Integritetsskydds myndigheten

Federerad maskininlärning mellan två vårdgivare

Slutrapport om Integritetsskyddsmyndighetens pilotprojekt med regulatorisk testverksamhet om dataskydd

Diarienummer
IMY-2023-2602

Datum
2023-03-15

Integritetsskydds myndigheten

Diarienummer:
IMY-2023-2602

Datum:
2023-03-15

Federerad maskininlärning mellan två vårdgivare – slutrapport från IMY:s pilotprojekt med regulatorisk testverksamhet

Innehåll

Sammanfattning 2

1. Inledning 4
   - 1.1 Regulatorisk testverksamhet – en form av försöksverksamhet 4
   - 1.2 Stor efterfrågan på stöd och vägledning i frågor som rör dataskydd 5
   - 1.3 Urval och arbetsprocess i pilotprojektet 6
2. Projektet Decentralized AI in Health Care – Federerad maskininlärning mellan två vårdgivare 7
   - 2.1 Kort om decentraliserad AI och projektet 8
   - 2.2 De rättsliga frågeställningarna i pilotprojektet 8
   - 2.3 Avgränsning i pilotprojektet 9
3. Finns det rättslig grund för den lokala personuppgiftsbehandlingen? 9
   - 3.1 Rättslig bakgrund 10
   - 3.2 Dialog med Socialstyrelsen 13
   - 3.3 IMY:s bedömning 14
4. Sker det vid den federerade maskininlärningen i det aktuella fallet ett utlämnande av personuppgifter mellan vårdgivarna? 15
   - 4.1 Beskrivning av tekniken i det aktuella projektet 16
   - 4.2 Två typer av möjliga attacker 17
   - 4.3 IMY:s bedömning 19
5. Finns det rättslig grund för utlämnande av personuppgifter mellan vårdgivarna? 20
   - 5.1 Rättslig bakgrund 21
   - 5.2 IMY:s bedömning 21
6. Reflektioner om att tillämpa dataskyddsregelverket på AI och annan ny teknik 22
7. Reflektioner om regulatorisk testverksamhet som arbetssätt 23

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Sammanfattning

- **Komplexa samhällsutmaningar kräver innovativa lösningar.** Sverige och EU står inför en mängd samhällsutmaningar där innovation och ny teknik kommer att vara avgörande. Innovationssystemet har en stark vilja att utveckla hållbara lösningar, men det är inte alltid enkelt att tillämpa befintlig reglering på ny teknik. För lagstiftaren och myndigheter som tolkar och tillämpar regelverken är det en utmaning att förstå och analysera den nya teknik som reglerna ska tillämpas på.

- **Det riskerar att bli ett gap mellan den snabba teknikutvecklingen och det mer trögrörliga arbetet med att ta fram, tolka och tillämpa regelverk.** Att utveckla nya arbetssätt i offentlig sektor är en viktig del av vägen framåt. Ett av de arbetssätt som diskuteras i sammanhanget är regulatorisk testverksamhet, ofta även kallat sandlåda eller *sandbox* på engelska. Det finns ingen allmänt vedertagen definition av vad arbetssättet innebär, men kärnan handlar om att innovatörer och till exempel tillsynsmyndigheter arbetar tillsammans för att tolka hur regelverk kan fungera i praktiken med innovativa produkter och tjänster.

- **Integritetsskyddsmyndigheten, IMY, har under hösten 2022 genomfört en pilot med regulatorisk testverksamhet.** IMY:s definition av regulatorisk testverksamhet är att vi ger fördjupad vägledning till ett specifikt innovationsinitiativ om hur dataskyddsregelverket bör tolkas och tillämpas. Kännetecknande för arbetssättet är att IMY tillsammans med den aktuella verksamheten identifierar de rättsliga frågor som vägledningen ska fokusera på. Vägledning ges därefter muntligt vid flera tillfällen under några månaders tid, i form av workshops eller andra dialogbaserade former. Arbetet utmynnar i en publik rapport där resonemang och bedömningar sammanfattas för att möjliggöra ett lärande för fler.

- **Projektet *Decentralized AI in Health Care – Federerad maskininlärning mellan två vårdgivare* är IMY:s första pilotprojekt.** Projektet handlar om att vårdgivarna Region Halland och Sahlgrenska Universitetssjukhuset vill utvärdera möjligheterna att gemensamt träna och utbyta maskininlärningsmodeller. Arbetet har skett med stöd av AI Sweden som är Sveriges nationella center för tillämpad AI. En informationsdriven vård, som i ökad utsträckning tar hjälp av AI, kan bidra till att beslut kan skräddarsys på individ- och systemnivå samt utveckla mer avancerade och träffsäkra diagnoser och behandlingar. I det specifika projektet är syftet att bättre kunna prediktera återinläggning av hjärtsviktspatienter inom 30 dagar från senaste sjukhusvistelsen med hjälp av federerad maskininlärning.

- **Federerad maskininlärning innebär att flera parter gemensamt tränar en maskininlärningsmodell utan att samla in data centralt.** Tekniken är den vanligaste formen av decentraliserad AI, som är ett nytt paradigm inom maskininlärning. I korthet innebär tekniken att parterna tränar varsin lokal maskininlärningsmodell med hjälp av sin egna data. I nästa steg kombineras lärdomarna ihop till en gemensam maskininlärningsmodell. Träningen upprepas därefter på den lokala datan. Ett skäl att använda federerad maskininlärning kan vara att parterna individuellt har otillräckligt med träningsdata. Vid utveckling av federerad maskininlärning är grundtanken att det inte ska ske någon överföring av personuppgifter mellan parterna.

- **Vägledningen i pilotprojektet har fokuserat på tre rättsliga frågeställningar** som Region Halland, Sahlgrenska Universitetssjukhuset, AI Sweden och IMY valt ut gemensamt. Utöver dessa tre frågeställningar finns andra juridiska frågor som

behöver beaktas men som inte analyserats inom ramen för den regulatoriska testverksamheten. Exempelvis behandlas inte hur de registrerades rätt till information eller principen om uppgiftsminimering ska tillgodoses.

- **Fråga 1. Finns det rättslig grund för den lokala personuppgiftsbehandlingen, det vill säga när vårdgivarna tränar maskininlärningsmodellen lokalt, enbart på sin egen patientdata?** IMY:s bedömning är här att det framstår som att det finns rättslig grund för den lokala personuppgiftsbehandlingen. Avgörande i sammanhanget är att IMY menar att det finns stöd för en dynamisk och teknikneutral tolkning av ändamålsbestämmelserna i patientdatalagen och hälso- och sjukvårdslagen, vilket innebär att vad som ryms inom dessa bestämmelser kan förändras över tid bland annat med hänsyn till teknikutvecklingen.

- **Fråga 2. Sker det vid den federerade maskininlärningen i det aktuella fallet ett utlämnande av personuppgifter mellan vårdgivarna?** Med hjälp av attackmetoder som kallas *Membership Inference Attack* och *Model Inversion Attack* skulle det vara möjligt, om än omständligt, för Region Halland eller Sahlgrenska Universitetssjukhuset att få fram personuppgifter från den andra parten. IMY:s bedömning är därför att Region Halland och Sahlgrenska Universitetssjukhuset i det aktuella fallet kan anses lämna ut personuppgifter till den andra parten i samband med att lärdomarna från den lokala träningen kombineras till en gemensam maskininlärningsmodell. Detta innebär dock inte att samma slutsats är giltig för alla former av federerad maskininlärning.

- **Fråga 3. Finns det rättslig grund för utlämnande av personuppgifter mellan vårdgivarna?** Om Region Halland och Sahlgrenska Universitetssjukhuset, som båda är myndigheter, med stöd av offentlighets- och sekretesslagen skulle begära ut patientdata från varandra skulle ett utlämnande eventuellt kunna vara möjligt under förutsättning att uppgifterna inte är sekretessbelagda. Generellt sett är dock patientdata inom hälso- och sjukvården sekretessbelagda. IMY har inte gjort någon bedömning av om någon sekretessbrytande bestämmelse skulle kunna vara tillämplig i det aktuella fallet.

- **Tvärfunktionellt arbete är avgörande för att framgångsrikt driva innovation och samtidigt säkerställa ett gott dataskydd.** Utifrån pilotprojektet gör IMY några generella reflektioner kring det tvärfunktionella arbetssätt som behövs i innovationsprocesser. En viktig erfarenhet är att det, för att kunna göra relevanta rättsliga bedömningar, krävs en förhållandevis djup förståelse för tekniken. God pedagogisk förmåga är därför nödvändigt både från tekniker och jurister. Strukturer och verktyg för att säkerställa en gemensam förståelse kan underlätta arbetet. Det kan också vara bra att bygga in i processen att löpande gå tillbaka till, och vid behov justera eller komplettera, de rättsliga frågeställningar som behöver utredas.

- **IMY:s bedömning är att regulatorisk testverksamhet som arbetssätt skapar nytta och lärande** både för de aktuella verksamheterna och för tillsynsmyndigheten. Region Halland, Sahlgrenska Universitetssjukhuset och AI Sweden uppger att de har fått värdefull vägledning, både genom de frågor som IMY ställt och de bedömningar som gjorts. För IMY är det stora mervärdet en ökad förståelse för federerad maskininlärning och de rättsliga frågor och utmaningar som uppstår i tillämpningen. IMY avser att under 2023 genomföra ytterligare ett pilotprojekt med regulatorisk testverksamhet.

1. Inledning

Sverige och EU står inför svåra och snabbt föränderliga samhällsutmaningar inom en rad områden. Klimatförändringar, säkerhetshot, energiförsörjning, demografiska förändringar, pandemier och migrationsströmmar är exempel på företeelser som i grunden har förändrat, och kommer att fortsätta förändra, välfärdens förutsättningar.

Gemensamt för samtidens samhällsutmaningar är att ny teknik, eller befintlig teknik som används på nya sätt eller i ny skala, många gånger kommer vara en nödvändig del av vägen framåt. Teknikutvecklingen går också framåt i rasande fart och erbjuder ständigt nya möjligheter. Artificiell intelligens, 5G, sakernas internet, kvantdatorer och annan innovativ teknik ger helt nya verktyg för att bidra till trygghet, hälsa, välfärd och tillväxt.

Internationellt såväl som i Sverige diskuteras allt mer intensivt hur den offentliga förvaltningen ska kunna möta de komplexa samhällsutmaningarna och dra nytta av ny eller befintlig teknik fullt ut. Tempot i teknikutvecklingen utmanar samhällets välbekanta arbetssätt, strukturer, ledarskap, roller och reglering. I internationell litteratur används ofta begreppet *otaktsproblemet* för att beskriva skillnaden i hastighet mellan den exponentiella teknikutvecklingen och den ofta trögrörliga regulatoriska processen. I Sverige har till exempel myndigheten Tillväxtanalys belyst utmaningarna med att reglera teknisk innovation.[1]

I innovationssystemet finns ofta en stark vilja att göra rätt och utveckla hållbara lösningar, men samtidigt en genuin osäkerhet om hur regelverken ska tillämpas på ny teknik. Risken finns att försiktighetsprincipen tar överhand och bromsar innovationskraften. För tillsynsmyndigheter som IMY är en av de främsta utmaningarna att hinna förstå och analysera den nya tekniken som reglerna ska tillämpas på.

1.1 Regulatorisk testverksamhet – en form av försöksverksamhet

Bland annat OECD menar att en viktig del av vägen framåt handlar om att stärka innovationsförmågan i offentlig sektor.[2] I Sverige har Kommittén för teknologisk innovation och etik, Komet, varit en stark röst för att förändringstakten i offentlig sektor behöver påskyndas för att Sverige fullt ut ska kunna dra nytta av digitaliseringens möjligheter. Ett av de utvecklingsspår som Komet föreslagit är att i större utsträckning driva försöksverksamheter.[3]

Komet definierar försök som *arbete som innebär test och verifiering av nya lösningar i verkliga miljöer, under kontrollerade former och med tydliga avgränsningar*. I vissa fall kan lagstiftaren införa särskilda regler för försöksverksamheter. Det förekommer också, även om det är ovanligt i Sverige, att lagstiftaren under särskilda förutsättningar medger avvikelser eller undantag från vissa regler i en försöksverksamhet.[4]

Regulatorisk testverksamhet är en särskild form av försöksverksamhet där utvecklare och till exempel tillsynsmyndigheter arbetar tillsammans för att tolka hur regelverket kan fungera i praktiken med innovativa produkter och tjänster. Avsikten är bland annat att öka den rättsliga förutsebarheten, förkorta tiden till att aktörens produkt eller tjänst når marknaden och underlätta för startup-företag och småföretag. Regulatorisk

[1] *Utmaningar vid reglering av teknisk innovation – möjliga policyåtgärder*, Tillväxtanalys rapport 2022: 042
[2] *OECD Declaration on Public Sector Innovation.* OECD/LEGAL/0450.
3 *Förnya taktiken i takt med tekniken – förslag för en ansvarsfull, innovativ och samverkande förvaltning.* SOU 2022:68.
4 *Försök!* Komet beskriver 2020:23, s. 22 ff.

testverksamhet kallas ibland också för sandlåda, sandbox, testbädd, växthus eller drivhus.

Inom EU har bland annat ministerrådet lyft fram regulatoriska sandlådor som ett sätt att bidra till innovation och tillväxt för företag.[5] Det utkast till AI-förordning som för närvarande förhandlas innehåller också förslag om regulatoriska sandlådor som ett sätt att främja och underlätta tillämpningen av AI.

På dataskyddsområdet har IMY:s motsvarigheter i Storbritannien, Norge och Frankrike under de senaste åren startat regulatoriska testverksamheter där vägledning ges om tillämpningen av dataskyddsförordningen[6], vanligtvis förkortad GDPR. Hos de dataskyddsmyndigheter som driver regulatorisk testverksamhet har det inte funnits någon särskild reglering för testverksamheten eller några undantagsbestämmelser från dataskyddslagstiftningen. Däremot är dataskyddsmyndigheterna tydliga med att de, när de går in i ett vägledningsarbete i en regulatorisk testverksamhet, inte har för avsikt att använda sina korrigerande befogenheter.

Grundtanken med regulatorisk testverksamhet på dataskyddsområdet är att tillsynsmyndigheten ger utforskande, dialogbaserad vägledning till utvalda innovationsprojekt i utbyte mot att arbetet sammanfattas i en publik rapport som möjliggör lärande för fler. Därmed utvecklas praktiska exempel inom områden där både tekniken och juridiken är komplicerad, relativt ny och oprövad. Samtidigt bidrar arbetssättet till att öka tillsynsmyndighetens förståelse för ny teknik och hur den kan tillämpas.

Med regulatorisk testverksamhet avser IMY **fördjupad vägledning till ett specifikt innovationsinitiativ om hur dataskyddsregelverket bör tolkas och tillämpas**.

Kännetecknande för arbetssättet är att

- innovationsaktörerna och IMY gemensamt identifierar de rättsliga frågor som vägledningen ska fokusera på
- vägledning ges muntligt vid flera tillfällen under några månaders tid i form av workshops eller andra dialogbaserade former
- arbetet utmynnar i en publik rapport där resonemang och bedömningar sammanfattas för att möjliggöra lärande för fler.

1.2 Stor efterfrågan på stöd och vägledning i frågor som rör dataskydd

IMY har under 2021 och 2022 haft ett regeringsuppdrag att ge stöd och vägledning till innovationssystemet i frågor som rör dataskydd.[7] För att fördjupa vår förståelse för innovationsaktörernas behov har vi genomfört bland annat workshops,

[5] Europeiska unionens råd. *Antagna rådsslutsatser om regulatoriska sandlådor och experimentklausuler som verktyg för ett innovationsvänligt, framtidssäkrat och motståndskraftigt regelverk som hanterar omvälvande utmaningar i en digital tidsålder.* Bryssel den 16 november 2020. Rådet definierade regulatoriska sandlådor som *ett strukturerat sammanhang för experiment som gör det möjligt att i en verklig miljö testa innovativa tekniker, produkter, tjänster eller metoder (för närvarande särskilt i samband med digitalisering) under en begränsad period och i en begränsad del av en sektor eller ett område som står under myndighetstillsyn för att säkerställa att det finns lämpliga skyddsåtgärder.*
[6] 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 och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[7] Uppdrag att genomföra kunskapshöjande insatser avseende integritets- och dataskyddsfrågor inom innovations-, utvecklings- och införandeprocesser, N2020/01266.

rundabordssamtal och intervjuer med allt från små startup-företag till stora myndigheter som arbetar med innovation.[8]

En viktig slutsats är att det finns en utbredd efterfrågan på fördjupad case-baserad vägledning i frågor som rör dataskydd. Många verksamheter uttrycker önskemål om att kunna få praktiskt stöd i innovationsprocessen genom fördjupad dialog och möjlighet att diskutera faktiska praktikfall med IMY. Vissa verksamheter har hört talas om andra dataskyddsmyndigheters arbete med regulatorisk testverksamhet och efterlyser en sådan verksamhet från IMY. Andra uttrycker ett mer generellt önskemål om att tidigt i en innovationsprocess kunna diskutera med IMY och testa vad som är den bästa lösningen på ett problem ur integritets- och dataskyddssynpunkt.

IMY har inte bedömt det som möjligt att starta en regulatorisk testverksamhet i någon större skala inom ramen för det nuvarande regeringsuppdraget, då erfarenheten från andra länder är att det kräver en långsiktig satsning och dedikerade resurser. I Storbritannien, Norge och Frankrike är *sandboxen* en tjänst dit innovationsaktörer väljs ut genom ett ansökningsförfarande. Datatilsynet i Norge har de senaste åren fått mellan 7 och 9 miljoner norska kronor årligen i särskilda medel för sin regulatoriska testverksamhet.

Komet lämnade våren 2022 ett förslag till regeringen om att ge IMY (tillsammans med Skatteverket och Vinnova) ett treårigt regeringsuppdrag att starta regulatorisk testverksamhet inom dataskydd. Uppdraget föreslogs komma med riktad finansiering om 6 miljoner kronor årligen till IMY.[9]

Eftersom IMY bedömer att både efterfrågan och den potentiella nyttan av arbetssättet är stor, beslutade vi att under hösten 2022 genomföra ett pilotprojekt med regulatorisk testverksamhet. Avsikten har varit att påbörja ett lärande och skapa förutsättningar för ett eventuellt kommande arbete i större skala.

1.3 Urval och arbetsprocess i pilotprojektet

Valet av innovationsprojekt till piloten inleddes genom en förfrågan till flera av IMY:s samverkansparter om lämpliga kandidater. Frågan ställdes till AI Sweden (Sveriges nationella center för tillämpad AI), Sjyst Data (ett samverkans- och innovationsprojekt om dataskydd och integritet som drivs av RISE) samt Cybernoden (den nationella kompetensgemenskapen för att accelerera forskning och innovation inom cybersäkerhet). Kriterier för ett lämpligt innovationsprojekt bedömdes vara att

- innovationsprojektet var i en tidig fas, i så måtto att den tänkta personuppgiftsbehandlingen inte redan pågick
- projektet kommit tillräckligt långt för att kunna definiera relativt konkreta rättsliga frågeställningar
- projektet matchade IMY:s planering i tid och kunde avsätta resurser för ett antal workshops och möten under hösten 2022
- de aktuella verksamheterna accepterade att IMY:s pilotprojekt skulle utmynna i en publik slutrapport.

Med utgångspunkt i dessa kriterier valdes projektet *Decentralized AI in Health Care – Federerad maskininlärning mellan två vårdgivare* med Region Halland, Sahlgrenska

---

[8] *Delredovisning av uppdrag om kunskapshöjande insatser till innovationssystemet om integritets- och dataskyddsfrågor.* IMY 2021-5817.
[9] *Förslag till regeringsuppdrag avseende regulatorisk testverksamhet inriktad på dataskyddsfrågor vid datadriven innovation*. Dnr 2022/00323/N 2018:04

Universitetssjukhuset och AI Sweden till att bli IMY:s första pilotprojekt avseende regulatorisk testverksamhet.

Efter valet av projekt har det praktiska arbetet i piloten haft tre faser.

- **Uppstartsfas.** Under perioden juni–september 2022 hölls inledande möten för att förstå det aktuella innovationsprojektet och med vilka förväntningar och förutsättningar de olika deltagarna gick in i pilotprojektet. IMY och deltagarna valde gemensamt ut de frågeställningar som vägledningen skulle fokusera på. I uppstartsfasen planerades och genomfördes också gemensamma kommunikationsinsatser, bland annat ett digitalt lanseringswebbinarium med cirka 400 åhörare där möjligheter och utmaningar med regulatorisk testverksamhet diskuterades.[10]

- **Vägledningsfas.** Huvuddelen av arbetet genomfördes i form av en serie workshops under perioden september - december 2022. Dialog fördes kring de fastställda rättsliga frågeställningarna och IMY gav löpande muntlig vägledning. Ett par särskilda mötestillfällen ägnades åt fördjupade genomlysningar av den aktuella tekniken. Vid det avslutande mötet reflekterade IMY och deltagarna också tillsammans kring arbetssättet med regulatorisk testverksamhet, vad som fungerat bra och vad som kan utvecklas. Totalt medverkade ett 15-tal personer från IMY, Region Halland, Sahlgrenska Universitetssjukhuset och AI Sweden i arbetet.

- **Rapportfas.** Under januari - februari 2023 har IMY arbetat med att sammanställa denna slutrapport, där arbetet och slutsatserna från pilotprojektet beskrivs. Region Halland, Sahlgrenska Universitetssjukhuset och AI Sweden har bistått med att bland annat kontrollera fakta i de delar som rör teknikbeskrivningarna.

2. Projektet Decentralized AI in Health Care – Federerad maskininlärning mellan två vårdgivare

En ökad användning av AI i hälso- och sjukvården lyfts fram av regeringen som en viktig del för att förbättra hälsan i befolkningen och att utveckla sjukvården.[11] Företrädare för hälso- och sjukvården beskriver också att informationsdriven vård, som i ökad utsträckning tar hjälp av AI, kan bidra till att beslut kan skräddarsys på individ- och systemnivå samt utveckla mer avancerade och träffsäkra diagnoser och behandlingar.[12]

En viktig basförutsättning för att kunna utveckla och tillämpa AI i vården är tillgång till stora mängder hälsodata. För närvarande pågår en rad politiska initiativ för att stimulera och förenkla användningen av hälsodata, bland annat det EU-gemensamma arbetet med förslaget till förordning om ett europeiskt hälsodataområde (EHDS).[13]

Även teknik för att göra det enklare att på ett effektivt och säkert sätt kunna dra nytta av stora datamängder utvecklas snabbt. En teknik som av många bedöms som särskilt

[10] IMY-bloggen: Innovationspilot med decentraliserad AI – nu kör vi! | IMY.
[11] *En nationell strategi för life science,* N2019/03157.
[12] Nytt arbetssätt testas för att ge innovationsprojekt vägledning om dataskydd | IMY.
[13] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_sv.

lovande, både inom vården och en rad andra samhällssektorer, är det som kallas decentraliserad AI.

2.1 Kort om decentraliserad AI och projektet

Decentraliserad AI är ett nytt paradigm inom maskininlärning där flera parter gemensamt kan träna en maskininlärningsmodell utan att samla in data centralt för träning, vilket är utgångspunkten för centraliserad AI. Den vanligaste formen av decentraliserad maskininlärning kallas federerad maskininlärning. AI Sweden ser decentraliserad AI som ett av de absoluta framtidsområdena inom AI-utvecklingen. Tekniken bedöms bland annat som central för att lösa juridiska och säkerhetsmässiga utmaningar inom en rad användningsområden.

Federerad maskininlärning är en typ av decentraliserad AI som kan användas om flera aktörer tillsammans vill utveckla AI för ett gemensamt ändamål, men inte kan eller vill utbyta data mellan varandra. Ett skäl att använda federerad maskininlärning kan vara att aktörerna var för sig inte har tillräckligt med träningsdata för att kunna träna en maskininlärningsmodell till att uppnå en acceptabel prestanda och därför behöver samverka för att kunna skapa en effektiv och ändamålsenlig maskininlärningsmodell. Vid utveckling av federerad maskininlärning är grundtanken att det inte ska ske någon överföring av data, till exempel personuppgifter, mellan aktörerna.

I projektet *Decentralized AI in Health Care - Federerad maskininlärning mellan två vårdgivare* samarbetar Region Halland och Sahlgrenska Universitetssjukhuset (hädanefter benämnda vårdgivarna) med stöd av AI Sweden för att utvärdera möjligheterna till att gemensamt träna och utbyta maskininlärningsmodeller.

Syftet med det specifika projektet är att bättre kunna prediktera återinläggning av hjärtsviktspatienter inom 30 dagar från senaste sjukhusvistelsen med hjälp av federerad maskininlärning.

Kort beskrivet innebär tekniken att vårdgivarna tränar varsin lokal maskininlärningsmodell med hjälp av patientdata[14] som respektive vårdgivare har tillgång till i den egna verksamheten. I nästa steg kombineras lärdomarna ihop till en gemensam global maskininlärningsmodell, och träningen upprepas därefter på den lokala patientdatan. En mer ingående beskrivning av processen finns i avsnitt 4.1 nedan.

2.2 De rättsliga frågeställningarna i pilotprojektet

IMY, Region Halland, Sahlgrenska Universitetssjukhuset och AI Sweden enades om att i den regulatoriska testverksamheten fokusera på bedömningen av tre rättsliga frågeställningar:

1. Finns det rättslig grund för den lokala personuppgiftsbehandlingen?
2. Sker det vid den federerade maskininlärningen i det aktuella fallet ett utlämnande av personuppgifter mellan vårdgivarna?
3. Finns det rättslig grund för utlämnande av personuppgifter mellan vårdgivarna?

I avsnitt 3-5 nedan följer en redogörelse för bedömningen av de tre rättsliga frågeställningarna.

---

[14] Med patientdata avses i denna rapport personuppgifter om patienter.

2.3 Avgränsning i pilotprojektet

Värt att notera är att det utöver de rättsliga frågeställningarna ovan också finns en rad andra juridiska frågor som behöver beaktas för att säkerställa efterlevnaden av dataskyddsförordningen och kompletterande nationell rätt, men som inte har analyserats inom ramen för detta pilotprojekt. IMY och projektdeltagarna har tillsammans valt ut de tre frågeställningarna ovan utifrån att de bedömts ha både stor relevans för framdriften i det aktuella projektet, men också vara relevanta för fler innovationsaktörer.

Det är varje personuppgiftsansvarigs skyldighet att se till att dess personuppgiftsbehandling är förenlig med dataskyddsförordningen och kompletterande nationell rätt. Till de frågor som inte har analyserats i pilotprojektet hör exempelvis fördelningen av de inblandade vårdgivarnas roller enligt dataskyddsförordningen. Det första steget i dataskyddsarbetet för alla verksamheter som står inför att börja behandla personuppgifter är att kartlägga den planerade personuppgiftsbehandlingen.[15] Det behöver också utredas i ett tidigt skede vem som är personuppgiftsansvarig för varje behandling, om det uppkommer ett gemensamt personuppgiftsansvar och om någon kan anses vara personuppgiftsbiträde. Därefter vidtar arbetet med att bedöma om personuppgiftsbehandlingen är förenlig med de krav som ställs i dataskyddsförordningen och kompletterande nationell rätt.

En utgångspunkt i den regulatoriska testverksamheten har varit att deltagarna i egenskap av vårdgivare är personuppgiftsansvariga för respektive lokal behandling av patientdata. Det har inte analyserats vilken part som är personuppgiftsansvarig för den centrala servern (om personuppgiftsansvaret inte kan anses vara gemensamt). Vidare har IMY inte bedömt om det finns rättslig grund för en vårdgivare att behandla personuppgifter som härstammar från en annan vårdgivare.

Andra exempel på frågor som behöver analyseras av de deltagande vårdgivarna, men som inte har ingått i pilotprojektet, är hur de registrerades rätt till information ska tillgodoses och frågan om kravet på personuppgiftsansvarig att inte hantera fler personuppgifter än nödvändigt (principen om uppgiftsminimering).

3. Finns det rättslig grund för den lokala personuppgiftsbehandlingen?

Den första frågan är om det finns rättslig grund för den personuppgiftsbehandling som sker inom ramen för den lokala träningen av maskininlärningsmodellen. I detta steg använder alltså Region Halland och Sahlgrenska Universitetssjukhuset enbart patientdata som de har tillgång till i den egna verksamheten. Vi har valt att kalla detta steg för den lokala personuppgiftsbehandlingen.

Som nämnts ovan behöver maskininlärningsmodellen tränas på patientdata. Respektive vårdgivare avser att träna den lokala modellen med hjälp av patientdata som den har tillgång till i den egna verksamheten. Patientdata utgör personuppgifter och att träna maskininlärningsmodellen innebär att personuppgifter behandlas. Behandling är ett brett begrepp och innefattar i princip allt som kan göras med

[15] För mer information om kartläggning av personuppgiftsbehandling, besök IMY:s Innovationsportal – Är det ni tänkt göra förenligt med GDPR? (https://www.imy.se/verksamhet/dataskydd/innovationsportalen/ar-det-ni-tankt-gora-ar-forenligt-med-gdpr/).

personuppgifter. Till exempel kan man samla in, registrera, lagra, analysera, lämna ut eller radera dem.[16]

3.1 Rättslig bakgrund

Aktuella bestämmelser[17]

Dataskyddsförordningen
Skäl 41
Artikel 4.7
Artikel 5.1 a
Artikel 6.1 e
Artikel 6.3
Artikel 9.1
Artikel 9.2 h
Artikel 9.3

Hälso- och sjukvårdslagen
5 kap. 4 §

Patientdatalagen
1 kap. 4 §
2 kap. 4 §
2 kap. 5 §
2 kap. 6 §
2 kap. 7 a §

3.1.1 Personuppgiftsansvar

Med personuppgiftsansvarig avses, enligt artikel 4.7 i dataskyddsförordningen, en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Enligt 2 kap. 6 § patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför.

3.1.2 Laglighet och rättslig grund

Dataskyddsförordningen är den allmänna rättsliga regleringen vid behandling av personuppgifter inom EU. Den gäller även inom hälso- och sjukvården.

Enligt artikel 5.1 a i dataskyddsförordningen ska personuppgifter behandlas på ett lagligt sätt. För att behandlingen ska anses vara laglig krävs att åtminstone ett av villkoren i artikel 6.1 är uppfyllt. Den rättsliga grund som är aktuell vid vårdgivares behandling av personuppgifter för att utveckla ett AI-verktyg av det slag som här är

[16] Jfr artikel 4.2 i dataskyddsförordningen.
[17] I listan anges endast de bestämmelser som diskuteras i förevarande avsnitt. Det finns även andra bestämmelser som är tillämpliga på den aktuella personuppgiftsbehandlingen, men som inte har beaktats inom ramen för pilotprojektet (se avsnitt 2.3 ovan). Listan ska alltså inte ses som uttömmande.

aktuellt är, enligt IMY:s bedömning, uppgift av allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen.

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 e i dataskyddsförordningen måste den vara *nödvändig* i förhållande till den rättsliga grunden. Nödvändighetskriteriet ska ses mot bakgrund av att undantag och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är absolut nödvändigt. Samtidigt följer av praxis att behandlingen kan anses nödvändig och därmed tillåten enligt artikel 6.1 om den leder till effektivitetsvinster.[18] Av praxis följer även att kravet på nödvändighet ska prövas tillsammans med principen om uppgiftsminimering enligt artikel 5.1 c i dataskyddsförordningen. Där anges att personuppgifter som samlas in ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Inom ramen för pilotprojektet har vi inte analyserat om de personuppgifter som avses användas för träning av maskininlärningsmodellen är förenlig med principen om uppgiftsminimering.

Vad gäller bland annat den rättsliga grunden uppgift av allmänt intresse, ställer artikel 6.3 i dataskyddsförordningen krav på att grunden för behandlingen ska regleras i EU-rätten eller medlemsstaternas nationella rätt. Den rättsliga grunden enligt artikel 6.3 är ofta fastställd i till exempel myndigheters instruktioner eller i annan reglering som styr verksamheten, till exempel hälso- och sjukvårdslagen och socialtjänstlagen (2001:453). På vissa områden kompletteras verksamhetsregleringen av en särskild författning som reglerar personuppgiftsbehandlingen, en så kallad registerförfattning. Den rättsliga grunden som fastställs i nationell rätt enligt artikel 6.3 omfattar då både verksamhetsregleringen och registerförfattningen. För svenskt vidkommande regleras grunden för behandling av personuppgifter inom hälso- och sjukvården bland annat i hälso- och sjukvårdslagen och patientdatalagen. Hälso- och sjukvårdslagen är en verksamhetsreglering och patientdatalagen utgör en registerförfattning.

En central fråga är de krav som ställs på den lag eller annan författning som reglerar den rättsliga grunden. Dataskyddsförordningen ställer nämligen krav på tydlighet, precision, förutsebarhet och proportionalitet (artikel 6.3 och skäl 41). Kravet på förutsebarhet ska ses från den registrerades – och inte den personuppgiftsansvariges – perspektiv (skäl 41). EU-domstolen har i sin praxis ställt höga krav på utformningen av de rättsliga grunder som ska ligga till grund för personuppgiftsbehandling.[19]

Det måste alltid göras en bedömning av personuppgiftsbehandlingens och verksamhetens karaktär för att avgöra hur stor grad av tydlighet och precision som krävs. Ett mer kännbart intrång kräver en mer preciserad rättslig grund, medan personuppgiftsbehandling med lägre integritetsrisker kan ske med stöd av en mer allmänt hållen rättslig grund.[20]

---

[18] Prop. 2017/18:105 s. 189.
[19] EU-domstolens dom den 24 februari 2022, Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, punkt 83, där EU-domstolen uttalar följande: ”I detta sammanhang ska det dock erinras om att för att uppfylla det proportionalitetskrav som föreskrivs i artikel 5.1 c i förordning 2016/679 (se för ett liknande resonemang, dom av den 22 juni 2021, Latvijas Republikas Saeima (Prickning), C-439/19, EU:C:2021:504, punkt 98 och där angiven rättspraxis), måste de föreskrifter som ligger till grund för behandlingen innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt ange minimikrav, så att de personer vars personuppgifter lämnas ut ges tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Dessa föreskrifter måste även vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd för behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt (dom av den 6 oktober 2020, Privacy International, C-623/17, EU:C:2020:790, punkt 68 och där angiven rättspraxis).”
[20] Prop. 2017/18:105 s. 51.

3.1.3 Känsliga personuppgifter

Av artikel 9.1 i dataskyddsförordningen framgår att behandling av särskilda kategorier av personuppgifter (så kallade känsliga personuppgifter) är förbjuden. Känsliga personuppgifter är bland annat uppgifter om hälsa. I artikel 9.2 finns undantagen som beskriver när känsliga personuppgifter trots allt får behandlas.

Av artikel 9.2 h framgår att behandling av känsliga personuppgifter får ske om det är nödvändigt av skäl som hör samman med bland annat förebyggande och tillhandahållande av hälso- och sjukvård. Behandlingen av personuppgifterna måste dock ske med stöd av antingen EU-rätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet. Ytterligare en förutsättning är att de villkor och skyddsåtgärder som avses i artikel 9.3 är uppfyllda. I denna bestämmelse finns krav om tystnadsplikt. Även tystnadsplikten måste vara reglerad i EU-rätten eller medlemsstaternas nationella rätt eller i bestämmelser som fastställs av nationella behöriga organ.

Det ovan sagda innebär att såväl den rättsliga grunden uppgift av allmänt intresse som behandling av känsliga personuppgifter med stöd av undantaget i artikel 9.2 h behöver kompletterande regler.

3.1.4 Kompletterande regler i patientdatalagen

Den allmänna regleringen om behandling av personuppgifter i dataskyddsförordningen kompletteras på hälso- och sjukvårdsområdet av patientdatalagen (1 kap. 4 § patientdatalagen).

Enligt patientdatalagen får personuppgifter behandlas inom hälso- och sjukvården om det behövs för de ändamål som anges i 2 kap. 4 § första stycket. Syftet med bestämmelsen är att fastställa de ändamål som tar sikte på den egentliga kärnverksamheten inom hälso- och sjukvården.[21] Bestämmelsen kompletteras av 2 kap. 5 § patientdatalagen som tillåter att personuppgifter som behandlas med stöd av 2 kap. 4 § också får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Vidare framgår av 2 kap. 5 § att personuppgifterna får behandlas för andra ändamål än de som anges i 2 kap. 4 §, om det är förenligt med den så kallade finalitetsprincipen. Det innebär att personuppgifter som redan finns i hälso- och sjukvårdsverksamheten får behandlas för andra ändamål än insamlingsändamålen under förutsättning att de nya ändamålen inte är oförenliga med de ursprungliga.

Enligt 2 kap. 4 § första stycket patientdatalagen får personuppgifter behandlas inom hälso- och sjukvården om det behövs för

1. att fullgöra de skyldigheter som anges i 3 kap. patientdatalagen och upprätta annan dokumentation som behövs i och för vården av patienter,
2. administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall,
3. att upprätta annan dokumentation som följer av lag, förordning eller annan författning,
4. att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten,

[21] Prop. 2007/08:126 s. 227.

5. administration, planering, uppföljning, utvärdering och tillsyn av verksamheten, eller
6. att framställa statistik om hälso- och sjukvården.

En av huvudfrågorna i den regulatoriska testverksamheten har varit om utvecklingen av ett AI-verktyg för prediktion av återinläggning av hjärtsviktspatienter kan anses omfattas av något av de ovannämnda ändamålen. Det ändamål som legat närmast till hands är 2 kap. 4 § första stycket 4 patientdatalagen som rör kvalitetsutveckling och kvalitetssäkring.

I förarbetena till patientdatalagen anges att användningen av modern informationsteknik förbättrar möjligheterna att bedriva kvalitetssäkringsarbete avsevärt samt att kvalitetssäkringsarbete kan ske i många former och med olika metoder. Av förarbetena framgår vidare att ändamålsbestämmelsen om kvalitetsutveckling och kvalitetssäkring ska läsas tillsammans med reglerna i hälso- och sjukvårdslagen.[22] Den lagen reglerar hur hälso- och sjukvårdsverksamhet ska organiseras och bedrivas i Sverige. Det är framför allt 5 kap. 4 § hälso- och sjukvårdslagen som har en koppling till ändamålsbestämmelsen om kvalitetsutveckling och kvalitetssäkring i patientdatalagen. I den bestämmelsen föreskrivs en skyldighet för vårdgivare att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten. Förarbetena till hälso- och sjukvårdslagen ger viss information om vad kvalitetsutveckling och kvalitetssäkring innebär, men det finns inte något uttryckligt stöd för att utvecklingen av nya metoder för att bedriva vård med hjälp av AI-teknik kan anses omfattas. De aktuella förarbetena tar istället främst sikte på olika former av tillbud och avvikelser i vården.[23]

Vidare har patientdatalagen regler om behandling av känsliga personuppgifter i 2 kap. 7 a §. Enligt denna bestämmelse får sådana uppgifter behandlas med stöd av artikel 9.2 h i dataskyddsförordningen under förutsättning att kravet på tystnadsplikt i artikel 9.3 i förordningen är uppfyllt.

3.2 Dialog med Socialstyrelsen

Det är Socialstyrelsen som är Sveriges kunskapsmyndighet för vård och omsorg.[24] Socialstyrelsens syn på huruvida utvecklingen av nya AI-verktyg inom hälso- och sjukvården skulle kunna utgöra arbete med kvalitetsutveckling och kvalitetssäkring, på det sätt som avses i 5 kap. 4 § hälso- och sjukvårdslagen, är därför av betydelse för IMY:s bedömning. Av denna anledning har IMY inom ramen för den regulatoriska testverksamheten haft dialog med Socialstyrelsen.

Socialstyrelsen menar att det inte kan uteslutas att ett AI-verktyg, likt det som vårdgivarna vill utveckla inom ramen för projektet, kan anses utgöra en del i arbetet med kvalitetsutveckling och kvalitetssäkring för det fall att verktyget kan förväntas leda till åtgärder för en bättre och säkrare vård.

Ett centralt argument enligt Socialstyrelsen är att hälso- och sjukvårdslagen är teknikneutral och lagstiftningens mål kan uppnås genom olika metoder. Mot bakgrund av den snabba utvecklingen inom såväl hälso- och sjukvården som samhället i övrigt

[22] Prop. 2007/08:126 s. 57–58 och 228. I förarbetena hänvisas till den tidigare gällande hälso- och sjukvårdslagen (1982:763).
[23] Prop. 1995/96:176 s. 53–54. Enligt förarbetena ska vårdgivaren inom hälso- och sjukvården utveckla metoder för att noga följa och analysera utvecklingen vad gäller kvalitet och säkerhet. Det gäller till exempel system som synliggör förekomsten av risktillbud eller så kallade avvikande händelser (onormala vårdtider, infektioner, komplikationer, reoperationer, återintagning etc.) eller som mäter servicegrad, patienttillfredsställelse osv.
[24] Jfr 1 och 4 §§ förordningen (2015:284) med instruktion för Socialstyrelsen.

skulle det medföra svårigheter om lagstiftningen inte skulle kunna tolkas utifrån den värld vi lever i. Av denna anledning finns det alltså enligt Socialstyrelsen utrymme att tolka bestämmelsen om kvalitetsutveckling och kvalitetssäkring i hälso- och sjukvårdslagen förhållandevis fritt i fråga om de metoder som används för att uppnå lagstiftningens mål.

3.3 IMY:s bedömning

IMY utgår i det följande från att Region Halland respektive Sahlgrenska Universitetssjukhuset är personuppgiftsansvarig vårdgivare enligt 2 kap. 6 § patientdatalagen för den egna lokala personuppgiftsbehandlingen.

Den övergripande frågan i detta avsnitt är om vårdgivarna har rättslig grund för den lokala personuppgiftsbehandlingen. Den rättsliga grunden för behandling av personuppgifter inom hälso- och sjukvården är fastställd bland annat i hälso- och sjukvårdslagen och patientdatalagen. För att behandlingen ska kunna ske med stöd av denna rättsliga grund krävs att behandlingen sker för något av de tillåtna ändamål som anges i patientdatalagen. Den ändamålsbestämmelse som främst aktualiseras är 2 kap. 4 § första stycket 4 om kvalitetsutveckling och kvalitetssäkring.

Vad gäller tolkningen av 2 kap 4 § första stycket 4 patientdatalagen, konstaterar IMY att bestämmelsens ordalydelse innebär att de ändamål som är aktuella i testverksamheten skulle kunna omfattas av bestämmelsen. Det ligger nära till hands att uppfatta ett arbete som syftar till att förbättra möjligheten att förutse återinläggning av hjärtsviktspatienter som ett bidrag till kvalitetsutveckling eller kvalitetssäkring av vården.

Det kan vidare konstateras att det i förarbetena till patientdatalagen understryks att kvalitetsarbetet kan ske i många former och med olika metoder samt att användningen av modern informationsteknik förbättrar möjligheterna att bedriva kvalitetssäkringsarbete avsevärt. Enligt IMY ger detta stöd för en dynamisk och teknikneutral tolkning av ändamålsbestämmelsen. En sådan tolkning innebär att vad som är kvalitetsutveckling och kvalitetssäkring i vården kan förändras över tid bland annat med hänsyn till teknikutvecklingen.

Samtidigt kan konstateras att regleringen om kvalitetsutveckling och kvalitetssäkring i patientdatalagen har en nära koppling till 5 kap. 4 § hälso- och sjukvårdslagen. Begreppen kan inte ges en vidare innebörd i patientdatalagen än i hälso- och sjukvårdslagen. I förarbetena till hälso- och sjukvårdslagen ges en beskrivning av kvalitetsarbetet som inte omfattar den typ av verksamhet som är aktuell i testverksamheten. Detta kan dock förklaras av att AI-tekniken i mitten av 90-talet, då förarbetena skrevs, inte hade nått en sådan utvecklingsgrad att den utgjorde ett naturligt inslag i kvalitetsarbetet. Enligt IMY kan beskrivningen i förarbetena snarast ses som en lägesbild av hur kvalitetsarbetet avsågs bedrivas vid den tidpunkt då de togs fram. Förarbetena utesluter inte, enligt IMY:s bedömning, en dynamisk och teknikneutral tolkning av vad som ingår i kvalitetsarbetet. Genom dialogen med Socialstyrelsen, som är kunskapsmyndighet för vård och omsorg, har också framkommit att Socialstyrelsen förordar en sådan tolkning.

IMY konstaterar mot den bakgrunden att det finns mycket som talar för att den tillämpning av AI-teknik som är aktuell i den regulatoriska testverksamheten kan anses som kvalitetsarbete enligt 2 kap. 4 § första stycket 4 patientdatalagen och 5 kap. 4 § hälso- och sjukvårdslagen. Det framstår vidare som att den lokala personuppgiftsbehandlingen uppfyller kravet på nödvändighet, eftersom den är central

för att ta fram ett fungerade AI-verktyg som förbättrar vårdkvaliteten för hjärtsviktspatienter.

Enligt 2 kap. 7 a § patientdatalagen får känsliga personuppgifter behandlas med stöd av artikel 9.2 h i dataskyddsförordning under förutsättning att kravet på tystnadsplikt i artikel 9.3 är uppfyllt. Enligt artikel 9.2 h får känsliga personuppgifter behandlas om det är nödvändigt av skäl som hör samman med bland annat förebyggande, eller tillhandahållande av, hälso- och sjukvård. För att på sikt kunna ta fram ett fungerade AI-verktyg som kan hjälpa hälso- och sjukvården att bättre prediktera risken för återinläggning av hjärtsviktspatienter är det enligt vårdgivarna nödvändigt att träna den aktuella maskininlärningsmodellen på patientdata. Patientdata utgör uppgifter om hälsa, vilket betraktas som känsliga personuppgifter enligt artikel 9.1 i dataskyddförordningen. Bestämmelser om tystnadsplikt för personer verksamma inom hälso- och sjukvården i Sverige finns i bland annat 25 kap. offentlighets- och sekretesslagen. Det finns således en tystnadsplikt som regleras i nationell rätt på det sätt som krävs enligt artikel 9.3 i dataskyddsförordningen. Detta innebär att vårdgivarna får behandla känsliga personuppgifter enligt 2 kap. 7 a § patientdatalagen inom ramen för den lokala personuppgiftsbehandlingen, i den utsträckning behandlingen är nödvändig för att bedriva kvalitetsarbete enligt 2 kap. 4 § första stycket 4 patientdatalagen.

Den rättsliga grund som fastställs i nationell rätt – i det här fallet främst hälso- och sjukvårdslagen och patientdatalagen – måste enligt artikel 6.3 och skäl 41 i dataskyddsförordningen uppfylla kraven på tydlighet, precision, förutsebarhet och proportionalitet. Dessa krav ska bedömas i förhållande till den behandling som är aktuell, bland annat utifrån hur integritetskänslig behandlingen är och vilka skyddsåtgärder som föreskrivs i den rättsliga grunden i nationell rätt. IMY konstaterar att det visserligen är fråga om behandling av känsliga personuppgifter, men att bland annat de skyddsåtgärder som föreskrivs i patientdatalagen och det starka allmänintresset kan tala för att nämnda krav är uppfyllda.

Mot den bakgrunden är IMY:s samlade bedömning att det framstår som att det finns rättslig grund för den lokala personuppgiftsbehandlingen för Region Halland respektive Sahlgrenska Universitetssjukhuset.

4. Sker det vid den federerade maskininlärningen i det aktuella fallet ett utlämnande av personuppgifter mellan vårdgivarna?

En i pilotprojektet central fråga är om vårdgivarna genom den federerade maskininlärningen ges tillgång till varandras patientuppgifter. Inte minst eftersom avsikten med den federerade maskininlärningen varit att undvika det. Frågan är av särskild betydelse då ett sådant utlämnande av personuppgifter, i likhet med all annan personuppgiftsbehandling, måste vara förenlig med tillämpliga dataskyddsregler (se mer i avsnitt 5 nedan).

För att kunna bedöma om det kan komma att ske ett utlämnande av personuppgifter mellan vårdgivarna har en fördjupad analys av hur tekniken fungerar i det aktuella fallet varit nödvändig.

Det är tydligt för IMY att vårdgivarna inte har någon önskan om att ge varandra tillgång till sina respektive personuppgifter. Att undvika detta har tvärtom varit ett bärande skäl till att välja en federerad maskininlärningsmodell. Frågan är dock om det finns en risk för att personuppgifter ändå kan komma att utlämnas. Nedan följer en beskrivning av den federerade maskininlärningsmodellen i det aktuella fallet, följt av en beskrivning av de risker som visat sig aktuella.

4.1 Beskrivning av tekniken i det aktuella projektet

För att tillsammans kunna utveckla AI genom federerad maskininlärning behövs lokala data (innefattande personuppgifter) från båda vårdgivarna samt ett gemensamt val av maskininlärningsalgoritm och arkitektur för maskininlärningsmodellen. Region Halland och Sahlgrenska Universitetssjukhuset har tillsammans satt upp nedan beskrivna lösning för att prova den i praktiken. Under projektet används dock inte riktiga personuppgifter.

Vårdgivarna tränar först varsin maskininlärningsmodell lokalt med egna lokala *träningsdata,* dvs. data som ska användas inom ramen för maskininlärningen. Hur maskininlärningsmodellen är uppbyggd, dvs. dess arkitektur och konfiguration kommer vårdgivarna överens om gemensamt på förhand innan träningen av de respektive modellerna påbörjas.

Vårdgivarnas uppsättning av lokala träningsdata är indelad i olika kategorier (*variabler*) av personuppgifter om hjärtsviktspatienter från den egna regionen, till exempel kön, ålder och vistelsetid. Vårdgivarna bestämmer gemensamt vilka kategorier som ska ingå i träningsdatan. I träningsdatan utgör personuppgifterna själva *värdena* i variablerna, till exempel kvinna, 68 år, 3 dagar. Information från en sjukhusvistelse från en hjärtsviktspatient består av ett antal variabelvärden, dvs. personuppgifter, där vart och ett utgör en så kallad *datapunkt*. Dessa datapunkter, tillsammans med svaret om patienten faktiskt hade en återinläggning inom 30 dagar eller inte, utgör träningsdatan. Träningsdatan matas under träningen in i maskininlärningsmodellen upprepade gånger (*iterationer*) för att modellen ska lära sig från dessa exempel. Under varje iteration får maskininlärningsmodellen tränas på varje datapunkt i träningsdatan en gång.

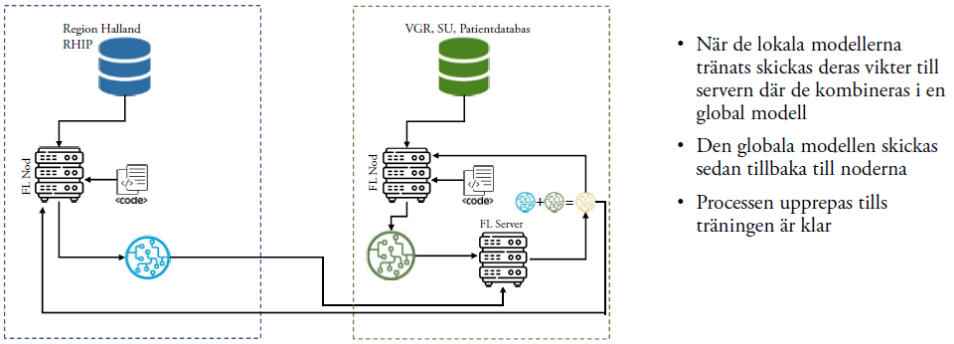
Från maskininlärningsmodellen kommer ett resultat, ett tal mellan 0 till 1, som ger värdefull information avseende ändamålet med den aktuella federerade maskininlärningen, nämligen prediktion av återinläggning inom 30 dagar för hjärtsviktspatienter. Talet mellan 0 och 1 visar på sannolikheten för en hjärtsviktspatient att bli återinlagd inom 30 dagar efter en vistelse på sjukhuset. I detta sammanhang är 0 lika med 0 procents sannolikhet att patienten kommer att bli återinlagd och 1 är lika med 100 procents sannolikhet att patienten kommer att bli återinlagd.

För att prediktionen ska bli bättre uppdateras modellen efter varje iteration. Detta sker genom att modellens så kallade *vikter* uppdateras. Vikterna beräknas fram med den lokala träningsdatan (som innehåller personuppgifter) genom en teknik som kallas för *backpropagation.* Från första början är siffran i vikterna slumpmässigt utvald.

Antalet iterationer övervakas och regleras för att förhindra det som kallas *överträning.* Överträning riskerar nämligen att modellen blir alltför specialiserad på den lokala träningsdatan. Om modellen har övertränats kommer den att ge ett bra resultat på

träningsdatan, men däremot vara dålig på att generalisera till annan data som modellen inte har tränats på.

Tanken är att enbart lärdomarna av träningen delas med den andra parten. Det sker när de lokala modellerna har genomfört det antal iterationer som bestämts på förhand, genom att modellernas vikter skickas till en central server där de kombineras i en så kallad global maskininlärningsmodell. Den globala modellens vikter skickas sedan tillbaka till vårdgivarnas lokala noder, där de lokala modellerna tränas. Båda vårdgivarna har nu en varsin kopia av den globala modellen med uppdaterade vikter. Vikterna justeras igen utifrån den lokala datan och efter ett antal iterationer så skickas de nya vikterna från de lokala modellerna till den centrala servern. Denna process repeteras därefter fram till dess att modellen bedöms vara färdigtränad, dvs. har genomfört det antal iterationer som man har kommit överens om på förhand.



Sammanfattningsvis sker alltså den ovan beskrivna träningen i följande steg.

1. Vårdgivarna kommer överens om maskininlärningsmodellens arkitektur och konfiguration.
2. Vårdgivarna kommer överens om de variabler, dvs. vilka kategorier av personuppgifter från lokala data, vars variabelvärden ska matas in i modellerna.
3. Ett antal vikter som består av siffror (slumpmässiga första omgången) läggs till vid varje variabel.
4. Iterationerna körs på lokal nivå. Efter varje iteration uppdateras vikterna.
5. Båda vårdgivarna skickar sina uppdaterade vikter till en central server där vikterna kombineras i en global modell.
6. De kombinerade vikterna, som är det sammanvägda resultatet av de båda vårdgivarnas lokala vikter, skickas sedan tillbaka till respektive part.
7. Den lokala modellens vikter uppdateras nu med den globala modellens uppsättning av vikter.

Steg 4–7 upprepas till dess att maskininlärningsmodellen bedöms vara färdigtränad, dvs. när det antal iterationer som vårdgivarna kommit överens om på förhand har körts.

4.2 Två typer av möjliga attacker

Som beskrivits ovan beräknas vikterna fram med hjälp av lokala data, som innehåller personuppgifter, genom en teknik som kallas för backpropagation. Vårdgivarna har beskrivit för IMY att det vid den här konfigurationen av federerad maskininlärning kan

finnas en risk att den lokala modellen, genom träningen, ”minns” de personuppgifter som ingått i den lokala träningsdatan. Därmed finns här en risk för att personuppgifter överförs till den centrala servern med hjälp av de lokala vikterna genom den tidigare beskrivna processen. Under projektets gång har det identifierats risker som skulle kunna möjliggöra att en av vårdgivarna, via maskininlärningsmodellen, bereder sig tillgång till den andra partens träningsdata. Det finns primärt två typer av attackmetoder som möjliggör detta, nämligen *Membership Inference Attack* och *Model Inversion Attack* vilka förklaras närmare nedan.

Grundläggande förutsättningar för att lyckas genomföra någon av dessa attacker i det aktuella fallet är att en part har tillgång till a) den tränade globala modellen och b) sin egna lokala träningsdata.

Vårdgivarna bedömer att det också behövs specialistkunskap i federerad maskininlärning, ett uppsåt och ett par veckors arbete för att använda metoderna och eventuellt lyckas. Det skulle då enligt vårdgivarna vara relativt omständligt, men i vissa fall möjligt, för någon av parterna att räkna fram de personuppgifter som den andra parten har använt i träningen av sin lokala modell.

Membership Inference Attack

Metoden syftar till att ta reda på om en viss datapunkt har ingått i träningsdatan eller inte. Det innebär att den attackerande parten till exempel kan ta reda på om personer med vissa variabelvärden (till exempel kvinna, 67 år, blodgrupp AB) har hjärtsvikt (och vilka som troligen inte har det) och därmed ingått i träningsdatan eller inte hos den andra parten.

För att kunna utföra denna typ av attack krävs tillgång till en hypotetisk datapunkt, vilket kan beskrivas som ett antagande eller förslag om en datapunkt med specifika variabelvärden som ska ”testas” om dessa tillhört träningsdatamängden eller inte. Detta kan båda vårdgivarna få fram från sitt egna träningsdata. Vidare behövs tillgång till den tränade globala modellen samt den egna träningsdatan, vilket båda vårdgivarna också har. För att utföra attacken krävs även att fördelningen av de hjärtsviktspatienter som ingår i träningsmängden från båda vårdgivarna har en någorlunda lika fördelning, dvs. delvis överlappar varandra. Till exempel behöver ålder och längd på vistelsetid vara någorlunda lika hos patienter från båda vårdgivarna.

För att genomföra en Membership Inference Attack börjar den attackerande parten med att undersöka vilka resultat som den globala maskininlärningsmodellen ger genom följande process.

- Datapunkter från den egna lokala träningsdatan (avseende riktiga hjärtsviktspatienter) och påhittade datapunkter som inte finns i träningsdatan matas in i den uppdaterade globala modellen för att få ut observationer som kopplar ihop datapunkter med sannolikheten för återinläggning.
- Med hjälp av information om dessa sannolikheter och kunskap om vilka datapunkter som matats in i den globala modellen, tränar den attackerande parten en så kallad skuggmodell (ytterligare en maskininlärningsmodell). Denna skuggmodell matas alltså i sin tur med samma datapunkter som tidigare för att modellen ska lära sig om en viss datapunkt tillhör träningsdatan eller inte.
- Därefter återanvänds skuggmodellen genom att matas med datapunkter från den egna träningsdatan och även närliggande datapunkter utanför träningsdatan för att uppskatta en sannolikhet om vilka andra datapunkter (dvs. uppgifter från hjärtsviktspatienter) som tillhör datamängden från båda

parterna. Vid det här skedet har den attackerande parten fått tillgång till personuppgifter om attacken lyckats (eftersom den andra partens träningsdata är personuppgifter).
- Genom att därefter utesluta datapunkterna från sin egna lokala träningsdata, kan man anta att resterande datapunkter (dvs. personuppgifter) förmodligen tillhör den andra partens träningsdata. Således kan man räkna ut vilka personuppgifter som härstammar från den andra parten.

Model Inversion Attack

Den andra metoden benämns Model Inversion Attack och syftar till att återskapa variabelvärdena i datapunkter från träningsdata.

Som beskrivits ovan innehåller den lokala träningsdatan personuppgifter. Genom en Model Inversion Attack finns en teoretisk möjlighet att i olika grad återskapa alla variabelvärden. Precis som vid en Membership Inference Attack är det en förutsättning att den attackerande parten har tillgång till a) den tränade globala modellen och b) sin egna lokala träningsdata – vilket båda vårdgivarna i detta projekt har.

I korthet går attacken till på följande vis:

1. Den attackerande parten börjar med att välja ut en slumpmässig datapunkt utifrån vissa kriterier.
2. Den slumpmässiga datapunkten matas in i den globala modellen som genererar ett resultat mellan 0 och 1 där siffran 0 innebär 0 procents sannolikhet för återinläggning och siffran 1 innebär 100 procents sannolikhet för återinläggning.
3. Därefter ändrar man successivt variabelvärdena i datapunkten så att resultatet från den globala modellen börjar närma sig 1 (dvs. 100 procents sannolikhet för återinläggning). Om man får ut ett tal som är nära 1 från modellens resultat ingår datapunkten sannolikt i träningsdatan.
4. Den attackerande parten upprepar steg 2–3 tills resultatet blir 1 eller strax därunder. På så sätt går det att fastställa att en viss datapunkt sannolikt har ingått i träningsdatan.

Vid en Model Inversion Attack skulle man något förenklat kunna säga att den attackerande parten vänder på maskininlärningsmodellen. Genom att använda sig av modellens slutresultat beräknar man alltså fram de variabelvärden som från början har matats in i maskinlärningsmodellen.

Genom att utesluta den egna träningsdatan kan man få fram de personuppgifter som finns i den andra partens träningsdata.

4.3 IMY:s bedömning

IMY bedömer att det, under de förutsättningar som funnits i det aktuella projektet, finns en risk för att de lokala vikterna ”minns” personuppgifter och att personuppgifter därmed lämnas ut till den andra vårdgivaren genom ovan beskrivna process. Detta kan ske genom de två beskrivna attackmetoderna. Även om det är omständligt kan det i det aktuella fallet göra det möjligt för en attackerande part att få fram personuppgifter från den andra parten.

Sammanfattningsvis kan det enligt IMY inte uteslutas att den federerade maskininlärningen i det aktuella fallet innebär att vårdgivarna ges tillgång till varandras personuppgifter. Detta utlämnande av patientuppgifter utgör en personuppgiftsbehandling som, för att vara tillåten, måste ha stöd i

dataskyddsförordningen samt kompletterande nationell rätt. Läs mer om den bedömningen i avsnitt 5 nedan.

4.4 Möjliga spår att undersöka vidare i utvecklingen av federerad maskininlärning

Pilotprojektet har visat att användningen av federerad maskininlärning under de förutsättningar som varit aktuella i projektet *Decentralized AI in Health Care - Federerad inlärning mellan två vårdgivare* riskerar att innebära att parterna ges tillgång till varandras personuppgifter. Detta innebär inte att samma slutsats är giltig för alla former av federerad maskininlärning.

Det finns flera områden som kan vara relevanta att utveckla vidare i syfte att höja integritetsskyddet vid användning av federerad maskininlärning. Bland annat kan nämnas följande faktorer, som dock inte undersökts närmare inom ramen för pilotprojektet.

- Utveckling av tekniken i en riktning som påverkar vikternas förmåga att lagra personuppgifter, till exempel genom att begränsa modellens komplexitet och träning för att minska risken för så kallad *överträning*.
- Utveckling av medel för att motverka användning av attacker eller andra metoder som möjliggör att personuppgifter kan återskapas från modellen.
- Riskreduktion genom säkerhetsåtgärder.
- Användning av metoder för att anonymisera personuppgifter genom utveckling av teknik som exempelvis differential privacy (en teknik som i korthet går ut på att man lägger på ett så kallat ”brus” på data för att minska risken att personuppgifter kan återidentifieras).

5. Finns det rättslig grund för utlämnande av personuppgifter mellan vårdgivarna?

Som konstaterats kan båda vårdgivarna anses komma att lämna ut personuppgifter till varandra i samband med att vikterna överförs mellan dem genom den iterativa process som beskrivs i avsnitt 4 ovan. Att lämna ut personuppgifter till en annan personuppgiftsansvarig utgör en personuppgiftsbehandling. Varje personuppgiftsbehandling måste kunna stödjas på en rättslig grund för att vara laglig. Frågan som vi fokuserar på i detta avsnitt är därför om det finns någon rättslig grund som kan ge stöd för utlämnande av personuppgifter mellan vårdgivarna.

5.1 Rättslig bakgrund

Aktuella bestämmelser[25]

Dataskyddsförordningen
Artikel 6.1 e
Artikel 6.3
Artikel 9.2 h

Patientdatalagen
2 kap. 4 §
2 kap. 5 §

Offentlighets- och sekretesslagen
6 kap. 5 §
10 kap. 28 §
25 kap. 1 §

Bedömningen av om utlämnande av personuppgifter mellan vårdgivarna kan vara laglig ska göras på motsvarande sätt som för den lokala personuppgiftsbehandlingen enligt avsnitt 3 ovan. Sammanfattningsvis behöver följande överväganden göras.

Som tidigare nämnts utgör patientdata personuppgifter. För att få behandla personuppgifter krävs bland annat att behandlingen kan stödjas på någon av de rättsliga grunderna i artikel 6.1 i dataskyddsförordningen. Enligt IMY:s bedömning kan det utlämnande av personuppgifter som skulle ske mellan vårdgivarna i samband med att de tränar den aktuella maskininlärningsmodellen utgöra en uppgift av allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen. Enligt artikel 6.3 i förordningen krävs att grunden för behandlingen fastställs i EU-rätten eller i medlemsstaternas nationella rätt. På hälso- och sjukvårdsområdet har så skett i Sverige i bland annat hälso- och sjukvårdslagen och patientdatalagen.

Eftersom patientdata utgör känsliga personuppgifter och därför är förbjuden att behandla enligt huvudregeln, behöver något av undantagen i artikel 9.2 i dataskyddsförordningen vara tillämpligt. Som redovisats i avsnitt 3 ovan kan, enligt IMY:s bedömning, undantaget i artikel 9.2 h i förordningen vara aktuellt i detta sammanhang.

5.2 IMY:s bedömning

Enligt 2 kap. 4 § första stycket patientdatalagen får personuppgifter behandlas inom hälso- och sjukvården förutsatt att det sker för något av de tillåtna ändamålen i lagrummet.

[25] I listan anges endast de bestämmelser som diskuteras i förevarande avsnitt. Det finns även andra bestämmelser som är tillämpliga på den aktuella personuppgiftsbehandlingen. Vidare finns det bestämmelser som reglerar hur patientdata får lämnas ut (se till exempel 5 kap. 6 § patientdatalagen och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården [HSLF-FS 2016:40]). Som nämns i avsnitt 2.3 ovan har vi inom ramen för detta pilotprojekt inte granskat samtliga rättsliga frågeställningar som skulle kunna aktualiseras, till exempel om ett gemensamt personuppgiftsansvar skulle kunna finnas för den personuppgiftsbehandling som sker i den centrala servern. Listan ska alltså inte ses som uttömmande.

I avsnitt 3 ovan har konstaterats att den lokala behandlingen kan omfattas av 2 kap. 4 § första stycket 4 patientdatalagen om kvalitetsutveckling och kvalitetssäkring. Denna punkt föreskriver att personuppgifter får behandlas för ”att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten”.

Begreppet verksamhet avser enligt IMY:s bedömning den personuppgiftsansvariges egen verksamhet. Det skulle kunna hävdas att utlämnande av uppgifter mellan vårdgivarna behövs för den egna verksamheten. Att maskininlärningsmodellen kan tränas på personuppgifter som härstammar från den andra vårdgivaren är nämligen en förutsättning för att modellen ska kunna bli tillräckligt effektiv, dvs. uppnå en tillräckligt hög prestanda. Det är dock osäkert om ändamålsbestämmelsen i patientdatalagen kan tolkas så att den möjliggör även utlämnanden som är till nytta för den egna verksamheten. Detta särskilt som det i 2 kap. 5 § patientdatalagen finns särskild reglering om utlämnande av personuppgifter som behandlas med stöd av 2 kap. 4 §.

Av 2 kap. 5 § patientdatalagen framgår att personuppgifter som behandlas med stöd av något av ändamålen i 2 kap 4 § patientdatalagen också får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Av förarbetena framgår att bestämmelsen bland annat möjliggör sådant utlämnande som sker med stöd av bland annat 6 kap. 5 § och 10 kap. 28 § offentlighets- och sekretesslagen.[26] Enligt den förstnämnda bestämmelsen ska en myndighet på begäran av en annan myndighet lämna ut uppgifter som den förfogar över, förutsatt att uppgiften inte är sekretessbelagd. Det innebär att om Region Halland och Sahlgrenska Universitetssjukhuset, som båda är myndigheter, skulle begära ut patientdata från varandra med stöd av 6 kap. 5 § offentlighets- och sekretesslagen skulle detta eventuellt kunna vara möjligt under förutsättning att uppgifterna inte är sekretessbelagda. Generellt sett är dock patientdata inom hälso- och sjukvården sekretessbelagda uppgifter enligt 25 kap. 1 § offentlighets- och sekretesslagen. Att bryta sekretessen kräver stöd i lag eller annan författning.

IMY gör inom ramen för denna regulatoriska testverksamhet inte någon bedömning av om någon sekretessbrytande bestämmelse skulle kunna vara tillämplig i detta avseende. Vidare har IMY inte bedömt om det skulle kunna finnas rättslig grund för en vårdgivare att behandla personuppgifter från en annan vårdgivare, dvs. om Region Halland skulle kunna ha rättslig grund att behandla personuppgifter som kommer från Sahlgrenska Universitetssjukhuset och vice versa.

6. Reflektioner om att tillämpa dataskyddsregelverket på AI och annan ny teknik

Utifrån arbetet i pilotprojektet går det att göra några generella reflektioner om att praktiskt arbeta med innovation, AI och annan ny teknik och samtidigt säkerställa ett gott dataskydd. Dessa reflektioner bedöms som relevanta även när innovationsprocessen sker inom en och samma verksamhet.

- Ett **tvärfunktionellt arbete**, där juridisk och teknisk kompetens har ett nära samarbete med företrädare för kärnverksamheten, är helt avgörande för framgång.

[26] Prop. 2007/08:126 s. 229. Hänvisningarna i propositionen avser den tidigare gällande sekretesslagen (1980:100).

- En förhållandevis **djup förståelse för tekniken är nödvändig för att kunna göra relevanta rättsliga bedömningar**. Att juristerna tidigt i processen uppnår förståelse för hur den aktuella AI-tekniken är uppbyggd är ofta nödvändigt för att till exempel kunna bedöma grundläggande dataskyddsfrågor som när och för vilka syften personuppgifter behandlas.
- Precis som teknikerna behöver utbilda juristerna i hur tekniken fungerar, behöver **juristerna ha god pedagogisk förmåga att förklara dataskyddsregelverket** och hur det är uppbyggt**.** För att kunna bygga in ett gott dataskydd kan de som utvecklar tekniken till exempel behöva ha förståelse för dataskyddsregelverkets grundläggande principer, att varje personuppgiftsbehandling behöver stödjas på en rättslig grund etc. En skicklig dataskyddsjurist behöver därför utveckla god pedagogisk förmåga.
- Utöver att jurister behöver förstå tekniken och teknikerna förstå juridiken behövs **strukturer och verktyg för att säkerställa en gemensam förståelse** i arbetsgruppen. Enkla men konkreta metoder kan vara att till exempel gemensamt identifiera och definiera nyckelbegrepp i en ordlista, att avsluta möten med att sammanfatta, att föra gemensamma minnesanteckningar och att vara noga med att ge tid för kontrollfrågor.
- De övergripande rättsliga frågeställningarna kan sannolikt identifieras när arbetet inleds. En central del av det juridiska arbetet är dock att **löpande gå tillbaka till, och vid behov justera, de rättsliga frågeställningarna** som behöver utredas. Är frågorna som inledningsvis ställdes fortfarande relevanta? Vilka artiklar i dataskyddsförordningen kan vara tillämpliga? Finns kompletterande lagstiftning som behöver beaktas?
- Det kan också vara en god idé att löpande i processen **överväga om det finns fler, interna eller externa, intressenter som behöver involveras.** Det kan handla om andra expertmyndigheter, men även interna funktioner för till exempel arkiv, inköp, upphandling eller säkerhet. Det kan också vara relevant att hämta in stöd, vägledning eller inspiration från experter inom till exempel ett visst teknikområde.

7. Reflektioner om regulatorisk testverksamhet som arbetssätt

När IMY inledde arbetet med att ge stöd och vägledning till innovationsaktörer genomfördes en kartläggning för att förstå hur behoven såg ut.[27] I kartläggningen kunde vi konstatera bland annat att:

- Datadelning är den fråga som uppfattas medföra flest legala utmaningar för innovationsaktörer. Särskilt komplicerat uppfattas datadelning av aktörer inom hälso- och sjukvården, som ofta hanterar känsliga personuppgifter vilka omfattas av stark sekretess.
- Det finns en stor efterfrågan på vägledning och rättsliga ställningstaganden från IMY. Många privata och offentliga verksamheter som arbetar med innovation vill se att IMY blir bättre på att förstå specifika teknikområden.
- Många önskar sig praktiskt stöd i innovationsprocessen genom fördjupad dialog och möjlighet att diskutera faktiska praktikfall med IMY.

[27] Delredovisning av uppdrag om kunskapshöjande insatser till innovationssystemet om integritets- och dataskyddsfrågor (imy.se).

När vi nu genomfört IMY:s första pilotprojekt med regulatorisk testverksamhet är den övergripande slutsatsen att arbetssättet skapar nytta och lärande både för de aktuella verksamheterna och för tillsynsmyndigheten.

Både IMY och de deltagande parterna har upplevt dialogformatet som värdeskapande. Arbetet i pilotprojektet har präglats av ett utforskande och prestigelöst klimat som lagt en god grund för ömsesidigt lärande. IMY:s bedömning är att regulatorisk testverksamhet skapar nytta för innovatörer, för myndigheter, som tolkar och tillämpar regelverk, och för samhället i stort.

För innovatörer är nyttan att de får bättre, mer och tidig vägledning och stöd kring hur regelverket bör tolkas och tillämpas. Tid kan sparas och risker reduceras, vilket innebär att verksamheterna snabbare och på ett säkrare sätt kan dra nytta av AI och annan modern teknik. Genom att resonemang och bedömningar dokumenteras och delas kan också fler än de som ingår i den regulatoriska testverksamheten få vägledning och dra nytta av lärdomarna från arbetet.

Region Halland, Sahlgrenska Universitetssjukhuset och AI Sweden uppger att de upplevt pilotprojektet som mycket positivt. De har fått värdefull vägledning, både genom de frågor som IMY ställt och de bedömningar som gjorts. Även om bedömningarna inte ger några slutliga svar uppger de att de fått en fördjupad förståelse som är användbar i deras fortsatta arbete med att utveckla användningen av AI inom hälso- och sjukvården.

För myndigheten är det stora mervärdet en ökad kunskap om och förståelse för innovativ teknik och de rättsliga frågor och utmaningar som uppstår i tillämpningen av tekniken.

Pilotprojektet har bidragit till stort lärande för IMY och gett en fördjupad förståelse för AI i allmänhet och federerad maskininlärning i synnerhet. Det har också gett viktiga insikter om hur vi som tillsynsmyndighet kan utveckla vårt arbete med att ge användbar vägledning och stöd till innovationsaktörer.

På samhällsnivå bedöms regulatorisk testverksamhet vara ett konkret sätt att främja innovation och utveckling av ny teknik och samtidigt bidra till att säkerställa dataskydd och informationssäkerhet. Arbetssättet är inte ensamt lösningen, men kan vara en pusselbit för att öka takten i Sveriges konkurrenskraft och digitala omställning och bidra till hållbara tekniklösningar som medborgarna kan känna tillit till.

Regulatorisk testverksamhet skulle också kunna leda till att behov av att ändra regleringen uppmärksammas. Tillsynsmyndigheten skulle i sådana fall kunna återkoppla detta till lagstiftaren.

En risk som IMY identifierat med begreppet regulatorisk testverksamhet är att det från vissa verksamheter kan finnas missuppfattningar eller orealistiska förväntningar kring vad arbetssättet innebär. Så har inte varit fallet i pilotprojektet, men i dialog med andra innovationsaktörer har vi ibland stött på den felaktiga bilden att regulatorisk testverksamhet på dataskyddsområdet innebär dispens från gällande regler.

Det kan också finnas en risk att verksamheter som ansöker till den regulatoriska testverksamheten har en förväntan om att fördjupad vägledning alltid kommer resultera i att den önskade personuppgiftsbehandlingen, på något sätt, kan genomföras. Erfarenheterna från de europeiska dataskyddsmyndigheter som drivit sin

regulatoriska testverksamhet en längre tid är dock att bedömningen i vissa fall kan utmynna i att det saknas rättsligt stöd för den tänkta personuppgiftsbehandlingen.

För IMY:s vidkommande, och andra myndigheter som överväger att starta ett arbete med regulatorisk testverksamhet, blir därmed en viktig uppgift att tydligt kommunicera vad arbetssättet innebär och vad deltagarna kan förvänta sig.

Sammanfattningsvis är IMY:s erfarenheter av pilotprojektet positiva, och vi har för avsikt att under 2023 genomföra ytterligare ett pilotprojekt.

Värt att notera är att arbetssättet är resursintensivt och förutsätter att både tillsynsmyndigheten och de verksamheter som ingår i den regulatoriska testverksamheten kan avsätta de resurser som krävs. I det budgetunderlag IMY lämnat till regeringen i mars 2023 har vi därför yrkat om en förstärkning av myndighetens anslag för att under 2024–2026 kunna skala upp arbetet med regulatorisk testverksamhet och göra det möjligt för fler privata och offentliga verksamheter att få den här typen av fördjupad vägledning.[28]

[28] *Integritetsskyddsmyndighetens budgetunderlag 2024-2026*, s. 6-9, IMY 2023-2407