställda inte får tillgång till kundens data (och därmed inte kan bryta mot tystnadsplikten), och/eller ha hög kapacitet att sätta in tekniska säkerhetsåtgärder, såsom kryptering, som gör det mycket svårt för någon obehörig att ta del av uppgifterna. Detta är något som vi även lyfter i avsnitt 12 i den här rapporten.

[32] Delbetänkandet s. 281–283.
[33] Delbetänkandet s. 338.
[34] https://pages.awscloud.com/rs/112-TZM-766/images/AWS_FAQ_om_Delbeta%CC%88nkandet_i_it_driftsutredningen_2021.pdf
[35] FAQn s. 5.
[36] Lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter
[37] Delbetänkandet s. 338.
[38] Delbetänkandet s. 299–300.

Bestämmelsen om sekretessbrytning kan underlätta utlämning av uppgifter vid utkontraktering av it-drift vilket kan gynna den offentliga it-driftsmarknaden som helhet och minska den rättsliga osäkerheten hos offentlig sektor. För att underlätta och möjliggöra utkontraktering av it-drift behöver myndigheterna stöd, kompetens och resurser för att kunna genomföra intresseavvägningar mellan behov av sekretesskydd och möjlighet till utkontraktering. I kombination med tystnadsplikts-lagen (se avsnitt ovan) bör det, om lagförslaget går igenom, för tjänster som ryms inom teknisk bearbetning och lagring, finnas ett gott skydd för de uppgifter som röjs.

It-driftsutredningen menar att det är problematiskt att använda en molntjänstleverantör om överföring innebär att personuppgifterna förs över till USA. Enligt utredningen sker en tredjelands-överföring om personuppgifter behandlas *genom användning av utrustning som finns i USA*, och inte direkt på grund av att molntjänstleverantören faller under amerikansk jurisdiktion (d.v.s. CLOUD Act, vilken kan innebära att information kan behöva lämnas ut till amerikanska myndigheter)[39]. Enligt it-driftsutredningen sker inte någon överföring av personuppgifter om uppgifterna behandlas uteslutande inom EU[40]. Utredningen tycker alltså annorlunda än eSam som menar att CLOUD Act innebär en risk för att uppgifter kan lämnas vidare till amerikanska myndigheter och att risken innebär att uppgifterna ska betraktas som röjda till dessa myndigheter. Frågan har inte prövats rättsligt av EU-domstolen som skulle kunna komma fram till en annan slutsats.

Slutbetänkandet ”Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift” (SOU 2021:97) fokuserade på förutsättningar och förslag på samordnad statlig it-drift och fastslår att ”Varje myndighet som vill ansluta sig till det samordnade statliga tjänsteutbudet måste ta ställning till om det är möjligt och lämpligt utifrån de krav som säkerhetsskyddslagen ställer på den egna verksamheten. De myndigheter som tillhandahåller tjänster inom det samordnade statliga tjänsteutbudet måste löpande ta ställning till hur tillhandahållandet påverkar myndighetens verksamhet utifrån säkerhetsskyddssynpunkt.” Slutbetänkandet ger inte vidare vägledning om den sekretessbrytande bestämmelsen som föreslogs i delbetänkandet (SOU 2021:1).

[39] Delbetänkandet s. 212.
[40] Delbetänkandet s. 215.

9 Tredjelandsöverföringar

Överföringar av personuppgifter till tredje land innebär att personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området. Sådana överföringar är enligt GDPR tillåtna under förutsättning att det finns ett beslut från EU-kommissionen om att ett visst land utanför EU/EES säkerställer så kallad adekvat skyddsnivå eller om den som för över personuppgifterna vidtagit lämpliga skyddsåtgärder, så som till exempel bindande företagsbestämmelser eller standardavtalsklausuler[41].

9.1 Schrems II-målet

Svenska myndigheter, regioner och kommuner behöver kunna köpa it-tjänster från det privata näringslivet där en stor del av marknaden domineras av amerikanska molntjänstleverantörer såsom Google, Amazon och Microsoft, alla med hemvist i USA. Detta leder till är en stor utmaning vad gäller att upprätthålla det höga skyddet för personuppgifter såsom dataskyddsförordningen föreskriver. EU:s bedömning har varit att USA inte upprätthåller det höga skyddet för personuppgifter såsom GDPR föreskriver, men genom Privacy Shield[42] var det ändå tidigare möjligt att föra över personuppgifter från EU till USA.

För drygt ett år sedan avgjorde EU-domstolen det så kallade Schrems II-målet (dom den 16 juli 2020 i mål C311/18[43]) där EU-domstolen ogiltigförklarade Privacy Shield som mekanism för överföring av personuppgifter mellan EU och USA. Trots att det gått en tid sedan domen föll råder fortfarande stor osäkerhet och oro bland alla aktörer för vad som ska hända med dataöverföringar utanför EU på sikt, men också hur man ska hantera alla de dataflöden som ständigt pågår och som är helt nödvändiga för att kunna bedriva och utveckla hälso- och sjukvård.

Skälet till att Privacy Shield ogiltigförklarades var att amerikansk lagstiftning CLOUD Act (se nästa avsnitt) ger amerikanska rättsvårdande myndigheter möjlighet att begära ut data från en amerikansk molntjänstleverantör, där data överförs från EU till mottagare i USA på ett sätt som inte anses förenligt med GDPR. EU-domstolen ansåg att Privacy Shield inte gav ett tillräckligt skydd för behandling av personuppgifter p.g.a. de övervakningsprogram som USA använder sig av[44]. EU-domstolen menade att data kunde krävas ut trots att det amerikanska molntjänstföretaget var anslutet till Privacy Shield-avtalet. Därmed ansåg domstolen att det inte fanns ett adekvat skydd för överförda personuppgifter. Privacy Shield ogiltigförklarades med omedelbar verkan vilket i praktiken inneburit att det inte längre är möjligt att stödja sig på denna skyddsåtgärd för en tillåten överföring av personuppgifter från EU till USA. Dataexportörer uppmanades att avbryta all överföring till USA som stödde sig på Privacy Shield, alternativt tillämpa en annan skyddsåtgärd.

[41] Se tex https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/
[42] Se tex https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en och https://www.privacyshield.gov/welcome
[43] Domen återfinns här: https://curia.europa.eu/juris/liste.jsf?num=C-311/18
[44] som grundar sig på den amerikanska lagstiftningen 702 Foreign Intellegence Surveillence Act (FISA) och presidentordern E.O. 12333

9.2 Närmare om US CLOUD Act

CLOUD Act innebär, något förenklat, att en leverantör av en elektronisk kommunikationstjänst eller fjärrdatatjänst som är börsnoterad i USA ska bevara, säkerhetskopiera eller avslöja innehållet i en molntjänst som gäller en kund eller abonnent inom dennes besittning, vårdnad eller kontroll, oavsett om sådan kommunikation, post eller annan information finns inom eller utanför USA. Data kan med andra ord teoretiskt begäras ut oavsett geografisk hemvist och det är alltså oväsentligt var själva servrarna står. Om molntjänstleverantören är ett amerikanskt företag lyder det under CLOUD Act, även om kunderna och kundernas data befinner sig i en annan jurisdiktion.

Det är tänkbart att CLOUD Act kan användas av amerikanska brottsbekämpande myndigheter för att begära ut data från en svensk myndighet som lagrar data i en molntjänst driftad av ett amerikanskt bolag. Detta alltså även om servrarna som lagrar den svenska myndighetens data finns utanför USA:s gränser.Ett dilemma för molntjänstleverantören som lagrar personuppgifter åt en svensk myndighets räkning är att myndigheten är personuppgiftsansvarig och leverantören personuppgiftsbiträde. Om krav ställs av amerikansk brottsbekämpande myndighet på att leverantören ska lämna ut person-uppgifter som lagras i molntjänsten kan leverantören tvingas välja lag att bryta mot - antingen lämna ut uppgifterna och då bryta mot GDPR alternativt välja att inte lämna ut uppgifterna och då riskera bryta mot CLOUD Act.

För att CLOUD Act ska vara tillämplig krävs, förutom att den aktuella molntjänstleverantören omfattas av amerikansk jurisdiktion, att det föreligger sannolika skäl för att ett brott har begåtts och att uppgifterna har relevans för brottsutredningen. CLOUD Act auktoriserar alltså inte systematisk övervakning av enskilda individer i stor skala. Det krävs målinriktade begäranden, s.k. ”warrants”, om utlämnade av information. En warrant utfärdas av amerikanska brottsbekämpande myndigheter och kräver en oberoende domstolsprövning. Utfärdandet av en warrant kräver en stark misstanke om att ett brott har begåtts vilket betyder att det inte är möjligt att tråla efter bevis om kriminell aktivitet i största allmänhet. Den leverantör som omfattas av en begäran har möjlighet att framföra invändningar mot densamma men det är inte klart i vilken utsträckning en tjänsteleverantör kan bestrida en begäran.

Som ovan nämnts har eSam tidigare uttalat att CLOUD Act innebär att sekretessreglerade uppgifter ska anses automatiskt röjda i den utsträckning som CLOUD Act är tillämpligt därför att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående. Med hänvisning till det som anförts ovan kan resoneras i motsatt riktning, d.v.s. att sannolikheten att uppgifter skulle komma att lämnas ut till amerikanska myndigheter inte är speciellt stor. Intressanta resonemang kring detta finns att ta del av i Delphis utlåtande i frågan om överföring av personuppgifter i samband med Cerner Sverige AB:s leverans av Skånes Digitala Vårdsystem[45].

Med detta sagt kan användning av en molntjänstleverantrör för utkontraktering anses vara tillåten enligt OSL men otillåten enligt GDPR. Två olika lagstiftningar måste beaktas vid utkontraktering. Står utkontrakteringen i strid med en av dessa lagar så är den inte tillåten[46]. I den intresseavvägning som myndigheten ska göra, inför beslut huruvida utkontraktering kan göras enligt OSL, kan risken för att personuppgiftsbehandlingen är i strid med GDPR vara en viktig faktor.

[45] https://prod.api.bbmpremium.se/globalassets/digital-halsa/dokument-digital-halsa/legal-memo-region-skane_final_210226_pdf_sekretessbedomnd.pdf
[46] Delbetänkandet s. 301.

9.3 Standardavtalsklausuler för överföring till tredje land

En av de vanligaste skyddsåtgärderna[47] för överföring till tredje land är EU:s standardavtalsklausuler (Standard Contractual Clauses, SCC)[48]. Ett avtal innehållande SCC som ingås med aktör utanför EU/EES tillåter överföring av personuppgifter till denna aktör. Även SCC var föremål för prövning i Schrems II. EU-domstolen fastslog att SCC även fortsättningsvis kan tillämpas vid överföring till tredje land[49]. Däremot är det inte alltid en lämplig överföringsmekanism. Domstolen prövade inte specifikt om SCC är olagliga i USA, men då amerikansk lagstiftning vad gäller Privacy Shield har funnits vara i strid med europeisk lagstiftning, så är risken överhängande att även SCC är otillräckliga och därmed inte lagliga vad avser överföring specifikt till USA[50]. *Att använda SCC för amerikanska molntjänster blir alltså i praktiken ett påtagligt problem idag eftersom de inte binder amerikanska myndigheter.*

Genom att i vissa fall implementera ytterligare skyddsåtgärder - där företagen själva ser till att mottagarlandet har ett likvärdigt dataskydd som GDPR uppställer - kan en tillräcklig säkerhetsnivå uppnås. I Schrems II gav domstolen ingen ledning om vilka kompletterande åtgärder som kan säkerställa ett tillräckligt skydd vid överföring till tredje land. Det är upp till varje enskild aktör som exporterar data att göra en riskutvärdering och bedöma om SCC innebär ett effektivt skydd i det enskilda fallet, eller om det behövs kompletterande åtgärder för att uppnå en adekvat skyddsnivå. I praktiken innebär detta att det är upp till den som överför personuppgifter att bedöma huruvida dataimportörens nationella lagstiftning erbjuder en skyddsnivå som säkerställer effektiviteten av SCC, d.v.s. en skyddsnivå som motsvarar den inom EU/EES. Om skyddet från SCC undergrävs genom att mottagarlandet inte efterlever GDPR är SCC därmed inte en lämplig skyddsåtgärd och kan inte användas.

Att genomföra en utredning av andra länders integritetsskydd och övervakning är krävande och kostsamt. EDPB, den europeiska dataskyddsstyrelsen har därför tagit fram rekommendationer[51,52] för den som exporterar respektive importerar personuppgifter till tredjeland, i syfte att underlätta tolkningen av GDPR. Vägledningen innehåller sex steg som ska följas och dokumenteras av alla som exporterar personuppgifter (oavsett de är personuppgiftsansvariga eller -biträden) när de utvärderar mottagarlandet och identifierar eventuella ytterligare skyddsåtgärder. Objektiva bedömningar måste göras utifrån mottagarlandets lagstiftning och hur denna i praktiken tillämpas. Om bedömningen kommer fram till att lagstiftningen i mottagarlandet i praktiken tillämpas på ett problematiskt sätt måste överföringen upphöra, alternativt bör ytterligare skyddsåtgärder vidtas för att motverka riskerna med överföringen[53]. *Oavsett vilka skyddsåtgärder som vidtas måste en skyddsnivå likvärdig den som uppställs av GDPR kunna garanteras vid överföring till tredje land. Överföringar som sker med stöd av SCC ska avbrytas eller förbjudas om klausulerna inte i praktiken kan efterlevas.*

---

[47] vid sidan om den tidigare tillämpliga Privacy Shield

[48] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/lampliga-skyddsatgarder/

[49] Schrems II-domen i denna del avser överföring till tredje land – inte enbart USA (som är fallet med Privacy Shield).

[50] EU-domstolen fann i Schrems II-domen att SCC i och för sig är giltiga, men att giltigheten är avhängig av att de aktuella parterna till standardavtalet (den part som exporterar uppgifter till tredje land och den part som importerar uppgifter från EU) i varje enskilt fall ska säkerställa att överföringen sker på ett lagligt sätt. SCC är dock enbart bindande för parterna som skrivit på dem. Myndigheter i det tredje landet är alltså inte part, och därför måste man bedöma om lagstiftning i det mottagande landet kan medföra att säkerheten för personuppgifterna verkligen upprätthålls.

[51] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

[52] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_sv

[53] I rekommendationerna anges att sådana ytterligare skyddsåtgärder kan vara pseudonymisering eller stark kryptering och teknisk lagring där endast myndigheten förfogar över krypteringsnyckeln Sid 30, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

9.4 Sammanfattande kommentar

Det oklara rättsläget innebär att det råder osäkerhet kring flera delar av lagligheten avseende användning av molntjänster och det ställs höga krav på en region som vill anlita en molntjänst-leverantör att utreda frågor kring laglighet, lämplighet och säkerhet. Att anlita en svensk molntjänst-leverantör borde, efter sedvanlig menprövning, inte vara några problem då molntjänstleverantören numera omfattas av en straffsanktionerad tystnadsplikt.

Om molntjänstleverantören är ett europeiskt eller ett bolag i tredje land med adekvat skyddsnivå (enligt beslut av kommissionen) är det inte lika självklart att kunna anlita detta, även om man vid en menprövning kommer fram till att uppgifterna kan lämnas ut. Detta eftersom det är oklart om den lagstadgade tystnadsplikten är tillämplig. Det skulle eventuellt kunna underlätta ett utlämnande om de anställda hos molntjänstleverantören omfattas av en straffsanktionerad tystnadsplikt enligt hemlandets lagstiftning.

Om molntjänstleverantören är ett bolag i tredje land som enligt EU inte anses ha adekvat skyddsnivå och som omfattas av en lagstiftning som kan innebära en skyldighet att lämna ut uppgifter till hemlandets myndigheter utan att behöva begära internationell rättshjälp, blir det problematiskt att anlita leverantören. Det skulle kunna innebära sanktionsavgifter från IMY eller att registrerade riktar skadeståndsanspråk mot regionen. En möjlighet kan vara att kryptera data och att endast regionen har tillgång till krypteringsnyckeln[54]. Lagring av data på en server inom EU ses däremot inte som en tredjelandsöverföring så länge inte någon teknisk fjärråtkomst sker från tredje land[55]. Frågan huruvida amerikanska myndigheter någon gång i framtiden skulle kunna begära ut uppgifter som ligger på servrar inom EU, men som tillhör ett amerikanskt bolag, ska ses som en tredjelands-överföring har inte prövats och rättsläget är oklart. Utifrån EDPB:s riktlinjer torde det inte ses som en tredjelandsöverföring, men i en situation där ett utlämnande enligt CLOUD Act skulle ske skulle det sannolikt vara i strid med GDPR. Av den anledningen kan risken av framtida utlämnande behöva beaktas av personuppgiftsansvarig vid valet av molntjänstleverantör.

I 10 kap 2 § OSL finns en bestämmelse om nödvändigt utlämnande, som bryter sekretessen då en uppgift lämnas till enskild eller en annan myndighet om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Av förarbetena framgår att bestämmelsen ska tillämpas restriktivt, se tex JO-beslutet från 2014, där det enligt JO i praktiken handlar om situationer av undantagskaraktär. Se också avsnitt ”Utredning om utkontraktering”, kapitel 8, och förslaget om införande av ny bestämmelse i 10 kap OSL.

[54] Se EDPB:s rekommendationer 01/20 om tredjelandsöverföring, 18 Juni 2021, bilaga 2.
[55] Se EDPB guidelines 05/2021

10 Olika aktörers vägledningar

Nedan följer exempel på vägledningar och rekommendationer från olika aktörer.

10.1 SKR tillhandahåller övergripande vägledning

Vad gäller kommunernas och regionernas användning av molntjänster har SKR tagit fram en vägledning[56] men på grund av den rådande rättsliga osäkerheten gällande förutsättningar för användning av molntjänster samt olika synsätt och tolkningar hos kommuner och regioner bedömer SKR att det för närvarande inte är möjligt att lämna generella rekommendationer utöver viss övergripande vägledning. Man överlämnar analys och riskbedömningar till de enskilda offentliga verksamheterna men rekommenderar en försiktighetsprincip vid användning av molntjänster för känsliga personuppgifter och information som omfattas av sekretess[57]. Med hänvisning till den kritik som riktats mot eSams uttalanden kan nämnas att SKR valt att inte stå bakom eSams uttalanden. I stället publicerade SKR ett eget ställningstagande om molntjänster[58] där SKR bland annat menar att det måste finnas utrymme för kommuner och regioner att göra en själv-ständig bedömning av risker när molntjänstleverantörer används. I en debattartikel i Dagens industri i maj 2021[59] uppmanade SKR regeringen att ta ansvar för att tydlighet ges i det osäkra rättsläge som råder kring frågan offentliga aktörers användning av molntjänster.

Även Adda (före detta SKL Kommentus), som ägs av SKR, har viss dokumentation på sin hemsida, främst här kopplat till Upphandling av ramavtal Programvaror och molntjänster 2019[60]. Adda har också nyligen beslutat att inte förlänga sitt volymavtal för programvara med Microsoft, detta till följd av att man bedömt att personuppgiftshanteringen inte kunnat regleras eller kartläggas[61].

10.2 Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (före detta Dataskyddsinspektionen), IMY, tillhandahåller information och vägledning om molntjänster och personuppgiftsbehandling inom vården.

- Överföring till tredje land (https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/)
- Schrems II-domen och överföringar till tredje land (https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/schrems-ii-domen-overforingar-till-tredje-land/)
- Personuppgiftsbehandling inom vården | IMY (https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/vard/)
- Vårdgivares skydd för patientuppgifter |IMY (https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/vard/vardgivares-skydd-for-patientuppgifter/)

---

56 https://skr.se/download/18.4d3d64e3177db55b1663107c/1615462780595/Molntj%C3%A4nster%20v%C3%A4gledning%20Cloud%20Act%20191025%20LI%20slutlig.pdf
https://skr.se/download/18.4d3d64e3177db55b1663107e/1615462780788/Molntj%C3%A4nster%20i%20verksamheten_191104_slutlig%20LI%20191104_rev%20191111.pdf

57 https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/molntjanster.7559.html

58 https://skl.se/tjanster/press/nyheter/nyhetsarkiv/molntjansternodvandigaforfortsattdigitalisering.27627.html

59 skr.se/skr/tjanster/press/skridebatten/debattartiklar/debattartiklar/dodlagetkringmolnethindrarvalfardensutveckling.53434.html

60 hadda.se/upphandling-och-ramavtal/vara-ramavtal-och-upphandlingar/ramavtal-och-avtalskategorier/programvaror/programvaror-och-molntjanster-2019/#t-1

61 adda.se/aktuellt/adda-inkopscentral-tackar-nej-till-nytt-volymavtal-med-microsoft/

Sommaren 2021 kom IMY med ett samrådsyttrande där man avråder från att verksamheter använder Microsofts populära molntjänster Azure AD och Teams[62]. IMY motiverar avrådan med att Microsoft bland annat kan komma att överföra personuppgifter till USA och de risker som detta innebär för enskildas personliga integritet. Förhandssamrådet med Stockholm Stad är inte publikt men det går att kontakta IMY vid önskan att begära ut det.

10.3 Europeiska Dataskyddsstyrelsen

Den Europeiska Dataskyddsstyrelsen, EDPB, har med anledning av Schrems II publicerat flera vägledningar och rekommendationer[63] på skyddsåtgärder vid överföring av personuppgifter utanför EU/EES, det senaste från juli 2021. Läs närmare om dessa under avsnitt ”Standardavtalsklausuler för överföring till tredje land”.

11 Enskilda bedömningar i regionerna

SKR har som nämnts ovan lämnat åt kommuner och regioner att utifrån sina förutsättningar och möjligheter själva gå igenom, utvärdera, göra egna riskbedömningar och vidta nödvändiga åtgärder vid användning av leverantörstjänster och produkter som genererar data som lagras i molnet. Då det i flera delar saknas ytterligare vägledning från tillsynsmyndigheter och domstolar råder viss osäkerhet i hur bedömningen av skyddet av personuppgifter i tredje land ska göras och vilka skyddsåtgärder som eventuellt kan väga upp brister i skyddet.

En effekt av att överlåta genomförandet av egna riskvärderingar på regionerna, liksom att enskilda regioner själva tolkar lagrum och tar fram egna vägledningar och riktlinjer kring användning av molntjänster, är att det ökar osäkerheten och minskar förutsägbarheten för såväl offentlig sektor som för leverantörer. I dagsläget finns ingen harmonisering regionerna emellan avseende processer och utvärderingar. Att det ser så olika ut bland Sveriges regioner och kommuner gör det komplicerat för leverantörer till offentlig sektor att tillhandahålla produkter och tjänster vilket i förlängningen riskerar att skapa en ojämlik vård för patienter i olika delar av landet. Många leverantörer till hälso- och sjukvården är multinationella företag som har svårt att skräddarsy enskilda lösningar för en så, relativt sett, liten marknad som Sverige och ännu mer komplicerat är det att skräddarsy olika kundanpassade tekniska lösningar för enskilda regioner/kommuner.

En uppfattning är att variationerna kring tolkning av rättsläget mellan de olika regionerna har minskat efter Schrems II-avgörandet samt de efterföljande vägledningar som tagits fram av EDPB. Regionerna ser relativt lika på vad som står i lagen och hur den ska tolkas men skiljer sig i benägenhet att ta risker; två olika sjukhus kan komma fram till att något inte är förenligt med GDPR, men ett av dem väljer att ta risken att göra fel i väntan på antingen ytterligare vägledning eller riktlinjer eller konsekvenser av ett felaktigt agerande, medan det andra sjukhuset väljer att avstå fram tills att man eventuellt finner en alternativ lösning. Utan ytterligare vägledning från tillsynsmyndigheter eller domstolar är det svårt att med säkerhet veta vilka skyddsåtgärder som bör vidtas. Variationerna resulterar i en begränsning av implementering av molntjänster och produkter innefattande molntjänstlösningar. I vissa regioner upphandlas idag enbart själva produkten och inte själva molnlösningen som behövs för vissa funktioner. Det kravställs således inte kring molntjänsten, i stället blir det en fråga som hanteras efter tilldelning.

[62] https://techlaw.se/sverige-imy-avrader-fran-anvandning-av-microsofts-molntjanster-azure-ad-och-teams/
[63] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/schrems-ii-domen-overforingar-till-tredje-land/

11.1 Region Stockholm

Det finns inga styrande dokument tillgängliga för nedladdning för leverantörer/anbudsgivare. Regionen hänvisar till de dokument som tillhandahålls av SKR liksom till den information som finns på IMY:s hemsida.

11.2 Region Östergötland

Regionen tillhandahåller inga vägledningar till leverantörer/anbudsgivare. Inom ramen för Innovationsmotorprojektet togs det 2019 fram en rapport, ”Ekosystem för E-hälsa - En juridisk genomlysning av hemmonitorering i hälso- och sjukvården”[64], med en genomlysning av informationssäkerhetskrav och de juridiska förutsättningarna för hemmonitorering i hälso- och sjukvården. Rapporten innehåller bedömningar och förslag på aktiviteter som en region bör vidta för att säkerställa följsamheten mot tillämplig lagstiftning. Förutom konkreta åtgärdsförslag, finns även en allmän redogörelse för tillämplig lagstiftning på området samt allmänna principer enligt GDPR som en region har att iaktta vid behandling av personuppgifter. I den juridiska genomlysningen beskrivs också JO-utlåtandet från 2014 och det rättsliga uttalandet av eSam från 2018. I rapporten anges att en region bör kravställa att en leverantör, som behandlar personuppgifter i tredje land på uppdrag av regionen, använder sig av till exempel standardavtalsklausuler eller är anslutna till Privacy Shield för att uppnå en adekvat skyddsnivå för uppgifterna. De legala förutsättningar för tredjelandsöverföringar har förändrats sedan rapporten togs fram vilket måste beaktas vid genomgång och tillämpning av informationen i rapporten.

11.3 Region Halland

Regionen tillhandahåller inga vägledningar till leverantörer/anbudsgivare. Regionen har tagit fram en handbok för informationsdriven vård som behandlar olika områden som påverkar vårdens omställning till att nyttja patientdata[65]. Det finns där bland annat ett avsnitt beträffande juridiken kring hanteringen av patientdata.

11.4 Region Skåne

Regionen tillhandahåller inga vägledningar till leverantörer/anbudsgivare. Instruktioner till medarbetare inom Region Skåne som hanterar dokument och behöver vägledning i val av systemstöd innefattar att risker och konsekvenser noggrant ska övervägas innan molntjänster används i Region Skåne, oavsett vilken information som ska hanteras i tjänsten. Beslut om att hantera information i en molntjänst ska fattas av informationsägaren och ska alltid föregås av informationsklassificering och riskanalys i enlighet med Region Skånes instruktioner[66].

Av hög relevans för det aktuella rättsläget är det arbete som pågår i Region Skåne avseende riskanalys och externa utlåtanden kring datahanteringen i Skånes digitala vårdsystem, SDV. SDV är ett nytt sammanhållet journalsystem för såväl slutenvården som primärvården där all digital vårdinformation hamnar på en och samma plattform. Region Skåne har köpt it-systemen Millennium och Health Intent från bolaget Cerner Sverige AB.

Satsningen har drabbats av förseningar bland annat på grund av riskerna kring datahanteringen i SDV. Både Region Skåne och Cerner har skaffat sig självständiga utlåtanden från oberoende advokatfirmor rörande hanteringen av känsliga personuppgifter och frågor rörande sekretess på patientdata

[64] https://vardgivarwebb.regionostergotland.se/pages/377873/Ekosystem%20e-H%C3%A4lsa%20En%20juridisk%20genomlysning%20av%20hemmonitorering%20i%20h%C3%A4lso-%20och%20sjukv%C3%A5rden.pdf
[65] https://www.ai.se/en/news/printed-handbook-information-driven-and-ai-ready-healthcare
[66] https://vardgivare.skane.se/siteassets/4.-uppdrag-och-avtal/arkiv/skapa---fillistning/krav-pa-systemstod-for-hantering-och-forvaring-av-digitala-dokument.pdf

som hanteras av företag utanför EU har utretts[67]. Kortfattat handlar frågorna bland annat om att data skickas till servrar utanför EU samt att driften av systemen sker i utlandet i och med att Cerner i Sverige ska anlita underbiträden i form av Cerner i USA och Cerner i Indien för teknisk drift och support av it-systemen. Därmed uppstår osäkerhet huruvida vårdinformation om svenska patienter blir tillgänglig för andra än svensk vårdpersonal. Med anledning av att regionen bedömt att det kvarstår en hög risk för behandling har regionen begärt förhandssamråd[68] med IMY.

11.4.1.1 IMY Råd 1 Rättsligt stöd för behandlingen

Mot bakgrund av det underlag som regionen inkommit med[69] råder IMY regionen att inte använda personuppgiftsbiträdena Cerner Indien och Cerner USA för den tilltänkta personuppgifts-behandlingen vid drift och support i Indien och USA av it-systemen. Detta eftersom IMY bedömer att det inte finns rättsligt stöd enligt artikel 9.2h i GDPR för att behandla känsliga personuppgifter hos dessa personuppgiftsbiträden, då kravet på tystnadsplikt i artikel 9.3 i GDPR inte är uppfyllt.

IMY för ett ingående resonemang kring kravet på tystnadsplikt i artikel 9.3 och vilka aktörer som omfattas av denna lagstadgade tystnadsplikt[70]. Artikel 9.3 innehåller inte någon uttrycklig begränsning av kravet på tystnadsplikt till behandling hos den personuppgiftsansvarige. IMY menar därför att bestämmelsens ordalydelse talar för att den även omfattar personuppgiftsbiträden. I Sverige regleras tystnadsplikten för det allmännas verksamhet inom hälso- och sjukvård i OSL. IMY konstaterar därför att villkoret gällande lagstadgad tystnadsplikt i artikel 9.3 i GDPR anses uppfylld för regionens egen hälso- och sjukvårdspersonal. Enligt bland annat JO-beslutet från 2014 (se avsnitt 6.1) omfattas inte personal hos de personuppgiftsbiträden som regionen anlitar av tystnadsplikt, se även 2 kap. 1 § andra stycket OSL.

IMY konstaterar att ett personuppgiftsbiträde som endast tekniskt bearbetar eller tekniskt lagrar uppgifter, såsom exempelvis drift och support av ett it-system, åt en myndighet, kan omfattas av tystnadspliktslagen (se kapitel 7). Av 4 § i lagen framgår att den som på grund av anställning eller på något annat sätt deltar i eller har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet endast tekniskt bearbeta eller tekniskt lagra uppgifter inte obehörigen får röja eller utnyttja dessa uppgifter. Av 3 § i samma lag framgår att med en tjänsteleverantör ska jämställas en underleverantör som medverkar till att fullgöra tjänsteleverantörens uppdrag. Tystnadsplikten enligt tystnadspliktslagen är straffsanktionerad enligt 20 kap. 1 § brottsbalken.

IMY anser emellertid att det råder osäkerhet om tystnadspliktslagens räckvidd vad gäller person-uppgiftsbiträden utanför Sveriges gränser. IMY konstaterar att tystnadspliktslagen inte innehåller någon uttrycklig reglering om lagens territoriella tillämpningsområde. Enligt IMY går det inte att utifrån förarbetena dra någon bestämd slutsats när det gäller i vilken utsträckning tystnadsplikts-lagen är avsedd att vara tillämplig i utlandet. Det framgår dock, enligt IMY att möjligheten att utöva svensk domsrätt vid överträdelser av tystnadsplikten utomlands är mycket begränsade[71]. IMY kan utifrån utredningen i ärendet inte heller dra någon slutsats om att det skulle finnas särskilda förutsättningar för detta i Indien eller USA.

---

[67] app.insiktmedicin.se/articles/752512?utm_campaign=DigitalH%C3%A4lsaPREMIUM_210510_Advokatbyr%C3%A5s%20second%20opinion%20tonar%20ned%20legala%20risker%20med%20SDV&utm_medium=email&utm_source=Eloqua&elqTrackId=0cb0000202ac418d8c3dd973875c962e&elq=b167913b4f3b4aff84b273c2deb97177&elqaid=41677&elqat=1&elqCampaignId=30685

[68] Samrådsyttrande diarienummer: DI-2021-2983 är inte publikt men det går att kontakta IMY vid önskan att begära ut det.

[69] Samrådsyttrandet, s. 3.

[70] Samrådsyttrandet s.12 ff.

[71] Prop. 2019/20:201 s. 20.

Eftersom IMY anser att regionen saknar rättsligt stöd för behandlingen av känsliga personuppgifter hos personuppgiftsbiträdena i Indien och USA konstaterar IMY att det saknas anledning för myndigheten att gå vidare till bedömningen av om en överföring till tredjeland är möjlig eller inte. IMY lyfter brist på vägledande praxis från domstol eller vägledning från EDPB om tolkningen av artikel 9.3 i GDPR och den aktuella situationen visar på vikten av att tystnadsplikten och frågan vilka som omfattas av den behöver utredas vidare. IMY ger därför regionen ytterligare ett råd avseende den planerade överföringen av personuppgifter för drift och support i tredjeland.

11.4.1.2 IMY Råd 2 Överföring till tredje land

IMY råder regionen att utreda tredjelands lagstiftning ytterligare. För det fall regionen efter utredningen kommer fram till att sektion 702 i Foreign Intelligence Surveillance Act (FISA), eller liknande lagstiftning som bedöms gå utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle, blir eller kan tänkas bli tillämplig på överföringen och/eller personuppgifts-biträdena i USA och Indien, och om behandlingen av personuppgifter kan komma att ske i klartext vid utförandet av drift och support av it-systemen i dessa länder, bör regionen inte gå vidare med behandlingen.

Region Skåne har, utöver att ingå personuppgiftesbiträdesavtal med underbiträdena för behandlingen av personuppgifter, också avsett att tillämpa EU-kommissionens standardavtals-klausuler, sekretessavtal och vidta ett antal tekniska, organisatoriska och avtalsmässiga säkerhetsåtgärder vid behandlingen.

Det råder idag stor osäkerheten bland offentliga och privata aktörer, vars tjänster och produkter lagrar hälsodata i molnet, kring vilka ytterligare säkerhetsåtgärder som bör vidtas för att kunna säkra hanteringen av hälsodata. IMY:s förhandsråd ger en god vägledning men det finns anledning att vara försiktig med att rakt av applicera IMY:s avrådan om att inte anlita utländska underbiträden på användning av molntjänster för lagring av patientdata i medicintekniska produkter. Detta bland annat eftersom användningen av molntjänster typiskt sett inte alltid innebär att anställda hos molntjänstleverantören tar del av kundernas uppgifter på det sätt som sker i det aktuella ärendet. Även om det finns anställda hos molntjänstleverantören som rent tekniskt kan komma åt uppgifterna finns det ofta instruktioner och organisatoriska åtgärder (tilldelning av åtkomsträttigheter, interna rutiner, instruktioner och riktlinjer) och tekniska säkerhetsåtgärder (exempelvis kryptering, pseudonymisering, behörighetsspärrar, inloggning) som begränsar denna åtkomst. Skillnaderna i detta hänseende skulle kunna påverka bedömningen. För att inte hindra de för vården helt nödvändiga dataflöden mellan Sverige, EU och länder som till exempel USA och Indien behöver regionerna liksom industrin tydligare vägledning i säkerhets- och riskutvärdering av hur mottagarlandet skyddar personuppgifter.

11.5 Västra Götalandsregionen

Regionen tillhandahåller inga vägledningar till leverantörer/anbudsgivare. Även Västra Götalands-regionen har upphandlat systemet Millennium, men uppger att drift inte kommer att ligga utomlands. Däremot finns viktiga funktioner som i nuläget kräver molntjänster utomlands. Inspektionen för vård och omsorg (Ivo) har inlett en granskning av informationssäkerheten[72].

[72] https://lakartidningen.se/aktuellt/nyheter/2021/05/ivo-granskar-millennium-i-skane-och-vastra-gotaland/

12 Det osäkra rättslägets effekt på medtechindustrin och hälso- och sjukvården

I denna rapport beskrivs en nulägesbild av det osäkra rättsläget kring förutsättningarna för offentlig sektor att upphandla privata molntjänstleverantörer. Vid sidan om frågan huruvida användning av molntjänster kan stå i strid med OSL har Schrems II-domen skapat rättslig osäkerhet kring överföringar av personuppgifter från EU till USA. Osäkerheten riskerar att bromsa digitala satsningar och domen har fått betydande konsekvenser för svenska företag och myndigheter. I slutändan är det hälso- och sjukvården, dess anställda men främst patienterna som påverkas eller blir lidande om överföring av personuppgifter mellan EU och USA försvåras eller hindras. Nyttjande av molntjänster är helt centralt för vårdens och omsorgens digitala utveckling och naturligtvis måste det ske på ett sätt som är lämpligt, lagligt och förenligt med en god informationssäkerhet.

Bild: BVMed

Fortsatt möjlighet till överföring av hälsodata avgörande för forskning, innovation och utveckling av nya medicintekniska produkter, för uppföljning av säkerhet och effektivitet av produkter som är satta på marknaden samt för tillhandahållandet av supporttjänster för medicintekniska produkter som används av patienter och brukare. Det finns en överhängande risk att patienter i drabbas i onödan om transatlantiska dataöverföringar begränsas eller hindras. Under tiden arbetet pågår med att ta fram en efterträdare till Privacy Shield måste säkerställas att dataöverföring mellan EU och USA inte förhindras. Genom att tillämpa de skyddsåtgärder som står till buds, och som också lagstiftning ställer krav på, kan man minimera eventuella integritets- och säkerhetsrisker.

I Schrems II-domen uttalade EU-domstolen oro för att Cloud Act kan ge amerikanska myndigheter tillgång till data som förs över från EU till USA. Syftet med Cloud Act och målet med underrättelse-tjänstövervakning är att ge amerikanska myndigheter tillgång till information från individer utbytt mellan individer[73]. Det finns däremot inga rapporterade fall där Cloud Act faktiskt har använts för att kräva ut data från en molntjänst som innehållit data som överförts för service eller forskning och utveckling av läkemedel eller medicintekniska produkter. Genom att använda sig av nyckelkodad information, där direkt identifierbara data skyddas/hålls konfidentiell med en kod som hålls skyddad är data inte längre identifierbar för amerikanska underrättelsetjänster för att identifiera kommunikation av intresse (t.ex. namn, adress, telefonnummer, epostadress etc.). Data kopplad till biverkningar, olyckor och tillbud liksom produktsäkerhet hanteras oftast inom regioner men kan av rapporterings- och analysskäl behöva behandlas och hanteras över nationsgränser. I en sådan situation ska så lite data som bara är möjligt behandlas (uppgiftsminimering) och även här är patient-informationen mycket sällan direkt identifierbar. Kraven som ställs i GDPR på tillverkare av medicin-teknisk utrustning för att skydda patientdata från obehörig åtkomst är höga och säkerhetsåtgärder inkluderar vanligtvis kryptering och höga autentiseringskrav för användaråtkomst. Det finns mycket sällan behov av att överföra direkt identifierbar patientinformation. Tjänster för monitorering av patienter kan kräva överföring av mer direkt identifierbar information, men då krävs att patienterna informeras och samtycker till dessa överföringar. Sammanfattningsvis finns det aspekter som talar för att dessa dataflöden inte utgör de typer av integritetsrisker som tas upp i Schrems II-domen.

[73] https://www.congress.gov/bill/115th-congress/house-bill/4943

12.1 Beskrivande case

IBD Home är en eHälsolösning som ska underlätta vardagen för personer som lever med inflammatorisk tarmsjukdom, IBD, genom möjligheten att kunna monitorera sjukdomen från hemmet. Patienterna tar prover och rapporterar direkt in till sjukhuset hemifrån via ett självtest och applikationer. IBD Home följer upp IBD-patienter och kopplar till riktlinjer och möjlig behandling. Patienten knappar själv in sin data som går direkt in till både ett eget konto och till kvalitetsregistret SWIBREG[74]. Sjuksköterskor kan via SWIBREG se hur värden ligger och får utifrån ”trafikljus” stöd att avgöra patientens status. Uppkoppling mot appen har gett mycket bättre täckningsgrad i registret. Och data från registret används som ett beslutsstöd för IBD-patienter och deras vårdgivare.

IBD Home utvecklades i samarbete mellan svenska specialister på mag- och tarmsjukdomar, Mag- och tarmförbundet, det nationella kvalitetsregistret SWIBREG, Telia, AbbVie och företaget bakom det hembaserade testet av inflammationsmarkören, Bühlmann. Idag äger Telia lösningen och de har ansvar för CE-märkningen. Lösningen har testats i flera olika pilotprojekt, bland annat i Västra Götalandsregionen[75]. En rapport framtagen från projektet visade att antalet läkarbesök sjönk i genomsnitt med 18% vid anslutning till IBD Home, vilket representerar en genomsnittlig minskning med ett läkarbesök hos knappt varannan patient och år. För hela VGR minskade akuta inläggningar med 32%.

Även i Region Uppsala startades en pilot. Regionen efterlyste en hemmonitoreringslösning som kunde följa patienterna i deras vardag. En pilot startades i det så kallade PHM-projektet (Patientens hemmonitorering), men stoppades då man stötte på hinder rörande molntjänster. I regionen upptäcktes att de inte fick nyttja amerikanskägda lösningar och IBD Home kördes då på en IBM-lösning. Det ser mycket olika ut i olika regioner om lösningen har implementerats efter pilotstadiet eller inte. Det finns fortfarande inga ersättningsmodeller för denna typ av lösning och tolkningen av juridiken varierar.

”Vi som kund och kravställare har varit omogna i hur man ska tolka reglerna och vilka krav som ska ställas.”

Projektledare pilotprojektet

Den medicintekniska produkten AsthmaTuner består av en trådlös spirometer med tillhörande mobilapplikation för patienten för egenkontroll och behandling av astma, samt ett webbgränssnitt som möjliggör för vårdpersonal att ta del av den information som patienten registrerat. I slutet av 2019 beslutade Tandvårds- och Läkemedelsförmånsverket (TLV) att AsthmaTuner som första digitala verktyg för behandling av astma skulle ingå i subventionen för barn med okontrollerad astma. Då det inte ingår i TVL:s mandat att granska frågor om informationshantering och säkerhet, behandlades denna fråga av NT-rådet[76]. I ett yttrande den 20 februari 2020 rekommenderade NT-rådet att regionerna skulle avvakta användning av AsthmaTuner tills frågor om juridik, informationshantering,

[74] Swedish Inflammatory Bowel Disease Registry, https://www.swibreg.se/
[75] https://www.vgregion.se/halsa-och-vard/vardgivarwebben/vardskiftet/utvecklingsarbete/ibd-home/
[76] https://www.janusinfo.se/nationelltinforandeavlakemedel/saarbetarvi/rollerochkontaktuppgifter/roller/ntradetnyaterapier.5.4771ab7716298ed82ba5e87.html

informationssäkerhet och organisering av vårdverksamhet hade utretts[77]. En juridisk vägledning togs fram av SKR. Den rättsliga analysen tittade man främst på att den juridiska lösningen som AsthmaTuner bygger på, den ansågs inte ändamålsenlig ut ett dataskyddsperspektiv eller ett individ-perspektiv. Lösningen ansågs skapa osäkerhet om personuppgiftsansvaret men slutsatsen var ändå att regionerna kunde ta tjänsten i anspråk villkorat att AsthmaTuner modifierade sin lösning gällande personuppgiftsansvaret.

En annan fråga rörde möjligheterna för hälso- och sjukvården att använda molntjänster för hantering känsliga personuppgifter. Skyddet bedömdes som lämpligt i relation till bl.a. arten av person-uppgifter, sammanhanget och ändamålet. AsthmaTuner förfogar själv enligt uppgift över krypto-nycklarna för den krypterade data som lagras i molnet. Uppgifterna bedömdes därför juridiskt sett inte kunna anses röjda för molntjänstleverantören eftersom denne, i den aktuella lösningen, inte förfogar över lagrade data. Sommar 2021 gick AsthmaTuner ut med information om att man för att ytterligare stärka tryggheten väljer en svensk molntjänstleverantör, vilket innebär att lagring och hantering av personuppgifter i AsthmaTuner kommer att ske fysiskt inom Sveriges gränser och regleras av svensk lagstiftning[78].

13 Avslutande kommentarer

För alla aktörer involverade i hälso- och sjukvård och omsorg och utvecklingen av densamma, är behovet av utbyte av data stort och internationella dataflöden centrala. En mer datadriven vård och ett ökat informationsflöde mellan vårdgivare, vårdtagare och tjänsteleverantörer kommer krävas framöver för fortsatt leverans av god vård.

Frågan kopplad till Schrems II-domen måste lösas på politisk nivå. På samma sätt som när det tidigare regelverket Safe Harbour ogiltigförklarades av EU-domstolen[79] måste nu Privacy Shield-regelverket omförhandlas och ersättas med ett nytt regelverk. Det pågår[80] direkta förhandlingar mellan EU och USA om vad man kallar ”ett förbättrat Privacy Shield-ramverk” men det ser ut att komma att dröja innan vi eventuellt har nytt regelverk på plats. Fram tills en politisk och juridisk lösning för dataflöden kommer på plats måste pågående transatlantiska dataöverföringar säkras för att inte riskera hindra införande av innovationer i vården och fördröjd, ojämlik vård och sämre tillgång till digitala lösningar för patienter och vården.

Industrin och regionerna behöver omgående stöd och vägledning i riskutvärdering av hur mottagar-landet skyddar personuppgifter och det vore högst önskvärt att EDPB och IMY tog fram tydliga rekommendationer och gemensamma riktlinjer på europanivå, samtidigt som en harmonisering i regionernas arbete är eftersträvansvärt för att underlätta för vårdorganisationernas användande av molntjänster utan att riskera säkerheten. Vidare skulle det, som IMY också lyfter i samråds-yttrandet[81], behövas tydlighet i vilken utsträckning tystnadspliktslagen är avsedd att vara tillämplig i utlandet och möjligheterna att utöva svensk domsrätt vid överträdelser av tystnadsplikten utomlands, inom respektive utanför EU:s gränser.

Den nationella life science-strategin har som mål att Sverige ska vara en ledande life science-nation. Regeringens intentioner att Sverige ska ha världens bästa sjukvård för alla, kräver införande av fler

[77] Se Vägledning avseende AsthmaTuner ur ett informationshanterings- och dataskyddsperspektiv, https://janusinfo.se/download/18.d7dd17917250a7462823f2a/1590644388737/V%C3%A4gledning%20avseende%20AsthmaTuner%20ur%20ett%20informationshanterings-%20och%20dataskyddsperspektiv.pdf
[78] https://asthmatuner.se/2021/06/08/asthmatuner-valjer-en-svensk-molnleverantor-for-framtida-expansion/
[79] https://www.nyteknik.se/digitalisering/eu-domstolen-safe-harbor-ogiltigt-6344294
[80] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443
[81] Samrådsyttrandet s.14.

digitala tjänster och lösningar i vården. För att vården ska vara rustad i frågan om informationsteknik och digitalisering måste möjlighet och medel ges till vården att satsa på robusta it-system och anställa de allra bästa experterna som besitter den kunskap som krävs för att Sverige ska kunna leva upp till ställda mål.

Vi vill med denna skrivelse också lyfta de många lösningar som Swedish Medtechs medlemsföretag besitter. Vi deltar gärna i en dialog för att utveckla vården att bättre kunna hantera och motverka den pågående pandemin, men också i det nödvändiga arbetet att skapa en beredskapsplan för nästa stora samhällskris. Utmaningarna vid införande av digitala lösningar i vården kan lösas i nära samverkan med industrin.

Med den här rapporten vill vi ge en ögonblicksbild av rådande rättsläge. Framtagandet inom ramarna för det nationella projektet Innovationsmotorer, som har som mål att höja takten på utvecklingsarbetet i vården. Syftet med projektet är att bättre använda den kunskap och erfarenhet som finns i sjukvården för att stärka sektorns roll som motor för utveckling av nya metoder och produkter. Innovationsmotorprojektet finansieras av det strategiska innovationsprogrammet Medtech4Health, i sin tur finansierat av Vinnova, Energimyndigheten och Formas. Programmet syftar till att vara en katalysator för fler medicintekniska idéer i vården, en effektiviserad hälso- och sjukvård samt en stärkt medicinteknisk industri. Rapporten kommer löpande att uppdateras. Kontakta oss gärna om du har frågor eller funderingar kring innehållet i rapporten, https://www.swedishmedtech.se/sidor/kontakta-oss.aspx.

Om Swedish Medtech och medicinteknikbranschen

Swedish Medtech är branschorganisationen för de medicintekniska förtagen i Sverige. Medicinteknikföretagen är heterogena vilket återspeglar sig i en stor variation av produkter. Det finns produkter inom röntgen, ortopediska implantat, minimalinvasiv kirurgi, pacemakers, dialys, hjälpmedel för funktionshindrade, journalsystem samt förbrukningsartiklar. Vissa medlemsföretag har egen tillverkning medan andra är distributörer. I Sverige finns idag runt 640 medicintekniska bolag med fler är 4 anställda. 2013 bedrev 180 av dessa företag forskning och utveckling i Sverige. Därutöver finns ett stort antal företag med 1–4 anställda. Den medicintekniska industrin arbetar med ständig utveckling och har under flera år varit den bransch som registrerat flest patent på europanivå, vilket inneburit över 13 000 patent årligen. Exporten för medicinteknikbolagen har ökat under 2000-talet med en topp 2010 för att sedan gå ner till att 2018 vara på drygt 20 miljarder svenska kronor.

Den medicintekniska branschen anställer idag ca 25 000 personer, vilket gör medicinteknikföretagen till den del inom life science-branschen med flest anställda. Den svenska marknaden för medicintekniska produkter och tjänster består till största delen av offentliga kunder såsom kommuner och regioner. Många av Swedish Medtechs medlemsföretag har därmed endast möjlighet att föra ut sina produkter på marknaden genom att delta i offentliga upphandlingar. En stor andel av företagens forskning och utveckling genomförs i samverkan med hälso- och sjukvården. Detta har lett till en rad nya produkter och framgångsrika innovativa behandlingsmetoder som kommit till nytta i vården och förbättrad livskvalitet för patienter.

14 Bilagor

14.1 Tillverkarens/Leverantörens ansvar

Tillverkare av medicintekniska produkter har enligt den medicintekniska förordningen, MDR, en skyldighet att säkerställa att produkterna är säkra och effektiva, och att övervaka användningen av produkterna på marknaden för att säkerställa patientsäkerheten. Produkter och processer ska noggrant dokumenteras för att trygga patientsäkerhet och minimera risker kring användning liksom att säkra att produkterna har utlovad effekt vid användning. För att uppfylla regelverket ska tillverkare ha en process för insamlande av eftermarknadsinformation. Vid eventuella avvikelser ska information och data samlas in på ett strukturerat sätt och delas relevanta tillsynsmyndigheter i de länder där produkten marknadsförs och säljs. När den gemensamma databasen EUDAMED är på plats kommer denna rapportering att ske i den.

14.2 Andra aktörers arbete och intressanta länkar

- Aida Data Sharing Policy: https://datahub.aida.scilifelab.se/sharing/
- Sweper: https://swelife.se/wp-content/uploads/2021/06/sweperboken_finalversion.pdf

14.3 Några begrepp och definitioner

ADDA	(Tidigare SKL kommentus) Verksamhetsstöd till offentlig sektor, ägs av SKR
CLOUD Act	The Clarifying Lawful Overseas Use of Data Act
Dataskyddslagen	Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
EDPB	Europeiska dataskyddsstyrelsen (European Data Protection Board) ett oberoende europeiskt organ som bidrar till en enhetlig tillämpning av dataskyddsreglerna inom hela EU/EES samt främjar samarbetet mellan de nationella dataskyddsmyndigheterna.
eSam	eSamverkansprogrammet
GDPR	EU:s dataskyddsförordning (General Data Protection Regulation), Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
IaaS	Infrastructure as a Service
IMY	Integritetsskyddsmyndigheten (tidigare dataskyddsmyndigheten)
JO	Riksdagens ombudsmän eller Justitieombudsmannen
NIS	lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
NIS 2	Reviderat förslag på ett nytt NIS-direktiv
NIST	National Institute of Standard and Technology
OSL	offentlighets- och sekretesslagen (2009:400)
PaaS	Platform as a Service
PDL	patientdatalagen (2008:355)
Personuppgiftsansvarig	fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt, se dataskyddsförordningen art 4:7
Personuppgiftsbiträde	fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

	personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ, se dataskyddsförordningen art 4:8
Personuppgiftsbiträdesavtal	Avtal enligt artikel 28 i GDPR
Privacy Shield	Överenskommelse om skydd för personuppgifter mellan EU och USA som träffades 2016
SaaS	*Software as a service* (mjukvara)
SCC	Standard Contractual Clauses (standardavtalsklausuler)
Schrems II-målet	EU domstolens dom den 16 juli 2020 i mål C311/18
SDV	Skånes digitala vårdsystem
SIS	Svenska institutet för standarder
SKR	Sveriges kommuner och regioner, arbetsgivarorganisation för alla kommuner och regioner
SSL	Säkerhetsskyddslagen ((2018:585)
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till europeiska ekonomiska samarbetsområdet (EES)
Tystnadspliktslagen	lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter
US	CLOUD Act Clarifying Lawful Overseas Use of Data Act
Vision eHälsa	Sverige har en vision för digitalisering i hälso- och sjukvården och socialtjänsten. År 2025 ska Sverige vara bäst i världen på att använda digitaliseringens och eHälsans möjligheter i syfte att underlätta för människor att uppnå en god och jämlik hälsa och välfärd samt utveckla och stärka egna resurser för ökad självständighet och delaktighet i samhällslivet.