



JURIDISKA FAKULTETEN

VID LUNDS UNIVERSITET

Izabella Bugsby de la Varga

En balans mellan individuell  
autonomi och kollektivt intresse av  
sekundär användning av e-hälsodata

En analys av EHDS-förordningen  
samt dess förhållande till rätten till radering

JURM02 Examensarbete

Examensarbete på juristprogrammet

30 högskolepoäng

Handledare: Petra Müllerová

Termin: VT 2024

# Innehåll

<b>Summary</b> .....	4
<b>Sammanfattning</b> .....	6
<b>Förord</b> .....	8
<b>Förkortningar</b> .....	9
<b>1 Inledning</b> .....	10
1.1 Bakgrund.....	10
1.2 Syfte och frågeställningar .....	12
1.3 Avgränsningar .....	13
1.4 Metod och material .....	14
1.5 Forskningsläge .....	16
1.6 Disposition .....	18
<b>2 Europeiska hälsodataområdet</b> .....	19
2.1 Bakgrund.....	19
2.2 Terminologi.....	20
2.2.1 E-hälsodata.....	20
2.2.2 Sekundär användning.....	21
2.2.3 Hälsodatainnehavare .....	22
2.2.4 Hälsodataanvändare .....	22
2.2.5 Hälsodataåtkomstorgan.....	22
2.3 Sekundär användning av e-hälsodata .....	23
2.3.1 Utgångspunkter.....	23
2.3.2 Tillgängliga e-hälsodatakategorier .....	24
2.3.2.1 Minimikategorier.....	24
2.3.2.2 Ytterligare kategorier .....	25
2.3.2.3 Datasetskataloger .....	26
2.3.3 Ändamål för vilka e-hälsodata får behandlas .....	27
2.3.4 Åtkomst till e-hälsodata .....	28
2.3.4.1 Datatillstånd .....	28
2.3.4.2 Begäran om hälsodata .....	30
2.3.4.3 Åtkomstgodkännande av en auktoriserad deltagare i Hälsodata@EU .....	31
2.3.5 Användning och hantering av e-hälsodata.....	31
2.3.5.1 Säker behandlingsmiljö.....	31
2.3.5.1 Uppgiftsminimering .....	32
2.3.5.2 Anonymisering och pseudonymisering.....	32
2.4 Opt-out rätt .....	34

2.4.1	Innebörd .....	34
2.4.2	Undantag .....	35
<b>3</b>	<b>Rätten till radering .....</b>	<b>37</b>
3.1	Costeja v. Google .....	37
3.2	Artikel 17 GDPR .....	39
3.2.1	Utgångspunkter .....	39
3.2.2	Grunder för rätt till radering .....	40
3.2.2.1	Behandling är inte längre nödvändig för de ursprungliga ändamålen .....	40
3.2.2.2	Återkallat samtycke .....	41
3.2.2.3	Invändning mot behandling .....	42
3.2.2.4	Olaglig behandling .....	43
3.2.2.5	Rättslig förpliktelse .....	44
3.2.3	Begränsningar av rätten till radering .....	44
3.2.3.1	Utövande av yttrande- och informationsfrihet .....	44
3.2.3.2	Uppfyllande av rättslig förpliktelse, utförande av uppgift av allmänt intresse eller led i myndighetsutövning .....	45
3.2.3.3	Viktigt allmänt intresse på folkhälsoområdet .....	46
3.2.3.4	Arkivändamål av allmänt intresse eller av vetenskapliga, historiska eller statistiska ändamål .....	46
3.2.3.5	För att kunna fastställa, göra gällande eller försvara rättsliga anspråk. ....	47
3.2.4	Bedömning och genomförande av radering .....	47
3.2.5	Utmaningar .....	48
3.2.5.1	Rättighetens tolkning och implementering .....	48
3.2.5.2	Privat aktör bedömer rättigheten .....	48
3.2.5.3	Intresseavvägningar .....	49
3.2.5.4	Tekniska utmaningar .....	49
<b>4</b>	<b>Radering av e-hälsodata vid sekundär användning .....</b>	<b>50</b>
4.1	E-hälsodata som känslig personuppgift .....	50
4.2	Begära radering .....	53
4.3	Grunder för rätt till radering .....	54
4.4	Begränsningar av rätt till radering .....	57
4.5	Sammanfattande kommentarer .....	58
<b>5</b>	<b>Avslutande diskussion .....</b>	<b>60</b>
	<b>Käll- och litteraturförteckning .....</b>	<b>66</b>
	<b>Rättsfallsförteckning .....</b>	<b>75</b>

## Summary

Secondary use of e-health data is an important step in directly and indirectly strengthening healthcare, both in Sweden and the EU. The anticipated EU regulation on a European Health Data Space (EHDS) will create a common health data space, allowing for the secondary use of the e-health data of up to 450 million EU citizens for research, innovation, and decision-making. This has the potential to revolutionize the healthcare sector through the development of new medicines, treatment methods, and much more.

Access to individuals' e-health data is crucial for the health data area, requiring trust in the system. Since e-health data comprises sensitive personal information, individuals' trust in the collection, handling, and use of their data is fundamental. Therefore, it is relevant to investigate privacy issues and data protection requirements. Additionally, it is pertinent to examine how individuals' rights under GDPR, such as the right to erasure, can be applied and fulfilled for various treatments conducted under EHDS regulations.

Using a legal dogmatic method and an EU legal method, the essay examines the EHDS regulation in order to analyze the relationship between the secondary use of e-health data and the right to erasure under GDPR.

Firstly, the extent to which the right to erasure under Article 17 GDPR can be applied to the secondary use of e-health data under EHDS is examined. The right to erasure is assessed based on the specific circumstances of each case and the conditions set out in Article 17 GDPR. Since e-health data is processed in multiple stages during secondary use, it is the responsibility of each data controller to make this assessment. The right to erasure may apply if e-health data is not sufficiently anonymized and a basis for erasure under Article 17.1 GDPR exists. However, the right to erasure has a very limited application because secondary use of e-health data relies on the data being shared in anonymized or pseudonymized form to prevent re-identification. Even if e-health data can still be traced to an individual and a basis for erasure exists, the right to erasure is still limited in the context of secondary use under the EHDS, due to possible restrictions under Article 17.3 GDPR when the processing is for public health purposes and public interest.

Secondly, the impact of the opt-out mechanism on the right to erasure is investigated, including whether it excludes or guarantees this right. Article 35f EHDS introduces an opt-out mechanism allowing individuals to choose at any time and without reason to opt out of their e-health data being used for secondary purposes. Comparing this with the right to erasure and considering its limited application, the thesis concludes that the opt-out mechanism can be seen as excluding the right to erasure in the context of secondary use.

The thesis concludes that the conditions for individuals' control and participation in the health data area are high, despite the limited application of the right to erasure. The introduction of the opt-out mechanism, along with other protective measures under the EHDS, provides individuals with increased control and autonomy over the use of their e-health data, thereby enhancing the system's credibility, security, and accessibility.

# Sammanfattning

Sekundär användning av e-hälsodata är ett viktigt steg i att direkt och indirekt stärka vården, både inom Sverige och EU. Inom kort förväntas den uppmärksammade EU-förordningen om ett European Health Data Space (EHDS) antas. Genom förordningen kommer ett gemensamt hälsodataområde skapas vilket bland annat möjliggör sekundär användning av uppemot 450 miljoner EU-medborgares e-hälsodata för exempelvis forskning, innovation och beslutfattande. Något som kan revolutionera hälso- och sjukvårdssektorn då nya mediciner, behandlingsmetoder och så vidare kan utvecklas.

Hälsodataområdet bygger således på tillgång till enskildas e-hälsodata och för god tillgång krävs ett förtroende för systemet. E-hälsodata består av känsliga personuppgifter och enskildas tillit till insamling hantering och användning av deras e-hälsodata blir därmed grundläggande. På så sätt är det relevant att utreda integritetsrättsliga frågor samt frågor kopplade till gällande dataskyddskrav. Det är vidare högst aktuellt att utreda hur enskildas rättigheter enligt GDPR, såsom rätten till radering, kan appliceras och tillgodoses för olika behandlingar som genomförs med stöd av EHDS:s bestämmelser.

Genom en rättsdogmatisk metod och en EU-rättslig metod undersöker uppsatsen på så vis EHDS-förordningen i syfte att analysera förhållandet mellan sekundär användning av e-hälsodata och rätten till radering enligt GDPR.

För det första utreds i vilken utsträckning rätten till radering enligt artikel 17 GDPR kan tillämpas vid sekundär användning av e-hälsodata enligt EHDS. Den enskildes eventuella rätt till radering av e-hälsodata ska bedömas utifrån omständigheterna i det konkreta fallet mot bakgrund av de i artikel 17 GDPR angivna förutsättningarna. Eftersom e-hälsodata behandlas i flera led vid sekundär användning är det upp till respektive personuppgiftsansvarige att göra den här bedömningen. En rätt till radering kan föreligga om e-hälsodata inte är avidentifierad i den grad att de inte utgör en personuppgift och en grund för radering enligt artikel 17.1 GDPR föreligger. På så vis har rätten till radering en mycket begränsad tillämpning eftersom sekundär användning av e-hälsodata bygger på att e-hälsodata delas i anonymiserad eller pseudonymiserad form för att förhindra en återidentifiering av den enskilde. För de fall e-hälsodata fortfarande går eller skulle kunna gå att härleda till en enskild individ och en grund för radering anses föreligga bedöms rätten till radering fortfarande limiterad i kontexten av sekundär användning enligt EHDS. Detta eftersom en begränsning av rätten till radering enligt artikel 17.3 GDPR mycket troligt anses föreligga vid sekundär användning av e-hälsodata. Detta eftersom behandling utifrån de i EHDS accepterade ändamålen för sekundär användning relaterar till folkhälsoändamål och samhällsintresset av att behandla uppgifterna.

För det andra undersöks huruvida opt-out mekanismen påverkar rätten till radering, alternativt om den kan anses exkludera eller garanterar rättigheten. Genom att en möjlighet för enskilda att opt-out införs i artikel 35f EHDS kan enskilda när som helst och utan att ange skäl välja att avstå från att deras e-hälsodata används för sekundär användning. Vid en jämförelse med rätten till radering samt med beaktande av rättighetens begränsade tillämpning på området kommer uppsatsen fram till att opt-out mekanismen kan anses exkludera rätten till radering vid sekundär användning.

Uppsatsen konkluderar att förutsättningarna för individers kontroll och delaktighet i hälsodataområdet är höga trots att rätten till radering har en begränsad tillämpning i sammanhanget. Detta då opt-out möjlighetens introducerande, tillsammans med övriga skyddsåtgärder enligt EHDS, ger enskilda ökad kontroll och självbestämmande över användning av deras e-hälsodata. Något som även kan bidra till systemets trovärdighet, säkerhet och tillgänglighet.

# Förord

Att blicka tillbaka på mina fem år på juristprogrammet i Lund framkallar en känsla av stolthet, lycka och tacksamhet. Genom detta arbete markeras inte enbart slutet på en fantastisk studietid utan även början på nästa spännande kapitel. Innan dess vill jag hinna tacka ett flertal personer som bidragit till att jag är den jag är idag och inom kort även jurist.

Först och främst vill jag rikta ett stort tack till min handledare Petra Müllerová som ständigt har funnits där med värdefulla råd, uppmuntrande ord och inte minst ett stort engagemang.

Till mina kompisar, för vad vore Lund utan er egentligen? Tack till alla som förgyllt min studietid både på och utanför Juridicum. Ett särskilt tack till Nabbe, Moa, Felicia och Calle för värdefull vänskap, oförglömliga minnen och sena kvällar. Gracias a Barcelona, ViaLaietana52 y a todas las personas maravillosas que hoy son unos de mis mejores amigos.

Jag vill även tacka min familj vars stöd varit ovärderlig i förverkligandet av den här uppsatsen. Tack mormor för att du alltid tror på mig. Tack Adrian för att du är den absolut bästa lillebror en storasyster någonsin skulle kunna önska sig. To James for always being there for me, no matter the time zone. Thank you for believing in me and never saying no to yet another adventure.

För att spara det bästa till sist, mamma. Utan dig hade inget varit möjligt. Tack för att du alltid finns där för mig oavsett var, när och hur. Du är min inspiration, förebild och bästa vän sedan dag ett. Te amo mami!

Lund, 21 maj 2023

*Izabella Bugsby de la Varga*



# Förkortningar

AI	Artificiell intelligens
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
EDPB	European Data Protection Board / Europeiska dataskyddsstyrelsen
EHDS	European Health Data Space / Europeiska hälso-dataområdet
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol
EU-kommissionen	Europeiska unionens kommission
EU-parlamentet	Europeiska unionens parlament
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
FEUF	Fördraget om Europeiska unionens funktionssätt
Förslag till EHDS	Förslag till Europaparlamentets och Rådets förordning om ett europeiskt hälsodataområde (COM (2022) 197 final), (SWD (2022) 132 final), Europeiska kommissionen, Bryssel den 3/5 2022.
GDPR	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 (dataskyddsförordningen)
Rådet	Europeiska unionens råd
Smer	Statens medicinsk-etiska råd
SOU	Statens offentliga utredningar

# 1 Inledning

## 1.1 Bakgrund

Den 3 maj 2022 presenterade EU-kommissionen sitt förslag till förordning avseende ett European Health Data Space (EHDS).<sup>1</sup> Förordningen förväntas träda i kraft inom kort och i skrivande stund väntar den preliminära överenskommelse på ett slutligt godkännande av Rådet, efter att ha godkänts av parlamentet den 24 april 2024.<sup>2</sup> EU har under en längre tid uttryckt sin ambition att etablera ett europeiskt hälsodataområde som det första i en rad tilltänkta domänspecifika europeiska dataområden och som ett steg på vägen mot en europeisk hälsounion.<sup>3</sup> Hälsodataområdet avser inte enbart utöka individens åtkomst och kontroll över sin hälsodata på nationell och EU-nivå för hälso- och sjukvårdsändamål (primär användning), utan avser även möjliggöra en förbättrad och bredare återanvändning av hälsodata för forskning, innovation och beslutsfattande inom EU (sekundär användning).<sup>4</sup> Något som bidragit till att ett gemensamt hälsodataområde beskrivs som en milstolpe i EU:s digitala transformation och en revolution i den europeiska medicinska historien.<sup>5</sup>

Att hälsodata i större utsträckning kan göras tillgänglig för bland annat forskare, vårdpersonal och beslutsfattare inom EU är önskvärt.<sup>6</sup> Genom sekundär användning kan hälsodata bland annat ha en avgörande roll i utvecklandet av AI-baserade verktyg i vården, läkemedel, vaccin, e-hälsa, life science och precisionsmedicin.<sup>7</sup> En ökad kunskap om sjukdomar och ohälsa kan nås, vilket bidrar till fördjupade kunskapsunderlag och mer evidensbaserade vårdbeslut. Något som i sin tur kan förebygga, behandla och bota sjukdomar i större utsträckning samt förbättra hälso- och sjukvårdens tillgänglighet, effektivitet och hållbarhet.<sup>8</sup> Därigenom är det även tänkbart att nationella vårdkriser där

---

<sup>1</sup> Förslag till Europaparlamentets och Rådets förordning om ett europeiskt hälsodataområde, COM(2022) 197 final av den 3 maj 2022.

<sup>2</sup> Regulation (EU) 2024/... of the European parliament and of the council on the European health data space, 2022/0140(COD), 7553/24, Bryssel, 18 mars 2024; Se även Europeiska rådet, *Det europeiska hälsodataområdet: rådet och parlamentet överens*, pressmeddelande, 15-03-2024; EU parlamentet, *EU Health Data Space to support patients and research*, pressmeddelande, 15-03-2024; EU parlamentet, *EU Health Data Space: more efficient treatments and life-saving research*, pressmeddelande 24-04-2024.

<sup>3</sup> Europeiska datasstrategin (2020).

<sup>4</sup> EU-kommissionen, *Assessment of the EU Member States' rules on health data in the light of GDPR, DG Health and Food Safety*, 2021, s. 57.

<sup>5</sup> EU-kommissionen, *Remarks by Vice-President Margaritis Schinas at the press conference on the European Health Data Space* (2022); EU-kommissionen, *Commission welcomes political agreement on European Health Data Space* (2024).

<sup>6</sup> Skäl 38 EHDS.

<sup>7</sup> Smer 2022:4 s. 2–3; N2019/03157 s. 17; Katrin Trysell, *Brist på hälsodata pekas ut som hinder för precisionsmedicin*, *Läkartidningen*, 17-11-2023.

<sup>8</sup> WHO, *Meeting on secondary use of health data*, 13 december 2022.

resurs- och kompetensbrist råder kan motverkas, vårdkvaliteten höjas och gränsöverskridande hälsohot bekämpas.

Hälso- och sjukvårdssektorn inom EU genererar och använder kontinuerligt stora mängder hälsodata. Något som dessutom ökar i takt med att den omfattande digitaliseringen som pågår inom hälso- och sjukvården öppnar upp för nya sätt att lagra, dela och sprida information om patienter. Bland annat genom en ökad inkorporeringen av digitala verktyg såsom elektroniska patientjournaler, e-recept och hälsoapplikationer.<sup>9</sup> Under Covid-19 pandemin blev det dock särskilt tydligt att det finns rättsliga, organisatoriska och tekniska hinder för att få tillgång till och dela hälsodata.<sup>10</sup> Vilket bidragit till att sekundär användning av hälsodata i dagsläget sker i en mycket begränsad omfattning. Många medlemsstater saknar dessutom adekvat lagstiftning på området i förhållande till dagens förutsättningar. Exempelvis bedöms Sveriges reglering vara bristfällig, utdaterad och svårtillämpad då den finns utspridd i flera olika författningar.<sup>11</sup> För att kunna nyttja den fulla potentialen av hälsodata krävs snabb tillgång och harmoniserade interoperabilitetskrav samtidigt som det bland annat måste säkerställas att hälsodata är överförbar, läsbar och användbar.<sup>12</sup> Därmed krävs ett lämpligt, säkert och tydligt regelverk som främjar innovation utan att för den skull äventyra individers förtroende för data-delning.

Hälsodata består av känslig information som kan avslöja mycket om en persons medicinska historia och hälsotillstånd. Vid sekundär användning av sådan data är det därmed av yttersta vikt att enskildas skydd för privatliv, integritet och data upprätthålls. Brister detta kan enskildas integritet hotas och allmänhetens förtroende för både sekundär användning i sig samt för hälso- och sjukvården i stort äventyras.<sup>13</sup> EU-kommissionen har dessutom betonat att tillit är en grundläggande faktor för hälsodataområdets framgång.<sup>14</sup> Därför är det avgörande att individer har kontroll över hur och när deras data används och behandlas. EU:s dataskyddsförordning (GDPR) skyddar individers rättigheter till sina personuppgifter, däribland personlig e-hälsodata, genom att ge enskilda en ökad kontroll över dessa.<sup>15</sup> I förordningens artikel 17 stadgas en rätt till radering, även känd som ”rätten att bli bortglömd”. Därigenom ges

---

<sup>9</sup> Se även Vision E-hälsa 2025 (2016).

<sup>10</sup> Gorska, Carrara, Davis, Bonten, W.Friedrich m.fl (2022).

<sup>11</sup> SOU 2023:76 s. 77 och 315.

<sup>12</sup> Jfr D. Wilkinson, Dumontier, Aalbersberg, Appleton m.fl, (2016) s. 1–9; skäl 3 EHDS.

<sup>13</sup> Skäl 3a EHDS.

<sup>14</sup> EU-kommissionen, *European Health Union: A European Health Data Space for people and science*, pressmeddelande, Bryssel, 3 maj 2022.

<sup>15</sup> Jfr skäl 4 EHDS.

enskilda en yttersta möjlighet att hävda skydd för sina personuppgifter genom att begära att dessa uppgifter ska raderas under vissa omständigheter.<sup>16</sup>

Vikten av att balansera hälsodataanvändares behov av omfattande och representativa dataset med individens autonomi över personlig e-hälsodata understryks allt mer. I vilken utsträckning enskilda ska ha kontroll över sekundär användning av sin egen hälsodata är dock en omdebatterad fråga som bland annat resulterat i splittrade synsätt mellan Rådet och Parlamentet. Något som även har medfört att en så kallad ”opt-out” klausul numera inkluderats i förslaget till EHDS. I EU-kommissionens ursprungliga förslag saknades nämligen en möjlighet för enskilda att avstå från att deras personliga e-hälsodata används för sekundär användning.

Både EU-rättslig och nationell reglering behöver oundvikligen hålla jämna steg med teknikutvecklingen för att förhindra att rättssäkerheten, etiken och patientsäkerheten riskeras. I och med det stundande inrättandet av EHDS behöver integritetsrättsliga frågor klarläggas för att säkerställa att sekundär användning av e-hälsodata inom EU främjas samtidigt som personers integritet och kontroll över sin data skyddas.

## 1.2 Syfte och frågeställningar

Uppsatsens syfte är att utreda och analysera förhållandet mellan gränsöverskridande sekundär användning av e-hälsodata enligt förslaget till EHDS och rätten till radering enligt GDPR. Vidare avser uppsatsen att undersöka den omdiskuterade opt-out mekanism som inkluderats i den provisoriska överenskommelsen avseende förslaget till EHDS och hur en sådan opt-out möjlighet kan påverka enskildas eventuella rätt till radering. Sekundär användning av e-hälsodata är ett viktigt steg i att direkt och indirekt stärka vården, både inom Sverige och EU. Därmed är det viktigt att utreda integritetsrättsliga frågor samt hur gällande dataskyddskrav och registrerades, det vill säga de personer vars uppgifter behandlas, rättigheter, såsom rätten till radering, kan appliceras i den här nya kontexten.

För att uppfylla syftet kommer följande frågeställningar besvaras:

- I vilken utsträckning kan rätten till radering enligt artikel 17 GDPR tillämpas vid sekundär användning av e-hälsodata enligt förslaget till EHDS?
- Påverkar opt-out mekanismen rätten till radering, alternativt exkluderar eller garanterar den?

---

<sup>16</sup> Axberger (2022) s. 238 ff.

### 1.3 Avgränsningar

För att uppnå mer konkreta och relevanta svar på ovan nämnda frågeställningar görs följande avgränsningar. Uppsatsen undersöker sekundär användning av e-hälsodata inom EU enligt förslaget till EHDS och dess angivna ändamål. Därmed utreds varken primär användning eller gränsöverskridande delning till ett tredje land. Sekundär användning av e-hälsodata för ändamål som faller utanför förslaget till EHDS behandlas inte heller, till exempel brottsbekämpning.<sup>17</sup> Fokus ligger på EU-rätt och ingen jämförelse av medlemsstaters nationella lagstiftning eller strukturer för sekundär användning av e-hälsodata kommer därmed att göras.<sup>18</sup> Medlemsstaters inställning till förslaget kommer inte heller att utforskas närmare. Både offentliga och privata aktörers förutsättningar för sekundäranvändning av e-hälsodata kommer granskas.

Det är den definition av e-hälsodata som anges i förslaget till EHDS som utgör utgångspunkten för uppsatsen. Således avser uppsatsen att undersöka den data som faller inom denna definition. Fokus ligger på vuxna personers e-hälsodata och aspekter som berör barns data och integritetsskydd kommer inte att diskuteras. Således kommer inte heller den utökade rätten att bli bortglömd för minderåriga i art. 17.1 f GDPR att diskuteras. Samtidigt som de generellt åtnjuter ett större skydd under GDPR har minderåriga begränsad rättshandlingsförmåga och autonomi.<sup>19</sup>

Till följd av uppsatsens omfång, och för att åstadkomma en mer detaljerad analys, kommer andra integritetsskyddande rättigheter såsom rätten till begränsning av behandling, rätten till insyn och information eller rätten till dataportabilitet inte att undersökas. Vidare står den enskildes kontroll och möjligheter till radering av e-hälsodata i fokus. Därmed analyseras inte personuppgiftsansvariges möjligheter eller skyldigheter att på eget initiativ radera sådana uppgifter. Det kommer inte heller att ske någon analys eller jämförelse kring hur rätten till radering implementerats i olika medlemsstater.

Sekundär användning av e-hälsodata som omfattar skyddade immateriella rättigheter och affärshemligheter kommer inte att analyseras.<sup>20</sup> Inte heller lagstiftning avseende offentlighet och sekretess kommer att analyseras. Därmed kommer de rättsliga förutsättningarna för att dela uppgifter som omfattas av sekretess, sekretessbrytande bestämmelser eller uppgiftsskyldighet som bryter sekretess inte att analyseras.

---

<sup>17</sup> Skäl 41a EHDS.

<sup>18</sup> Se Finnish Social and Health Data Permit Authority (Findata); Health Data Hub; The Danish Health Data Authority.

<sup>19</sup> Ausloos (2020) s. 152.

<sup>20</sup> Skäl 40c EHDS.

Pågående eller avslutade initiativ på EU-nivå avseende generella mekanismer för datadelning kommer inte utredas.<sup>21</sup> Således kommer inte möjligheten för offentliga myndigheter att erhålla data som innehas av privata aktörer i syfte att förebygga, reagera på eller hjälpa till att återhämta sig från offentliga nödsituationer enligt dataakten att behandlas.<sup>22</sup> Trots att ytterligare insikter om hälsobestämmande faktorer kan fås genom länkning av hälsodata med data från andra datarum såsom miljö, jordbruk och socialt, kommer sådan interoperabilitet inte att behandlas.<sup>23</sup>

Frågor med koppling till cybersäkerhet och cybersäkerhetskrav vid delning av e-hälsodata faller även det utanför uppsatsen och därmed även NIS2-direktivet.<sup>24</sup> Vidare kommer inte tekniska frågor kring tillgängliggörande av data eller formatfrågor att utredas närmare.<sup>25</sup> Kostnadsaspekter med anknytning till förslaget till EHDS eller datadelning i stort kommer inte heller att lyftas.

När det kommer till rätten till radering kommer uppsatsen inte att utreda enskildas tillgång till effektiva rättsmedel. Trots att detta utgör en viktig komponent i att säkerställa rätten till radering är uppsatsens fokus rättighetens applicering och inte enskildas möjligheter att genomdriva den. I uppsatsen görs ingen åtskillnad mellan rätten till radering och rätten att bli bortglömd utan de används synonymt och förutsätts ha samma innebörd.

## 1.4 Metod och material

Uppsatsen grundar sig i en rättsdogmatisk metod där skilda rättskällor undersöks och värderas i syfte att klargöra gällande rätt på området.<sup>26</sup> Eftersom förslaget till EHDS och GDPR utgör de centrala rättsakterna där frågeställningarnas besvarande tar sin utgångspunkt kommer även en EU-rättslig metod att användas. Genom användandet av en EU-rättslig metod kan EU-rätten granskas på ett lämpligt sätt då hänsyn tas till EU-rättens särskilda rättskälllära med en stark normhierarki som uppvisar vissa särdrag i förhållande till svensk rätt.<sup>27</sup> De EU-rättsliga rättskällorna består av primärrätt, sekundärrätt,

---

<sup>21</sup> Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsförordningen).

<sup>22</sup> Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen).

<sup>23</sup> Art. 52.12 EHDS och skäl 55b EHDS.

<sup>24</sup> Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

<sup>25</sup> Skäl 39 EHDS.

<sup>26</sup> Kleineman (2018) s. 21 ff.

<sup>27</sup> Reichel (2018) s. 110–111.

rättspraxis och doktrin. Primärrätten utgörs av EU:s fördrag, EU stadgan och EU-domstolens allmänna principer. Sekundärrätten har antagits med stöd av någon rättslig grund i EU-fördragen och ska tolkas mot bakgrund av primärrätten. Förordningar är en del av sekundärrätten och är bindande samt direkt tillämpliga för samtliga medlemsstater. När EU-rätt tolkas tillmäts EU-domstolens praxis stor betydelse.<sup>28</sup> Även doktrin kan användas för att kontextualisera och ge en mer nyanserad tolkning av de övriga rättskällorna.<sup>29</sup>

I uppsatsen används beaktandeskälerna i de relevanta regleringarna som vägledning för individuella bestämmelser samt för att belysa ändamålen bakom dessa. Det ska dock betonas att skälerna endast bör anses innehålla vägledande förklaringar och att de inte utgör bindande bestämmelser.<sup>30</sup> För att tillhandahålla fler perspektiv på frågeställningarna används även soft law i viss mån i form av icke-bindande rapporter och uttalanden från EU:s institutioner. Även om soft law inte är bindande kan det bidra till rättslig förståelse i väntan på att lagstiftaren tydliggör hur regelverket mer precist ska tolkas.<sup>31</sup> En del information har även hämtats från internetbaserade källor då ämnesområdet är relativt nytt och det råder brist på tryckta källor. I dessa fall har fakta som använts jämförts för att säkerställa dess tillförlitlighet.

Eftersom huvudsakligt fokus ligger på förslaget till EHDS utreds därmed en potentiell ny lagstiftning. Detta innebär att stor vikt läggs på utformningen samt det bakomliggande syftet med förordningen. Detta då det ännu inte finns rättspraxis eller mycket doktrin att tillgå rörande förordningen. Uppsatsen har därmed även analyserat samtliga versioner av förslaget till EHDS; EU-kommissionens förslag av den 3 maj 2022<sup>32</sup> (hädanefter EU-kommissionens förslag), Rådets version av den 6 december 2023<sup>33</sup> (hädanefter Rådets version), Parlamentets version av den 13 december 2023<sup>34</sup> (hädanefter Parlamentets version) och den provisoriska överenskommelsen som de medlagstiftande parterna enades om den 14 mars 2024<sup>35</sup> (hädanefter EHDS-förordningen). Utgångspunkt tas i sistnämnda provisoriska överenskommelse då det är denna som ligger till grund för omröstning och antagande. På så vis är det den här versionen som åsyftas om hänvisning inte görs till andra versioner. Skillnader

---

<sup>28</sup> Hettne & Otken-Eriksson (2011) s. 34 f.

<sup>29</sup> Hettne & Otken Eriksson (2011) s. 123 f.

<sup>30</sup> Hettne & Otken-Eriksson (2011) s. 41 ff., 85 och 93 f.; Reichel (2018) s. 125 f.

<sup>31</sup> Reichel (2018) s. 127 f.

<sup>32</sup> Förslag till Europaparlamentets och Rådets förordning om ett europeiskt hälsodataområde, COM(2022) 197 final av den 3 maj 2022.

<sup>33</sup> Proposal for a regulation of the European parliament and of the council on the European Health Data Space, 2022/0140(COD), 16048/1/23, Bryssel, 7 december 2023.

<sup>34</sup> Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)).

<sup>35</sup> Regulation (EU) 2024/... of the European parliament and of the council on the European health data space, 2022/0140(COD), 7553/24, Bryssel, 18 mars 2024.

mellan versionerna belyses i den grad de är relevanta i förhållande till uppsatsens syfte för att belysa övervägningarna och resonemang genom lagstiftningsprocessen.

För att tolka och klargöra GDPR samt rätten till radering används även ett antal riktlinjer från European Data Protection Board (EDPB). Trots att de inte har ställning som rättskälla tillmäts de likväl stor betydelse som tolkningsverktyg. EDPB ersatte den tidigare Artikel 29-gruppen efter GDPR:s ikraftträdande och är ett oberoende EU-organ som sammankopplar de nationella dataskyddsmyndigheterna och ser till att GDPR tillämpas enhetligt inom EU.<sup>36</sup> Enstaka yttranden och vägledningar utfärdade av Artikel 29-gruppen används i den mån de innefattar tolkningar som fortfarande bedöms aktuella. EU-kommissionen och EDPB använder sig fortfarande av dessa för att tolka GDPR.<sup>37</sup> Även doktrin används för att tolka GDPR och klargöra det som ovan nämnda källor inte besvarar.

## 1.5 Forskningsläge

Forskning kring e-hälsodata och sekundär användning är fortfarande begränsad, särskilt juridiskt. Litteratur avseende förslaget till EHDS är utöver detta knapphändig och behandlar inte rättsfrågor hänförliga till uppsatsens syfte och frågeställningar. På så vis finns det ett tydligt forskningsutrymme avseende sekundär användning av e-hälsodata och frågor förknippade med rätten till radering samt enskildas kontroll över sin egen e-hälsodata.

Fördelarna med sekundär användning av e-hälsodata för forskning och utveckling inom hälso- och sjukvårdssektorn lyfts i stor utsträckning. Vid sidan av detta läggs stort fokus i forskningen på förutsättningarna att skapa gemensamma digitala infrastrukturer på både nationell och EU-nivå för att möjliggöra delning av hälsodata. Med hänsyn till detta och utvecklandet av EHDS pågår exempelvis en utredning för att möjliggöra en svensk nationell digital infrastruktur för hela hälso- och sjukvården. Utredningen undersöker även befintliga rättsliga möjligheter till sekundäranvändning av hälsodata för vård och klinisk forskning samt föreslår lagändringar för utökade sådana möjligheter.<sup>38</sup> Därtill har E-hälsomyndigheten i uppdrag att ta fram ett förslag till färdplan för genomförandet av en nationell digital infrastruktur för hälso- och sjukvården.<sup>39</sup> Myndigheten för digital förvaltning (Digg) bedriver även arbete inom ramen för Ena, Sveriges digitala infrastruktur, i syfte att ta fram en

---

<sup>36</sup> EDPB, *Föregångare: Artikel 29-arbetsgruppen*; EDPB, *EDPB:s ordförandeskap*.

<sup>37</sup> Jfr EU-kommissionen, *Vad betyder "grundat på berättigat intresse"?*; Öman (2023), under rubriken EU-rättsligt källmaterial.

<sup>38</sup> SOU 2023:76; Dir. 2022:41.

<sup>39</sup> eHälsomyndigheten (2023).



sektorsövergripande digital infrastruktur.<sup>40</sup> Socialstyrelsen har också utfört en studie hur EHDS-förordningen kommer att påverka myndigheten.<sup>41</sup>

Det finns även ett antal multinationella EU-finansierade forskningsprojekt som berör data harmonisering och datadelning.<sup>42</sup> Kontinuerligt genomförs dessutom forskning som syftar att kartlägga medborgares syn på och inställning till delning av e-hälsodata. På EU-nivå har en arbetsgrupp inom ramen för Joint Action för EHDS (TEHDAS) fokuserat på EU-medborgarnas syn på hälsodata och gett föreslag på ökad transparens kring hälsodata.<sup>43</sup> Sveriges innovationsmyndighet Vinnova har också publicerat en rapport gällande svenska patienter kunskap om hälsodata. Här undersöks även vad som saknas och vilka områden som anses vara viktiga för att som patient känna tillit till att de hälsodata som hen varit med och genererat används på ett tryggt sätt.<sup>44</sup>

I takt med ett ökat intresse för personlig integritet och dataskydd har rätten till radering blivit ett alltmer populärt ämne för juridisk forskning. Det finns olika perspektiv avseende rättighetens innebörd, dess implementering och potentiella konsekvenser av dess tillämpning.<sup>45</sup> Främst har fokus legat på rätten att få personliga uppgifter raderade från internet till följd av rätten till privatliv. Exempelvis *The right to erasure in EU data protection law* av Jef Ausloos där huvudfokus ligger på internetleverantörer.<sup>46</sup> Ett fåtal artiklar finns publicerade där rättigheten diskuteras i förhållande till hälsodata.<sup>47</sup> Här bör särskilt nämnas *The right to be forgotten and Covid-19: Privacy versus public interest* av Mónica Correia, Guilhermina Rego och Rui Nunes. Där diskuteras om rätten till radering överhuvudtaget ska appliceras vid undantag för nödsituationer i dataskyddskontext och isåfall enligt vilka etiska överväganden.<sup>48</sup>

Till följd av det begränsade forskningsläget avseende sekundär användning av e-hälsodata enligt EHDS finns det en förhoppning om att framställningen kan klargöra förutsättningarna för sekundär användning. Vidare att uppsatsen kan ligga till grund för att förstå hur rätten till radering kan tillämpas på e-hälsodata vid sekundär användning samt dess relation till opt-out rätten. På så vis finns även en önskan om att uppsatsen kan bidra till den

---

<sup>40</sup> Myndigheten för digital förvaltning (Digg) (2023).

<sup>41</sup> Socialstyrelsen (2023).

<sup>42</sup> Reconciliation of Cohort data in Infectious Diseases (ReCoDID); Connecting European international cohorts to increase common and effective response to SARS-CoV2 Pandemic (ORCHESTRA); Unravelling Data for Rapid Evidence-Based Response to COVID-19) (un-CoVer); SYnergies for Cohorts in Health: integrating the ROle of all Stakeholders. (SYNCHROS).

<sup>43</sup> Tehdas, *Results*.

<sup>44</sup> Vinnova, *Patientens röst om hälsodata*, maj 2022.

<sup>45</sup> Wendleby (2021).

<sup>46</sup> Ausloos (2020).

<sup>47</sup> Se även Nordberg (2020).

<sup>48</sup> Correia, Rego & Nunes (2021).

samhällsjuridiska debatten och till att rättighetens omfattning klargörs i förhållande till sekundär användning av e-hälsodata samt fungera som vägledning vid tillämpning av den stundande EHDS-förordningen.

## 1.6 Disposition

Uppsatsen består av fem kapitel och inleds med en bakgrundsbeskrivning som ligger till grund för uppsatsens syfte och frågeställningar. Därefter presenteras de avgränsningar som gjorts, vald metod och material samt forskningsläge.

I kapitel två undersöks det europeiska hälsodataområdet och hur förslaget till EHDS avser att reglera sekundär användning av e-hälsodata. Först klargörs centrala begrepp såsom e-hälsodata och sekundär användning och sedan beskrivs de olika aktörernas roller i syfte att skapa en grundläggande förståelse för den sekundära användningen enligt EHDS-förordningen. Vidare sker en utförlig redogörelse av förutsättningarna för sekundär användning. På så vis skapas en solid grund för att förstå hälsodataområdets komplexitet avseende den sekundära användningen av e-hälsodata inom EU. Därefter utreds den nyligen införda bestämmelsen gällande enskildas möjlighet till opt-out.

I kapitel tre behandlas rätten till radering med fokus på artikel 17 GDPR. Här lyfts skyddet av den personliga integriteten fram, med särskild tonvikt på e-hälsodata som en särskilt känslig och skyddsvärd personuppgift. Kapitlet inleds med en beskrivning av rättighetens uppkomst. Sedan utreds förutsättningarna för att utöva rätten till radering, där villkor och begränsningar klargörs. Vidare analyseras praktiska problem som kan uppstå vid rättighetens tillämpning.

I kapitel fyra analyseras rätten till radering i förhållande till sekundär användning av e-hälsodata för att därigenom besvara uppsatsens första frågeställning. På så vis problematiseras grunderna för och begränsningarna av rätten till radering i syfte att utreda i vilken utsträckning rättigheten kan tillämpas vid sekundär användning av e-hälsodata.

I kapitel fem genomförs en avslutande diskussion kring opt-out mekanismens påverkan på rätten till radering i syfte att besvara uppsatsens andra frågeställning. Även de slutsatser som kan dras med beaktande av uppsatsens frågeställningar presenteras och framtida utmaningar identifieras.

## 2 Europeiska hälsodataområdet

### 2.1 Bakgrund

Tidigare har utbyte av elektroniska hälsouppgifter på EU-nivå till viss del behandlats i direktivet om gränsöverskridande hälso- och sjukvård (patientrörlighetsdirektivet).<sup>49</sup> I direktivets artikel 14 berörs e-hälsa och här anges att EU ska ”stödja och främja samarbete om och utbyte av information mellan medlemsstaterna inom ramen för ett frivilligt nätverk som kopplar ihop nationella myndigheter som är ansvariga för e-hälsa, utsedda av medlemsstaterna”.<sup>50</sup> Dock har direktivet både haft en begränsad inverkan på personers tillgång till och kontroll över sin e-hälsodata samt haft en låg effektivitet gällande den sekundära användningen av e-hälsodata. Något som kan förklaras av att det varit frivilligt för medlemsstater att ansluta sig till nätverket.<sup>51</sup>

Genom att tillhandahålla EU-gemensamma regler förväntas hälsodataområdet förhindra skillnader i nationella regelverk, strukturer och processer som försvårar tillgång till och delning av hälsodata. Området kan därmed bidra till interoperabilitet, harmonisering och ett gemensamt synsätt inom EU på användningen av elektronisk hälsoinformation då gemensamma standarder och praxis tillåts växa fram. Interoperabilitet innebär att olika organisationer, applikationer eller enheter från samma eller olika tillverkare kan samarbeta. Att det går att dela information och kunskap mellan dem utan att ändra datainnehållet under processens gång.<sup>52</sup>

Förordningen medger att det finns risker med förverkligandet av fördelarna med sekundär användning av e-hälsodata. Även om riskerna inte närmare preciseras får de anses kopplade till att känslig hälsodata kräver ett lämpligt skydd så att enskildas integritet upprätthålls.<sup>53</sup> Förordningen avser därmed att säkerställa dataskydd, säkerhet, konfidentialitet och etisk användning av personlig e-hälsodata. Detta genom att tillhandahålla nödvändiga skyddsåtgärder både på nationell nivå och EU-nivå. Något som dessutom avser främja personers förtroende för säker hantering av deras hälsodata vid sekundär användning.<sup>54</sup>

---

<sup>49</sup> Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

<sup>50</sup> Art. 14 patientrörlighetsdirektivet.

<sup>51</sup> Motivering p. 1 st. 5 EU-kommissionens förslag till EHDS.

<sup>52</sup> Art. 2.2 f EHDS.

<sup>53</sup> Skäl 37a EHDS.

<sup>54</sup> Skäl 3a EHDS.

## 2.2 Terminologi

### 2.2.1 E-hälsodata

E-hälsodata kan enligt förslaget till EHDS delas in i både personlig och icke-personlig e-hälsodata.<sup>55</sup> Personlig e-hälsodata definieras som uppgifter om hälsa och genetiska uppgifter enligt definitionerna i GDPR som behandlas i elektroniskt format.<sup>56</sup> Därmed en snävare definition i jämförelse med EU-kommissionens förslag som anger att även uppgifter avseende bestämningsfaktorer för hälsa, eller uppgifter som behandlas i samband med tillhandahållande av hälso- och sjukvårdstjänster omfattas.<sup>57</sup>

GDPR definierar uppgifter om hälsa som personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus.<sup>58</sup> På så vis består hälsodata generellt sett av alla de uppgifter som samlas in och dokumenteras inom hälso- och sjukvården som rör en persons tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Hit räknas journaluppgifter, testresultat och andra patientuppgifter, men även uppgifter som samlas in för forskningsändamål eller genom den enskilde patienten själv när denne exempelvis använder olika hälsoappar. En hälsoapp är varje anordning eller programvara som tillverkaren avser ska användas av en fysisk person för att behandla e-hälsodata, särskilt för att tillhandahålla information om enskilda personers hälsa eller för leverans av vård för andra ändamål än tillhandahållande av hälso- och sjukvård.<sup>59</sup> Uppgifter om hälsa kan även innebära resultat från alkoholtest, uppgifter om eventuella missbruk, graviditet, utskrivna läkemedel eller om någon har en funktionsnedsättning.<sup>60</sup> Uppgifterna är dock oberoende av källa och kan exempelvis ha samlats in från en läkare, annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.<sup>61</sup> Enligt EU-domstolen ska uppgifter om hälsa tolkas brett.<sup>62</sup>

Genetiska uppgifter enligt GDPR är alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför

---

<sup>55</sup> Art. 2.2 c EHDS.

<sup>56</sup> Art. 2.2 a EHDS.

<sup>57</sup> Art. 2.2 a EU-kommissionens förslag till EHDS

<sup>58</sup> Art. 4.15 GDPR.

<sup>59</sup> Art. 2.2 aea EHDS.

<sup>60</sup> EDPB-riktlinjer 03/2020 p. 7–8.

<sup>61</sup> Skäl 35 GDPR.

<sup>62</sup> C-101/01 *Lindqvist*, p. 50.

allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga.<sup>63</sup>

Icke-personlig e-hälsodata är hälsodata som faller utanför nyss nämnda definition av personlig e-hälsodata och omfattar både anonymiserad data som inte längre kan kopplas till en identifierad eller identifierbar fysisk person och data som aldrig har varit kopplad till den registrerade.<sup>64</sup> I EU-kommissionens förslag till EHDS beskrivs icke-personlig e-hälsodata inte utgöra en personuppgift enligt art. 4.1 GDPR. Alltså inte vara en uppgift som direkt eller indirekt kan identifiera en fysisk person. Därmed läggs stor betoning på att icke-personlig e-hälsodata inte ska vara möjlig att hänföra till en person.

### 2.2.2 Sekundär användning

Sekundär användning innebär behandling av e-hälsodata för ett av de ändamål som anges i kapitel tre i förslaget till EHDS. Detta ändamål ska skilja sig från det ändamål för vilka e-hälsodata samlades in eller producerades för.<sup>65</sup> EHDS definition av sekundär användning tar därmed inte avstamp i syftet för insamlingen utan för vilka ändamål e-hälsodata sedan avser att användas till. Alltså refererar sekundär användning till situationen när e-hälsodata som ursprungligen samlats in för ett specifikt syfte används på andra sätt eller för andra ändamål.

Enligt EU-kommissionens förslag till EHDS anges att både personlig e-hälsodata som ursprungligen samlades in i samband med primär användning och e-hälsodata som samlats in för sekundär användning omfattas.<sup>66</sup> Att sekundär användning kan omfatta både personlig e-hälsodata som samlats in för primär användning och för sekundär användning tycks dock även falla inom nuvarande definition då vikt läggs på syftet med användningen och inte syftet som e-hälsodatan samlades in för. På så vis kan sekundär användning även innebära en vidareanvändning av e-hälsodata som samlats in för primär användning. E-hälsodata som samlats in för primär användning utgörs av personlig e-hälsodata som är kopplade till att tillhandahålla hälso- och sjukvård till enskilda.<sup>67</sup> Informationen kan exempelvis avse kritiska hälsoaspekter som medicinska tillstånd och historik av läkemedelsanvändning, utförda procedurer, patientens hälsotillstånd och vaccinationer. Därmed även patientöversikter, elektroniska recept och deras expediering, medicinska bilder och bildrapporter, laboratorieresultat och utskrivningsrapporter.<sup>68</sup>

---

<sup>63</sup> Art. 4.13 GDPR.

<sup>64</sup> Art. 2.2 b EHDS.

<sup>65</sup> Art. 2.2 e EHDS.

<sup>66</sup> Art. 2.2 e EU-kommissionens förslag till EHDS.

<sup>67</sup> Art. 2.2 d EHDS.

<sup>68</sup> Jfr art. 5 EHDS.

### 2.2.3 Hälsodatainnehavare

En hälsodatainnehavare kan antingen vara en fysisk eller juridisk person, offentlig myndighet, organ eller annan enhet inom hälso- och sjukvård eller omsorgssektorn eller som bedriver forskning inom dessa sektorer.<sup>69</sup> Hit räknas också fysiska eller juridiska personer som utvecklar eller tillverkar produkter eller tjänster avsedda för hälso- och sjukvårdssektorn, inklusive hälsoappar. Även de som bedriver hälso- och sjukvårdsrelaterade forskning eller hanterar dödsfallsregister anses som hälsodatainnehavare, liksom institutioner, organ och byråer inom EU. Dessa aktörer kan antingen ha en rättighet eller skyldighet att behandla personliga e-hälsodata enligt nationell rätt eller EU-rätt eller så kan de ha tekniska möjligheter att hantera icke-personliga e-hälsodata genom att kontrollera designen av relevanta produkter och tjänster.<sup>70</sup> Termen hälsodatainnehavare är relativt allmänt hållen vilket innebär att samtliga individer, myndigheter, företag eller organisationer som är delaktiga i hälso- och sjukvården eller omsorgssektorn kan vara ansvariga för hantering av personuppgifter relaterade till hälsa och vård. Alltså kan datainnehavare bland annat vara enskilda forskare men även sjukhus, vårdcentraler, laboratorier, forskningsinstitutioner eller andra vårdgivare och organisationer inom hälso- och sjukvård oberoende av om de är offentliga, privata eller ideella.

### 2.2.4 Hälsodataanvändare

En hälsodataanvändare är en fysisk eller juridisk person som getts laglig tillgång till personliga eller icke-personliga e-hälsodata för sekundär användning. Det kan exempelvis röra sig om forskare, företag och institutioner. Även EU:s institutioner, organ och byråer omfattas. Laglig tillgång kan antingen erhållas genom ett datatillstånd, en begäran om hälsodata eller ett åtkomstgodkännande av en auktoriserad deltagare i Hälsodata@EU.<sup>71</sup>

### 2.2.5 Hälsodataåtkomstorgan

Ett hälsodataåtkomstorgan är ett organ med ansvar för tillgång till hälsodata och vissa utpekade arbetsuppgifter avseende sekundäranvändning av sådan data.<sup>72</sup> Enligt förslaget till EHDS ska varje medlemsstat utse ett sådant organ. Mer än ett organ kan utses men i sådana fall krävs samordning mellan dessa och att gemensamma rapporter förbereds och publiceras.<sup>73</sup> Hälsodataåtkomstorganet ska bland annat handlägga ansökningar om datatillstånd, säkerställa transparens i sekundär användning, tillhandahålla information för personer angående de villkor under vilka e-hälsodata görs tillgängliga för sekundär användning samt tillgängliggöra och upprätthålla en nationell datasetskatalog.<sup>74</sup>

---

<sup>69</sup> Art. 2.2 y EHDS.

<sup>70</sup> Skäl 40 EHDS.

<sup>71</sup> Art. 2.2 z EHDS.

<sup>72</sup> Jfr art. 36–37, 39, 42, 44–45, 47 EHDS.

<sup>73</sup> Art. 36 EHDS och skäl 42 och 44b EHDS.

<sup>74</sup> Skäl 44b EHDS.

Hälsodataåtkomstorgan ska dessutom vidta åtgärder såsom administrativa böter, efterlevnadsåtgärder eller uteslutningar från hälsodataområdet i upp till fem år om hälsodataanvändare eller hälsodatainnehavare inte uppfyller sina skyldigheter eller agerar i strid med regelverket.<sup>75</sup>

## 2.3 Sekundär användning av e-hälsodata

### 2.3.1 Utgångspunkter

Sekundär användning av e-hälsodata regleras i kapitel tre i förslaget till EHDS. Här lägger förordningen grunden för ett system baserat på att hälsodatainnehavare ska tillgängliggöra den hälsorelaterade information de innehar, antingen till följd av ett datatillstånd eller en begäran om hälsodata. Målet är att hälsodata som samlas in av vårdgivare, yrkesorganisationer, offentliga institutioner, regleringsorgan, företag för hälsoappar, forskare, försäkringsbolag, etc. i samband med deras verksamhet tillgängliggörs för sekundär användning.<sup>76</sup>

Genom att samtliga hälsodatainnehavare tillgängliggör olika kategorier av e-hälsodata som de innehar kan fördelarna med sekundär användning nyttjas under förutsättningar att det utförs genom effektiva och säkra processer. Därmed avser förordningen inte hindra eller ersätta befintliga avtal eller andra mekanismer utan möjliggör ett nytt system för att få tillgång till e-hälsodata för sekundär användning över hela EU.<sup>77</sup> Förordningen avser även bidra till att förtydliga mycket av den rättsliga osäkerhet avseende sekundär användning av e-hälsodata som orsakats av medlemsstaternas ojämna implementering och tolkning av GDPR.<sup>78</sup>

Individuella forskare och fysiska personer samt juridiska personer som är att anse som mikroföretag är emellertid undantagna de skyldigheter som åläggs hälsodatainnehavare enligt förordningen.<sup>79</sup> Ett mikroföretag är ett företag som sysselsätter mindre än 10 personer och vars omsättning eller balansslutning understiger 2 miljoner euro per år.<sup>80</sup> Hur som helst får medlemsstater genom nationell rätt utöka skyldigheterna till att även omfatta dessa aktörer om de omfattas av deras jurisdiktion.<sup>81</sup> Att kräva att dessa aktörer ska uppfylla samma krav som ställs på stora institutioner eller företag kan dock innebära

---

<sup>75</sup> Art. 43 EHDS och skäl 48 EHDS.

<sup>76</sup> Skäl 38 EHDS.

<sup>77</sup> Skäl 37 EHDS.

<sup>78</sup> Jfr motivering p. 1 st. 2 EHDS; EU-kommissionen (2021), s. 9 f.

<sup>79</sup> Art. 32a EHDS.

<sup>80</sup> Art. 2 i bilagan till kommissionens rekommendation 2003/361/EG.

<sup>81</sup> Art. 32a EHDS.

en oproportionerlig börda då dessa aktörer kan antas ha begränsad kapacitet och resurser.<sup>82</sup>

Medlemsstater får genom nationell rätt även besluta att vissa hälsodatainnehavare har möjlighet att fullgöra sina skyldigheter genom att förmedla arbetet till en förmedlingsenhet. Sådana enheter kan tillgängliggöra, registrera, tillhandahålla, behandla, begränsa åtkomst eller utbyta e-hälsodata som tillhandahålls av hälsodatainnehavare för sekundär användning. Om detta görs ska hälsodata fortfarande anses tillgängliggjord från flera datainnehavare.<sup>83</sup>

## 2.3.2 Tillgängliga e-hälsodatakategorier

### 2.3.2.1 *Minimikategorier*

EHDS ställer krav på hälsodatainnehavare att göra ett antal minimikategorier av e-hälsodata tillgängliga för sekundär användning.<sup>84</sup> Mot bakgrund av ett datatillstånd eller en begäran om hälsodata kan hälsodataåtkomstorgan begära att hälsodatainnehavare tillhandahåller dessa e-hälsodata inom tre månader.<sup>85</sup> Dessa kategorier bör vara tillräckligt omfattande och flexibla för att tillgodose hälsodataanvändares föränderliga behov samtidigt som de begränsas till hälsorelaterad data eller data kända för att påverka hälsan.<sup>86</sup>

Relevant data från hälso- och sjukvårdssystemet i form av elektroniska patientjournaler, data från sjukdomsregister och genetiska data ska inkluderas i dessa minimikategorier samt data som påverkan hälsan, såsom socioekonomiska, beteendemässiga och miljömässiga bestämningsfaktorer för hälsan.<sup>87</sup> Elektroniska patientjournaler utgörs av en uppsättning e-hälsodata om en fysisk person som har samlats in i hälso- och sjukvårdssystemet och som behandlas för tillhandahållandet av hälso- och sjukvård.<sup>88</sup> Här bör tilläggas att förordningen påpekar att personer bör kunna lägga till hälsoinformation i sina elektroniska patientjournaler men att sådan data bör särskiljas från den data som läggs in och verifieras av hälso- och sjukvårdspersonal då den inte är lika tillförlitlig. Det ska dock inte vara möjligt för personer att ändra information som hälso- och sjukvårdspersonal lagt in.<sup>89</sup> Data angående professionell status, specialisering och institution till hälso- och sjukvårdspersonal som deltar

---

<sup>82</sup> Jfr skäl 40 EHDS.

<sup>83</sup> Art. 32a EHDS.

<sup>84</sup> Art. 33.1 EHDS.

<sup>85</sup> Art. 41 EHDS.

<sup>86</sup> Skäl 39 EHDS.

<sup>87</sup> Art. 33.1 a–ea och skäl 39 EHDS.

<sup>88</sup> Art. 2.2m EHDS.

<sup>89</sup> Skäl 10 EHDS.



i en individs behandling ska även det tillgängliggöras för sekundär användning.<sup>90</sup>

Vidare faller automatisk genererade data från medicintekniska apparater och data som individer själva genererar genom hälsoappar inom minimikategorierna.<sup>91</sup> Så gör även vissa data som ursprungligen samlades in för andra ändamål som exempelvis forskning, statistik och patientsäkerhet. Även data från olika typer av register som exempelvis folkhälsoregister, medicinska register, dödsfallsregister och register över läkemedel och medicintekniska produkter omfattas.<sup>92</sup> Liksom annan data från medicintekniska produkter samt e-hälso-data från biobanker och associerade databaser.<sup>93</sup>

Data från kliniska provningar, studier och undersökningar kan delas frivilligt av hälsodatainnehavaren innan de avslutats men tillåts även tillgängliggöras först efteråt. Efter att resultat publicerats från forskningskohorter, frågeformulär och undersökningar med anknytning till hälsa ska data göras tillgänglig.<sup>94</sup> Det faktum att det ska röra sig om avslutade studier framkommer dock inte i bestämmelsen utan enbart i skälen till förordningen. Att det endast ska röra sig om studier genomförda efter ikraftträdandet av EHDS anges inte heller uttryckligen. Sist men inte minst ska även europeiska databaser som förklarar återanvändning av tillgängliga data inom vissa områden, bland annat cancer och sällsynta sjukdomar, inkluderas i minimikategorierna.<sup>95</sup>

I EU-kommissionens förslag inkluderas ytterligare två kategorier. Dels elektroniska data om försäkringsstatus, yrkesstatus, utbildning, livsstil, välbefinnande och beteende som är relevanta för hälsan. Dels e-hälso-data som innehåller olika förbättringar, till exempel korrigeringskommentar, beräkning, och som datainnehavaren har mottagit efter en behandling som grundar sig på ett datatillstånd.<sup>96</sup> Trots denna reducering av kategorier omfattar förslaget till EHDS fortfarande ett brett utbud e-hälso-data, som insamlats av både offentliga och privata aktörer, som kan bli aktuella för sekundär användning.

### 2.3.2.2 *Ytterligare kategorier*

Vid sidan av ovan nämnda minimikategorier ges medlemsstater möjlighet att genom nationell lagstiftning föreskriva ytterligare kategorier av e-hälso-data

---

<sup>90</sup> Art. 33.1 g EHDS.

<sup>91</sup> Art. 33.1 f-fa EHDS.

<sup>92</sup> Art. 33.1 h, i, k och ka EHDS.

<sup>93</sup> Art. 33.1 k och m EHDS.

<sup>94</sup> Art. 33.1 j och l EHDS och skäl 39 EHDS.

<sup>95</sup> Skäl 40 EHDS; European cancer information system (ECIS); European platform on rare disease registration (EU RD platform).

<sup>96</sup> Jfr art. 33.1 n och o EU-kommissionens förslag till EHDS.

som ska göras tillgängliga för sekundär användning.<sup>97</sup> Genom att ge medlemsstater detta utrymme blir omfattningen av tillgängliga e-hälsodata delvis en nationell fråga. Staterna ges ett stort bedömningsutrymme och därmed kan potentiellt tillgängliga kategorier av e-hälsodata för sekundär användning inom EU vara svåra att överblicka.

Medlemsstater har också möjlighet att introducera nationella åtkomstbegränsningar för vissa mer känsliga hälsodatkategorier som exempelvis genetisk data, biobanker och data från hälsoappar.<sup>98</sup> Att sådan data till följd av dess känslighet eventuellt anses behöva ytterligare skyddsregler riskerar att antyda att mindre känslig e-hälsodata inte är fullkomligt säkrade i hälsodataområdets system.

### 2.3.2.3 *Datasetskataloger*

Hälsodataåtkomstorgan ska tillgängliggöra och upprätthålla en nationell datasetskatalog med aktuell och strukturerad information om tillgängliga e-hälsodata och deras karaktär.<sup>99</sup> På så vis kan hälsodataanvändare se vilka hälsodata som finns tillgängliga för sekundäranvändning i en medlemsstat och därigenom bedöma deras eventuella användbarhet för dem. Varje dataset bör därför innehålla en beskrivning om källan, datans ursprung och villkoren för att data ska göras tillgänglig.<sup>100</sup> Genom dessa dataset kan tillgång till verklig data och dess evidens, inklusive patientrapporterade utfall, fås. Datasett bör därför vara så fullständiga som möjligt för att kunna skapa störst samhällsnytta genom att regelverk, policy, forskning och hälso- och sjukvårdsteknologi tillåts bygga på tillräcklig evidens.<sup>101</sup>

På EU-nivå ska även EU-kommissionen tillhandahålla en EU-datasetskatalog.<sup>102</sup> Därigenom kan upptäckten av tillgängliga dataset i hälsodataområdet förenklas vilket minskar administrationsbördan för användare av databaser samt ökar användarvänligheten, tillgängligheten och kostnadseffektiviteten.<sup>103</sup> Genom att medlemsstaterna i sin tur säkerställer interoperabilitet mellan EU:s datakatalog, de nationella datakatalogerna och datasetskataloger från europeiska forskningsinfrastrukturer kan onödig registrering av datamängder undvikas.<sup>104</sup>

---

<sup>97</sup> Art. 33.8 EHDS.

<sup>98</sup> Art. 33.5 EHDS.

<sup>99</sup> Art. 2.2 ab, art. 55 EHDS och skäl 44b EHDS.

<sup>100</sup> Skäl 58 EHDS.

<sup>101</sup> Skäl 37b EHDS.

<sup>102</sup> Art. 57.1 EHDS.

<sup>103</sup> Skäl 58 EHDS.

<sup>104</sup> Art. 57.2 EHDS och skäl 60 EHDS.

### 2.3.3 Ändamål för vilka e-hälsodata får behandlas

Det är först om det avsedda ändamålet med behandlingen av de e-hälsodata som den sökande hälsodataanvändaren eftersträvar överensstämmer med artikel 34 EHDS som tillgång till data kan ges. Det är på så sätt upp till hälsodataåtkomstorganet att, i samband med en ansökan om datatillstånd eller en begäran om hälsodata, pröva om behandlingen av begärd hälsodata är nödvändig för hälsodataanvändaren enligt någon av dessa ändamål.<sup>105</sup>

För det första är sekundär användning tillåten på grund av allmänintresse inom folkhälsa och företagshälsovård. Exempelvis kan åtkomst till e-hälsodata ges för att bidra till skydd mot allvarliga gränsöverskridande hälsohot såsom pandemier eller för övervakning av folkhälsan. Åtkomst kan även godkännas för att använda e-hälsodata i syfte att säkerställa en hög kvalitets- och säkerhetsnivå för hälso- och sjukvården samt för läkemedel eller medicintekniska produkter.<sup>106</sup> Företagshälsovård relaterar till arbetstagares hälsa och kan däribland avse tjänster för att säkerställa arbetstagares fysiska, mentala och sociala välmående i deras arbetsmiljö.<sup>107</sup>

För det andra kan e-hälsodata användas för beslutsfattande och regleringsverksamhet som stöd till offentliga myndigheter eller EU:s institutioner, byråer och organ, inklusive tillsynsmyndigheter, inom hälso- och sjukvårdssektorn eller omsorgssektorn för att de ska kunna utföra sina fastställda uppgifter.<sup>108</sup> För det tredje kan åtkomst till e-hälsodata ges för statistik med anknytning till hälso- och sjukvårdssektorn eller omsorgssektorn.<sup>109</sup>

För dessa tre uppräknade ändamål får dock åtkomst till e-hälsodata endast beviljas medlemsstaters offentliga myndigheter eller EU:s institutioner, organ, kontor och byråer som utövar sina uppgifter till följd av EU-rätt eller nationell rätt. Detta gäller även om databehandlingen för att utföra dess uppgifter utförs av en tredje part för deras räkning.<sup>110</sup>

För det fjärde kan åtkomst till e-hälsodata ges för utbildning eller undervisning i hälso- och sjukvårdssektorn eller omsorgssektorn på yrkesutbildningsnivå eller högre utbildningsnivå.<sup>111</sup>

För det femte kan vetenskaplig forskning med koppling till hälso- och sjukvårdssektorn eller omsorgssektorn utgöra en grund för beviljad åtkomst. E-hälsodatan ska då bidra till folkhälsan eller bedömning av hälso- och

---

<sup>105</sup> Art. 34.1 EHDS.

<sup>106</sup> Art. 34.1 a EHDS.

<sup>107</sup> WHO, *Occupational health*.

<sup>108</sup> Art. 34.1 b EHDS.

<sup>109</sup> Art. 34.1 c EHDS.

<sup>110</sup> Art. 34.2 EHDS.

<sup>111</sup> Art. 34.1 d EHDS.

sjukvårdsteknologi, eller säkerställa höga nivåer av kvalitet och säkerhet inom hälso- och sjukvården, av läkemedel eller medicintekniska produkter. E-hälsodatan ska därutöver syfta att gynna slutanvändarna, såsom patienter, hälso- och sjukvårdspersonal och hälsoadministratörer. Alternativt gynna utvecklings- och innovationsaktiviteter för produkter eller tjänster, eller gynna träning, testning och utvärdering av algoritmer bland annat inom medicintekniska produkter, in vitro-diagnostiska medicintekniska produkter, AI-system och digitala hälsoapplikationer.<sup>112</sup> På så sätt bör sekundär användning för forskningsändamål bidra till någon form av samhällsnytta. Exempelvis i form av nya läkemedel, medicintekniska produkter, hälsovårdsprodukter och tjänster för EU-medborgare.<sup>113</sup> Att forskningen ska vara vetenskaplig bör tolkas brett och inkluderar teknologisk utveckling och demonstration, grundforskning, tillämpad forskning och privat finansierad forskning.<sup>114</sup> Hur stark anknytningen till hälso- och sjukvårdssektorn eller omsorgssektorn behöver vara för att användningen ska anses tillåten och vad som egentligen klassificerar forskningen som vetenskaplig är oklart. Något som får klargöras i samband med förordningens eventuella ikraftträdande och efterföljande praxis.

För det sjätte kan åtkomst till e-hälsodata även tillåtas för att förbättra vårdens utförande, optimera behandling och tillhandahålla hälso- och sjukvård, på grundval av andra fysiska personers hälsodata.<sup>115</sup> Här öppnar alltså förordningen upp för vidareanvändningen av hälsodata för vård av en annan patient än den som personuppgifterna avser. Något som ofta anses utgöra en viktig komponent i framtagandet av precisionsmedicin.<sup>116</sup>

Sammantaget lägger de uppräknade ändamålen stor betoning på samhällets allmänna intresse som grund för tillgång till data för sekundär användning.<sup>117</sup> Listan över accepterade ändamål är omfattande och relaterar både till forskning och beslutsfattande. Innovation och förbättring av hälso- och sjukvården för samhällets bästa sätts i förgrunden.

## 2.3.4 Åtkomst till e-hälsodata

### 2.3.4.1 *Datatillstånd*

En hälsodataanvändare kan få tillgång till personlig e-hälsodata genom att ansöka om och beviljas ett datatillstånd. Ett sådant tillstånd är ett administrativt beslut som utfärdas av en medlemsstats hälsodataåtkomstorgan senast tre

---

<sup>112</sup> Art. 34.1 e EHDS.

<sup>113</sup> Skäl. 41 EHDS.

<sup>114</sup> Skäl. 41 EHDS.

<sup>115</sup> Art. 34.1 h EHDS.

<sup>116</sup> Jfr EU-kommissionen, *Personalised medicine*; Rådets slutsatser om individualiserad behandling för patienter (2015/C 421/03), p. 8.

<sup>117</sup> Jfr skäl 41 EHDS.

månader från ansökan, ibland ytterligare tre månader om det anses nödvändigt.<sup>118</sup> För ett enhetligt utfärdande av datatillstånd inom EU bör liknande ansökningsförfaranden utföras inom samtliga medlemsstater. EU-kommissionen bör här tillhandahålla ansökningsmallar för att främja harmonisering.<sup>119</sup> Därmed kan en ansökan göras effektivt oberoende av medlemsstat. Om en hälsodataanvändare söker tillgång till personlig e-hälsodata från flera hälsodatainnehavare i olika medlemsstater ska detta kunna göras genom en enda ansökan till ett hälsodataåtkomstorgan. Detta hälsodataåtkomstorgan ska sedan samarbeta med de andra hälsodataåtkomstorganen vilket undviker en repetitiv ansökningsprocess för hälsodataanvändaren. Respektive organ bestämmer emellertid fortfarande självständigt om de ska utfärda ett datatillstånd som tillåter åtkomst inom sitt område.<sup>120</sup>

Ett utfärdat datatillstånd är bundet till den ansökande hälsodataanvändaren. Att ge tillgång till eller på annat sätt tillgängliggöra e-hälsodatan för en tredje part som inte anges i tillståndet är förbjudet. Därmed ska identiteten hos auktoriserade personer som kommer att ta del av e-hälsodata, som exempelvis huvudansvarig forskare, anges i tillståndet.<sup>121</sup> Genom datatillståndet specificeras även vilken e-hälsodata som omfattas av tillståndet och för vilket av de i förordningen accepterade ändamål den får användas.<sup>122</sup> Genom att hälsodataåtkomstorgan ges rätt att utfärda datatillstånd kommer de att vara dem som närmare bestämmer vad som faller under dessa ändamål. I själva tillståndsansökan bör hälsodataanvändare, vid sidan av de avsedda ändamålen för användning, ange att användningen inte riskerar att leda till stigmatisering eller skada på individernas eller gruppernas värdighet. Här kan även en etisk bedömning begäras enligt nationell rätt om det anses behövligt.<sup>123</sup>

Det är möjligt att ändra ett datatillstånd till att omfatta ytterligare användningar av e-hälsodata eller förlänga dess giltighetstid. Något som bland annat kan möjliggöra ytterligare analys av data.<sup>124</sup> Ett datatillstånd är giltigt i högst 10 år och bestäms utifrån vad som bedöms nödvändigt för att fullfölja de ändamål som ansökan baseras på. Hälsodataanvändaren kan begära förlängning med ytterligare 10 år om det finns giltiga skäl för detta.<sup>125</sup>

Statliga myndigheter, EU-kommissionen samt andra EU institutioner, organ och byråer som har ett rättsligt mandat inom folkhälsan kan ha ett fortlöpande behov att ha tillgång till e-hälsodata. Detta kan antingen bero på EU-rätt eller

---

<sup>118</sup> Jfr art. 37.1 a och 41.1 b EHDS.

<sup>119</sup> Art. 47a EHDS och skäl 50 EHDS.

<sup>120</sup> Art. 37.1 o och art. 53.1 EHDS och skäl 57 EHDS.

<sup>121</sup> Art. 35d och 41a EHDS och skäl 41aa EHDS.

<sup>122</sup> Art. 2.2 aa EHDS.

<sup>123</sup> Skäl 50 EHDS.

<sup>124</sup> Skäl 51 EHDS.

<sup>125</sup> Art. 46.9 EHDS.

nationell rätt under krisperioder, eller för att de regelbundet ska kunna tillhandahålla vetenskapligt underlag och tekniskt stöd för unionspolitik.<sup>126</sup> Således ska medlemsstater kunna tillämpa ett accelererat förfarande där sådana hälsodataanvändare snabbare ges tillgång till data. Dock enbart för de ändamål som anges i art. 34.1 a) till c) EHDS.<sup>127</sup>

Därutöver kan ett förenklat förfarande genomföras genom att medlemsstater utser betrodda hälsodatainnehavare som genom sin expertis kan bedöma tillståndsansökningar och ge rekommendationer om datatillstånd. Dessa rekommendationer är dock inte bindande och hälsodataåtkomstorganet behåller ansvaret för att utfärda datatillståndet.<sup>128</sup> Hur detta förfarande ska utföras och på vilket sätt förfarandet avser att vara förenklat framkommer inte. Hälsodataanvändare måste fortfarande ansöka om datatillstånd eller skicka en begäran om hälsodata till hälsodataåtkomstorganet eftersom det endast är detta organ som kan fatta bindande beslut om dataåtkomst.

Hälsodataåtkomstorganet ska säkerställa transparens i sekundär användning genom att tillhandahålla information om beviljade datatillstånd, vidtagna åtgärder för att skydda individers rättigheter och utfallen av sekundäranvändning.<sup>129</sup> Sistnämnda kan bland annat ske genom länkar till vetenskapliga publikationer.<sup>130</sup> Hälsodataanvändare kan här också lämpligen ge en sammanfattning för allmänheten bestående av resultaten av hur e-hälsodata använts och informera hälsodataåtkomstorganet om eventuella fynd som är relevanta för individens hälsa. På så vis kan tillit hos enskilda främjas då de kan få information om behandlingens syfte och de data som behandlas för sekundär användning enligt ett datatillstånd. Vidare ska hälsodataåtkomstorganet tillhandahålla lättillgänglig information för personer angående de villkor under vilka e-hälsodata görs tillgängliga för sekundär användning, däribland den rättsliga grund varpå hälsodataanvändaren beviljats åtkomst och hur enskilda kan utöva de rättigheter som stadgas i GDPR:s tredje kapitel, vilket inkluderar rätten till radering.<sup>131</sup>

#### 2.3.4.2 *Begäran om hälsodata*

Ett annat tillvägagångssätt för hälsodataanvändare att få tillgång till hälsodata är genom en begäran om hälsodata.<sup>132</sup> Begäran skickas till ett hälsodataåtkomstorgan och tillgång till data kan enbart ske i ett anonymiserat statistiskt

---

<sup>126</sup> Skäl 52 EHDS.

<sup>127</sup> Art. 46.3 aa EHDS; Se avsnitt 2.2.3.

<sup>128</sup> Art. 49 EHDS och skäl 53 EHDS.

<sup>129</sup> Art. 37 EHDS.

<sup>130</sup> Skäl 44 EHDS.

<sup>131</sup> Art. 35e EHDS.

<sup>132</sup> Art. 47 EHDS.

format. Eventuellt betrodda hälsodatainnehavare ska, som vid datatillstånd, kunna fatta beslut om en begäran genom ett förenklat förfarande.<sup>133</sup>

### 2.3.4.3 *Åtkomstgodkännande av en auktoriserad deltagare i Hälsodata@EU*

Laglig tillgång till e-hälsodata för sekundär användning kan även uppnås genom ett åtkomstgodkännande av en auktoriserad deltagare som deltar och är ansluten i Hälsodata@EU. Inrättandet av Hälsodata@EU, som ska drivas av EU-kommissionen, regleras i förslaget till EHDS och genom denna infrastruktur kan gränsöverskridande sekundär användning av e-hälsodata påskyndas för de auktoriserade deltagarna samtidigt som rättssäkerheten ökar, fysiska personers integritet respekteras och interoperabilitet främjas.<sup>134</sup> Inom Hälsodata@EU kan ett informationsutbyte mellan nationella hälsodataåtkomstorgan och auktoriserade deltagare ske för hantering av gränsöverskridande åtkomstförfrågningar samt kataloger över tillgängliga e-hälsodata.<sup>135</sup> Auktoriserade deltagare kan bestå av forskningsinfrastrukturer eller liknande strukturer som inrättats enligt EU-rätt och som stödjer användning av e-hälsodata för forskning, beslutsfattande, statistik, patientsäkert och regleringssyften.<sup>136</sup> Varje medlemsstat ska även utse en nationell kontaktpunkt för sekundäranvändning av e-hälsodata som ska sammankopplas med Hälsodata@EU samt EU:s dataåtkomsttjänst. Det är möjligt att ett hälsodataåtkomstorgan utses till nationell kontaktpunkt.<sup>137</sup>

## 2.3.5 Användning och hantering av e-hälsodata

### 2.3.5.1 *Säker behandlingsmiljö*

Med hänsyn till den känsliga karaktären hos e-hälsodata är det viktigt att dataanvändares tillgång till sådana uppgifter begränsas. Därmed ska hälsodataåtkomstorgan, efter ett godkänt datatillstånd eller begäran, säkerställa att tillgången till e-hälsodata ges i en säker behandlingsmiljö och att endast icke-personliga e-hälsodata kan laddas ned av hälsodataanvändare.<sup>138</sup> En sådan miljö avser alltså att förhindra att e-hälsodata överförs direkt till hälsodataanvändare och lagras i deras egna databaser, vilket därmed begränsar risken för vidareutnyttjande av data.<sup>139</sup> Hälsodataåtkomstorganet eller den hälsodatainnehavare som ansvarar för tillgången till e-hälsodata kan därmed bibehålla kontrollen över dataåtkomsten.

---

<sup>133</sup> Jfr art. 49 EHDS; se avsnitt 2.3.4.1.

<sup>134</sup> Art 2.2 x EHDS och skäl 55 EHDS.

<sup>135</sup> Skäl 55b EHDS.

<sup>136</sup> Art. 52 EHDS.

<sup>137</sup> Art. 52 EHDS och skäl 55b EHDS.

<sup>138</sup> Skäl 54 EHDS och art. 43a.5 b EHDS.

<sup>139</sup> Art. 2.1 c EHDS; jfr art. 2.20 dataförvaltningsförordningen.

Hälsodataåtkomstorgan ska dessutom använda säkerhetsåtgärder inom den säkra behandlingsmiljön för att minimera integritetsrisker och se till personuppgiftsbehandlingen är lagenlig.<sup>140</sup> Exempelvis begränsa åtkomst och bearbetning till auktoriserade personer som anges i datatillståndet eller begäran och därmed minimera risk för obehörig åtkomst eller ändring av data. Att använda unika användaridentiteter nämns också liksom loggföring av åtkomst och aktiviteter under minst ett år. Sist men inte minst ska hälsodataåtkomstorganet genomföra regelbundna revisioner av miljöerna för att identifiera och åtgärda potentiella brister.<sup>141</sup> E-hälsodata ska raderas från den säkra behandlingsmiljön inom 6 månader efter att ett datatillstånd blir ogiltigt.<sup>142</sup>

### 2.3.5.1 Uppgiftsminimering

Som ett led i att minska riskerna för fysiska personers integritet ska principen om uppgiftsminimering tillämpas. Det faller här på hälsodataåtkomstorganet att säkerställa att tillgång enbart sker till efterfrågad e-hälsodata som är adekvata, relevanta och begränsade till vad som är nödvändigt med avseende på ändamålet med behandlingen, såsom det framkommer i datatillståndet eller i godkänd begäran om hälsodata.<sup>143</sup>

### 2.3.5.2 Anonymisering och pseudonymisering

Den sekundära användningen bygger på att personlig e-hälsodata pseudonymiseras eller anonymiseras av hälsodataåtkomstorgan eller hälsodatainnehavare tidigt i processen så information kan behandlas på ett integritetsbevarande sätt och identifiering av den enskilde förhindras.<sup>144</sup> Eftersom betoning läggs på ett tidigt genomförande kan det innebära att hälsodatainnehavare, som första aktör i behandlingen av hälsodata för sekundär användning, bör vidta pseudonymiseringen eller anonymiseringen. Detta får dock tydliggöras genom vägledning och praxis.<sup>145</sup> För att förhindra identifiering av den enskilde föreligger även ett återidentifieringsförbud för hälsodataanvändare.<sup>146</sup>

Hälsodataanvändare ska i sin ansökan eller begäran om hälsodata motivera sitt behov av tillgång till anonymiserad e-hälsodata. Om hälsodataåtkomstorganet sedan bedömer att ändamålet med behandlingen kan uppnås med sådan data ska e-hälsodata tillhandahållas i anonymiserad form.<sup>147</sup> Vid en begäran om hälsodata kan även hälsodataanvändare kräva svar i ett anonymiserat statistiskt format och på så vis endast behandla icke-personlig e-hälsodata. Då

---

<sup>140</sup> Art. 50 EHDS.

<sup>141</sup> Art. 50 EHDS.

<sup>142</sup> Art. 46.9 EHDS.

<sup>143</sup> Art. 44 EHDS.

<sup>144</sup> Skäl 37b och 49 EHDS.

<sup>145</sup> Jfr art. 36.2a och 37.1 d EHDS.

<sup>146</sup> Art. 2.1a EHDS.

<sup>147</sup> Art. 44 EHDS.



kvarstår hälsodataåtkomstorganet ensamt personuppgiftsansvarig för den personliga e-hälsodata som krävs för att svara på begäran.<sup>148</sup>

En alltför anonymiserad data kan dock riskera att påverka data kvaliteten, pålitligheten och användbarheten. Detta då e-hälsodata behöver bibehålla en lämplig detaljnivå för att förbli meningsfull och innehålla nödvändig information för till exempel forskningsändamål. På så vis kan e-hälsodata även i undantagsfall tillhandahållas i pseudonymiserat form under förutsättning att hälsodataanvändaren, utifrån de i artikel 6 GDPR angivna ändamålen, kan visa att ändamålet med behandlingen inte kan uppnås med anonymiserad data.<sup>149</sup> Vid pseudonymisering kodas uppgifterna så att de inte längre kan tillskrivas en specifik person. Informationen som krävs för att avpseudonymisera ska endast vara tillgänglig för hälsodataåtkomstorganet eller en myndighet som agerar som betrodd tredje part enligt nationell rätt.<sup>150</sup> Till skillnad från anonymiserade uppgifter anses de härigenom fortfarande utgöra personuppgifter, och därigenom fortfarande omfattas av dataskyddslagar, då det hade varit möjligt att utifrån dessa uppgifter identifiera en individ.<sup>151</sup> Dessutom ökar risken för så kallad bakvägsidentifiering ju mer data som finns tillgänglig om en individ.<sup>152</sup>

Anonymiseringsprocessen är komplicerad, särskilt vid stora dataset innehållande en bred samling personuppgifter.<sup>153</sup> Huruvida en enskild är identifierbar grundar sig i om denne direkt eller indirekt går att identifiera genom de hjälpmedel som antingen den personuppgiftsansvarige eller en annan person rimligen kan komma att använda. För att bedöma hjälpmedlets rimlighet får faktorer såsom kostnader och tidsåtgång för identifiering beaktas liksom tillgänglig teknik vid behandlingstidpunkten men även den tekniska utvecklingen.<sup>154</sup> Trots användning av avancerade anonymiseringstekniker vid behandling av e-hälsodata kan således en risk kvarstå att det genom uppgifterna går eller skulle kunna gå att återidentifiera personer. Särskilt om medel utöver vad som anses rimligt och sannolikt skulle användas. Dessutom är det tänkbart att hälsodata avseende sällsynta sjukdomar, där antal fall är begränsade, är ännu svårare att fullständigt anonymisera.<sup>155</sup> Svårighet att fullständigt avidentifiera e-hälsodata lägger oftast grunden för e-hälsodatas känslighet och i takt med teknologins och precisionsmedicinens utveckling kommer allt fler

---

<sup>148</sup> Skäl 49 EHDS.

<sup>149</sup> Art. 46.1 c EHDS.

<sup>150</sup> Art. 44 EHDS.

<sup>151</sup> Art. 4.5 GDPR; David, Frydlinger, Tobias, Edvardsson, Caroline, Olstedt Carlström, Sandra, Beyer, *GDPR – juridik, organisation och säkerhet enligt dataskyddsförordningen* (2018, JUNO), under rubriken 3.8 Ytterligare definitioner; EDPB riktlinjer 03/2020 fotnot 17; skäl 28 GDPR; Artikel 29-gruppens yttrande 4/2007, p. 18–21.

<sup>152</sup> Socialstyrelsen (2022) s. 26.

<sup>153</sup> EU-kommissionen, *Ethics and data protection*, 14 november 2018, s. 8.

<sup>154</sup> Jfr skäl 26 GDPR.

<sup>155</sup> Skäl 64 EHDS.

typer av data att bli problematiska att anonymisera, till exempel medicinsk avbildning.<sup>156</sup>

Det finns således en risk att hälsodata som exempelvis ingår i elektroniska patientjournaler, sjukdomsregister, biobanker och persongenererade data skulle kunna leda till identifiering av en individ. Antingen genom att länkas med annan information eller genom utvecklade av nya tekniska metoder.<sup>157</sup> Därmed är det osäkert hur och när anonym data återigen kan bli personlig data. Särskilt då det saknas en EU-gemensam syn på vad som konstituerar en tillräcklig anonymisering och därmed även hur anonymisering ska ske beroende på e-hälsodata. Något som utmynnar i att medlemsstater saknar en gemensam förståelse för både anonymiserings och pseudonymiseringstekniker.<sup>158</sup> Således bör hälsodataåtkomstorgan utbyta praxis på området och EU-gemensamma procedurer fastställas för att förhindra att olika tillvägagångssätt och standarder hindrar datadelning för hälsodataanvändare.<sup>159</sup>

## 2.4 Opt-out rätt

### 2.4.1 Innebörd

Enligt den provisoriska överenskommelsen inkluderar nu förslaget till EHDS ett krav att samtliga medlemsstater ska införa en opt-out möjlighet. Detta ger enskilda möjlighet att påverka behandlingen av sin personliga e-hälsodata genom att ges rätt att när som helst och utan att ange skäl välja att inte tillåta att deras e-hälsodata behandlas för sekundär användning.<sup>160</sup>

Om en medlemsstat väljer att opt-out möjligheten ska utövas hos hälsodataåtkomstorgan åläggs organet att tillhandahålla allmän information om rättigheten, själva förfarandet, fördelar och nackdelar med utövandet av rättigheten samt även underlätta utövandet av den.<sup>161</sup>

Om en enskild väljer att avstå får den personens data inte delas med hälsodataanvändare, vare sig i ursprunglig eller i anonymiserad form. Data får inte göras tillgänglig eller på annat sätt behandlas enligt ett senare beviljat data-tillstånd eller en begäran om hälsodata. Detta påverkar inte behandlingen av enskildas personliga e-hälsodata för sekundär användning enligt datatillstånd

---

<sup>156</sup> Chikwetu m.fl. (2023) s. 245 f.; Nakayama m.fl. (2023) s. 71 f.

<sup>157</sup> Skäl 64 EHDS.

<sup>158</sup> Tehdas (2022).

<sup>159</sup> Skäl 43 EHDS; Groos & van Veen (2020) s. 499 f.

<sup>160</sup> Art. 35f EHDS.

<sup>161</sup> Art. 35e.2 EHDS.

eller begäran om hälsodata som har beviljats innan individen valt att inte delta.<sup>162</sup>

Tillägget av en opt-out mekanism är kontroversiell och har mött kritik. Bland annat har det anförts att EU-kommissionens förslag till EHDS redan tillhandahåller tillräckliga skyddsåtgärder och att enskilda ges möjlighet att avstå kan resultera i att inte tillräckliga data finns för att uppnå de tilltänkta fördelarna med hälsodataområdet. Vissa hävdar motsatsvis att en opt-out möjlighet kan förhindra att patienter underlåter att söka vård på grund av rädsla av att deras känsliga hälsouppgifter ska spridas och nyttjas för andra ändamål än för vilka de samlades in för.<sup>163</sup>

Hur som helst stödjer och förespråkar EU-parlamentet en utökning av den enskildes delaktighet avseende sekundär användning av dennes e-hälsodata genom en opt-out möjlighet. En möjlighet för enskilda att avstå från att deras e-hälsodata behandlas anses motiverat, speciellt då sekundär användning inte förutsätter den enskildes samtycke.<sup>164</sup> Här kan även tilläggas att opt-out mekanismen presumerar att samtycke föreligger till dess att den enskilde aktivt motsätter sig behandling. Något som skiljer sig från en opt-in mekanism där samtycke måste inhämtas innan behandling påbörjas.<sup>165</sup> Att enskilda inte nyttjar möjligheten till opt-out bör inte anses utgöra ett samtycke från den berörda personen i enlighet med artikel 4.11 GDPR.<sup>166</sup>

#### 2.4.2 Undantag

Medlemsstater kan genom nationell rätt införa undantag till opt-out möjligheten.<sup>167</sup> Alltså i vilka situationer det ska anses tillåtet att behandla e-hälsodata även om en person valt att avstå. För att ett sådant undantag ska anses accepterat måste det uppfylla tre kumulativa kriterier.<sup>168</sup> För det första kan det endast tillämpas av nationella offentliga myndigheter eller relevanta europeiska institutioner som ansvarar för folkhälsan eller för andra offentliga uppgifter inom detta område för de accepterade ändamål för sekundär användning som anges i artikel 34(1) punkterna a)–c) och för vetenskaplig forskning som utförs av offentliga organ av viktiga skäl för allmänintresset.<sup>169</sup> Exempel på

---

<sup>162</sup> Art. 35f.2 a EHDS.

<sup>163</sup> Patrick Breyer, *European Health Data Space (EHDS): Patients risk losing control over their data*, 8 mars 2024; *Hundratusen i protest mot delad patientdata i EU*, Dagens Nyheter, 13-09-2023.

<sup>164</sup> Jfr bl.a. skäl 39a och art. 33.5a Parlamentets version.

<sup>165</sup> EDPB-riktlinjer 05/2020 p. 81.

<sup>166</sup> Jfr bl.a. skäl 39a och art. 33.5a Parlamentets version.

<sup>167</sup> Art. 35f EHDS.

<sup>168</sup> Art. 35f.3 EHDS.

<sup>169</sup> Se avsnitt 2.3.3.

vetenskaplig forskning kan vara studier om ovanliga sjukdomar eller nya hälsorisker.<sup>170</sup>

För det andra ska data inte kunna erhållas på andra sätt på ett snabbt och effektivt sätt under likvärdiga förhållanden och för det tredje ska hälsodataanvändaren motivera varför hälsodata likväl ska göras tillgänglig trots opt-out. Undantagen ska vidare respektera individens grundläggande rättigheter och vara proportionerliga i förhållande till det allmänna intresset.<sup>171</sup>

---

<sup>170</sup> Skäl 37c EHDS.

<sup>171</sup> Art. 35f EHDS.

## 3 Rätten till radering

### 3.1 Costeja v. Google

Rätten till radering anses av många ha sitt ursprung i EU-domstolens avgörande Costeja mot Google den 13:e maj 2014 (Costejadomen). Där gjorde domstolen ett uppmärksammat ställningstagande till värnande av den personliga integriteten genom att etablera en rätt att bli bortglömd.<sup>172</sup> I målet begärde den spanska medborgaren Mario Costeja González att vissa länkar till hans personliga information skulle tas bort från Google. När Costejas namn söktes på Google visades sökresultat med koppling till en försäljning av fastigheter på exekutiv auktion år 1998 vilka hade utmätts på grund av obetalda socialförsäkringsavgifter. Informationen kom från en gammal annons hos nätupplagan av den spanska tidningen La Vanguardia.<sup>173</sup>

Att vem som helst skulle kunna få åtkomst till den här informationen ansåg Costeja vara integritetskränkande vilket föranledde honom att lämna in ett klagomål till den spanska dataskyddsmyndigheten. Klagomålet bifölls och Google ålades att rensa uppgifterna från sina sökresultat. Google invände med anledning av att uppgifterna fortfarande skulle gå att finna på La Vanguardias hemsida och ifrågasatte varför Costeja inte begärde radering av personuppgifterna direkt från denna hemsida. EU-domstolen konstaterade här att La Vanguardias hemsida, till skillnad från sökmotorer, omfattas av det journalistiska undantaget. Det skulle därmed innebära ett rättssäkerhetsproblem om personer skulle se sig tvungna att först radera uppgifterna från den ursprungliga hemsidan innan de kan tas bort från sökresultaten hos sökmotorer. Dels på grund av att olika hemsidor kan ha olika etableringsplatser och därmed olika EU-rättsliga skyldigheter vilket bidrar till att vissa hemsidor även kan omfattas av det journalistiska undantaget.<sup>174</sup>

EU-domstolen fastslog att företag bakom internetbaserade sökmotorer som Google, Bing och Yahoo anses vara personuppgiftsansvariga eftersom de för sina egna ändamål indexerar all tillgänglig information på internet.<sup>175</sup> Detta anses enligt domstolen avgörande för att skydda individens integritet på internet.<sup>176</sup> Personuppgiftsansvar är en förutsättning för individer att kunna begära att bli bortglömda från sökmotorernas index, vilket är viktigt eftersom allt som publicerats med en persons namn på internet kan återupptäckas genom en enkel sökning.<sup>177</sup> Rätten att bli bortglömd syftar till att hantera

---

<sup>172</sup> C-131/12 *Google Spain SL, Google Inc. v. Costeja m.fl.*

<sup>173</sup> Förslag till avgörande av generaladvokat Jääskinen i mål C-131/12, p. 18.

<sup>174</sup> C-131/12 p. 85.

<sup>175</sup> C-131/12 p. 41.

<sup>176</sup> C-131/12 p. 87–88.

<sup>177</sup> C-131/12 p. 80.

riskerna för personlig integritet som uppstår på grund av den stora mängden lättillgänglig information på internet, i databaser och andra former av elektroniska förvarings- och spridningsmetoder.<sup>178</sup> Denna rättighet, som illustreras i Costejadomen, är kopplad till tidsaspekten och den minskande relevansen över tid för data som fortsätter att finnas tillgänglig på internet och är associerad med en viss person.<sup>179</sup>

I sin bedömning uttrycker EU-domstolen att dåvarande dataskyddsdirektiv ska tolkas mot bakgrund av EU-stadgan.<sup>180</sup> Särskilt artikel 7 om skydd för privatliv och artikel 8 om skydd för personuppgifter.<sup>181</sup> Domstolen betonar att sökmotorer behandlar personuppgifter genom att väga individens intressen och grundläggande rättigheter mot de berättigade intressen hos personuppgiftsansvariga och tredje parter till vilka uppgifterna lämnats ut. För att bevilja rätten att bli bortglömd måste den registrerades rätt till privatliv och skydd för personuppgifter väga tyngre än sökmotorernas vinstintresse och allmänhetens informationsintresse. Domstolen anser att möjligheten för sökmotorer att samla in all information om en individ utgör ett allvarligt hot mot den enskildes rätt till skydd för privatlivet och att sökmotorernas ekonomiska intresse inte får överväga individens intresse av att skydda sina rättigheter.<sup>182</sup> Rättighetens tillämpning beror även på om behandlingen av personuppgifterna strider mot dataskyddsdirektivets artikel 12 b) och 14.1 a) som bland annat anger att en enskild har rätt att motsätta sig personuppgiftsbehandling och att ofullständiga eller felaktiga personuppgifter som behandlas i strid med direktivet ska utplånas. Dessa bestämmelser gäller inte bara när uppgifterna är felaktiga eller skadliga för individen, utan även när de blir irrelevanta, felaktiga eller lagras längre än nödvändigt i förhållande till det berättigade intresse som motiverade behandlingen. Möjligheten att få personuppgifter raderade förstärks alltså över tid när uppgifterna blir mindre relevanta, vilket innebär att sökmotorer måste möjliggöra att uppgifterna faller i glömska.<sup>183</sup>

EU-domstolen slog på så vis fast att individer har rätt att begära att sökmotorer tar bort länkar till deras personliga information från sina sökresultat. Förutsatt att informationen är felaktig, irrelevant eller oskälig och det inte heller finns ett allmänintresse i att uppgifterna fortfarande finns tillgängliga. Därmed fastställde domen principen om rätten att bli bortglömd för EU-medborgare. Domstolen betonade dock att rättigheten måste balanseras mot andra

---

<sup>178</sup> C-131/12 p. 80.

<sup>179</sup> C-131/12 p. 93.

<sup>180</sup> Jfr C-274/99 *P. Connolly mot Kommissionen*, p. 37; I de förenade målen C-465/00, C-138/01 och C-139/01 *Österreichischer Rundfunk m.fl.*, p. 68.

<sup>181</sup> C-131/12 p. 68.

<sup>182</sup> C-131/12 p. 81.

<sup>183</sup> C-131/12 p. 94–97.

rättigheter, såsom yttrandefrihet och informationsfrihet, och att en individuell bedömning krävs i varje enskilt fall för att avgöra om rätten ska tillämpas.

## 3.2 Artikel 17 GDPR

### 3.2.1 Utgångspunkter

Sedan EU:s antagande år 2018 av GDPR återfinns numera rätten till radering kodifierad i förordningens artikel 17. Härigenom ges personer en uttrycklig rätt att begära att få sina personuppgifter raderade genom att vända sig till det företag, den myndighet eller den som behandlar uppgifterna.<sup>184</sup> Rättigheten såsom den kommer till uttryck i GDPR har utvecklats till att vara mer omfattande än enligt tidigare praxis.<sup>185</sup> Numera riktar sig bland annat rättigheten inte enbart till sökmotorer utan till samtliga personuppgiftsansvariga.<sup>186</sup> Möjligtvis för att hantera växande integritetshot i samband med teknologiska framsteg.

I sin begäran om radering bör den enskilde motivera vilka personuppgifter som ska raderas, även om en allmän begäran om radering av samtliga personuppgifter lär kunna göras.<sup>187</sup> En personuppgift är all slags information som direkt eller indirekt kan knytas till en levande fysisk person. Bland annat kan det här röra sig om namn, adress, personnummer, foton men även information som, när den sammanställs, kan leda till identifiering av en specifik person.<sup>188</sup>

Att uppgifter raderas innebär att de utplånas eller avidentifieras så att de inte längre anses utgöra personuppgifter. Därmed gäller rätten till radering inte om den personuppgiftsansvarige kan visa att det genom uppgifterna inte går att identifiera den registrerade.<sup>189</sup> Vad som i det enskilda fallet krävs för att personuppgifter ska anses utplånade får överlämnas åt praxis men generellt sett innebär det att de inte ska kunna återskapas.<sup>190</sup> Det finns dock särskilt utvecklade tekniker som syftar till att återskapa information som på något sätt blivit förstörd. Dessutom sker en ständig utveckling av nya tekniker vilket kan resultera i att det som i nuläget anses som förstört möjligtvis kan återskapas inom en snar framtid.<sup>191</sup> När personuppgifter istället avidentifieras avlägsnas alla identifieringsmöjligheter så att de inte direkt eller indirekt kan hänföra till en specifik fysisk person. På så vis anses en avidentifiering utgöra

---

<sup>184</sup> Art. 17 GDPR.

<sup>185</sup> Jfr C-131/12 & C-136/17.

<sup>186</sup> Art. 17 GDPR.

<sup>187</sup> Öman (2023), kommentaren till artikel 17 GDPR.

<sup>188</sup> Art. 4.1 GDPR.

<sup>189</sup> Martin Brinnen, *Allmänna dataskyddsförordningen (GDPR)*, Karnov, 11-04-2024 (JUNO), kommentaren till artikel 17.

<sup>190</sup> SOU 1997:39 s. 400.

<sup>191</sup> Öman (2023), kommentaren till artikel 17 GDPR.

en radering enligt bestämmelsen då identifiering inte längre är möjlig.<sup>192</sup> Alltså ska data till följd av en radering inte vara möjlig att använda för några andra ändamål längre men detta förhindrar inte att data fortfarande bevaras och behandlas av andra aktörer i andra kontexter.<sup>193</sup>

Grunderna för rätt till radering reflekterar utgångspunkten att behandling och lagring av personuppgifter förutsätter en laglig grund och om en sådan grund inte längre är gällande ska uppgifterna raderas.<sup>194</sup> Begränsningar i rättighetens utövande har emellertid tillförts för att säkerställa att rätten till radering inte inskränker andra rättigheter och skyldigheter. Trots att utgångspunkten är att personuppgifter ska raderas efter att en individ har begärt det är rätten till radering således inte absolut. Rättigheten måste vägas mot andra rättigheter vilket innebär att personuppgiftsansvarige i vissa fall kan neka radering.<sup>195</sup> Att notera är att det också är möjligt för respektive medlemsstat att specificera och göra undantag från rätten att till radering vilket gör att enskildas rättigheter kan variera beroende på medlemsstat.<sup>196</sup> Hur som helst bör samtliga begränsningar av de registrerades rättigheter endast tillämpas i den mån det är absolut nödvändigt.<sup>197</sup>

### 3.2.2 Grunder för rätt till radering

#### 3.2.2.1 *Behandling är inte längre nödvändig för de ursprungliga ändamålen*

Det föreligger en rätt till radering om uppgifterna inte längre behövs för de ändamål som de samlades in för.<sup>198</sup> Detta återspeglas även i att den huvudsakliga begränsningen av personuppgiftsbehandling är att personuppgifter endast får samlas in för behandling i uppfyllande av specifika ändamål och inte senare behandlas för ändamål som strider mot dessa.<sup>199</sup> Den registrerade ska helt enkelt inte bli överraskad över att dennes personuppgifter behandlas för ett nytt ändamål som är oförenligt med de ändamål för vilken uppgifterna samlades in.<sup>200</sup> Genom att ge rätt att radera personuppgifter som faller under denna punkt kan mängden personuppgifter hållas aktuella, relevanta och begränsade. Denna bestämmelse ger därför uttryck för en princip om ändamålsbegränsning vilket medför att de som behandlar personuppgifter måste vara

---

<sup>192</sup> Öman (2023), kommentaren till artikel 17 GDPR.

<sup>193</sup> Ausloos (2020) s. 114.

<sup>194</sup> Sartor (2014) s. 64; art. 8 EU-stadgan och art. 16 FEUF.

<sup>195</sup> Karlsson Alverhill (2023) s. 108 f.

<sup>196</sup> Art. 89.2 GDPR och skäl 156 GDPR.

<sup>197</sup> C-345/17 *Buivids* p. 64.

<sup>198</sup> Art. 17.1 a GDPR.

<sup>199</sup> Jfr art. 5.1 a GDPR.

<sup>200</sup> Se David, Frydinger, Tobias, Edvardsson, Caroline, Olstedt Carlström, Sandra, Beyer, *GDPR – juridik, organisation och säkerhet enligt dataskyddsförordningen* (2018, JUNO), under rubriken 2.4.2. Ändamålsbegränsning; Vrabc (2021) s. 141 f.



medvetna om varför behandling sker.<sup>201</sup> Att principen betonas har ansetts positivt i samband med att data i större utsträckning sekundär används.<sup>202</sup>

Nödvändigheten i behandlingen får bedömas utifrån om personuppgiftens användning är en förutsättning för att uppnå behandlingens ändamål. EU-domstolen har betonat att det krävs att det intresse som eftersträvas med behandlingen av personuppgifterna inte rimligen kan uppnås på ett lika effektivt sätt genom andra medel som är mindre ingripande i de registrerades grundläggande fri- och rättigheter.<sup>203</sup> Således kan behandlingen inte längre anses nödvändig om exempelvis den enskildes personuppgifter är felaktiga på grund av tidsförloppet eller helt enkelt föråldrade. Exempelvis när information om denne som behandlats av ett företag tagits bort från ett offentligt register eller fortsätter behandlas utöver en lagstadgad lagringstid.<sup>204</sup> Dock finns det ingen övergripande tidsram som indikerar uppgifters föråldrande. Bedömningen kring behandlingens fortsatta nödvändighet kan tyckas ge ett skönsmässigt utrymme för personuppgiftsansvariga angående informationens relevans. Här kan även diskuteras hur uppgifters framtida värde egentligen bör bedömas. Databehandling är oftast baserad på vaga ändamålsdefinitioner för att möjliggöra oförutsedda framtida användningar. På så vis kan all sekundär användning bedömas vara relevant i relation till de ändamål för vilka data samlades in. Dessutom kan den enskildes och den personuppgiftsansvariges synsätt skilja sig åt gällande vad som anses nödvändigt för de ursprungliga ändamålen.<sup>205</sup>

En behandlings förenlighet med de ursprungliga ändamålen får bland annat bedömas utifrån sambandet mellan de ursprungliga ändamålen och den ytterligare behandlingen, sammanhanget där data samlades in och konsekvenserna för den registrerade. Här anger Vrabc att vidarebehandling för vetenskapliga forskningsändamål kan antas vara förenliga under förutsättning att lämpliga säkerhetsåtgärder existerar och principen om dataminimering respekteras. Kravet på förenlighet gäller dock inte om samtycke utgör grund för behandling då den sekundära användningen isåfall får anses accepterad till följd av att ett giltigt samtycke ska vara specifikt.<sup>206</sup>

### 3.2.2.2 Återkallat samtycke

Vidare föreligger en rätt till radering om den enskildes samtycke ligger till grund för behandlingen och samtycket sedan återkallas.<sup>207</sup> Detta grundar sig

---

<sup>201</sup> Jfr art. 5.1 b GDPR.

<sup>202</sup> Vrabc (2021) s. 141.

<sup>203</sup> C-252/21 *Meta Platforms m.fl.* p. 108; C-439/19 *Latvijas Republikas Saeima* p. 110; C-708/18 *Asociația de Proprietari bloc M5A-ScaraA*, p. 47.

<sup>204</sup> Ausloos (2020) s. 199–201.

<sup>205</sup> Vrabc (2021) s. 142.

<sup>206</sup> Vrabc (2021) s. 201–204; Ausloos (2020) s. 202–204.

<sup>207</sup> Art. 17.1 b GDPR.

i att den registrerades samtycke är en rättslig grund för personuppgiftsbehandling.<sup>208</sup> För att ett samtycke ska vara giltigt ska det vara frivilligt, otvetydigt, informerat, specifikt och påvisbart i efterhand.<sup>209</sup> Om samtycket lämnas som en del av ett större sammanhang ska det vara särskilt, exempelvis genom godkännande av användarvillkor.<sup>210</sup> Om den registrerade har lämnat ett tidsbegränsat samtycke och tiden löpt ut torde även detta aktualisera en rätt till radering.<sup>211</sup> Alltså tar den här raderingsgrunden utgångspunkt i om samtycke från den enskilde har använts som laglig grund för behandling av dennes personuppgifter hos en specifik personuppgiftsansvarig.<sup>212</sup> Ett återkallande av samtycke ska enligt GDPR kunna ske lika lätt som det har lämnats.<sup>213</sup>

### 3.2.2.3 *Invändning mot behandling*

Att den registrerade invänder mot viss typ av behandling av dennes personuppgifter är även det en grund för radering om behandling sker baserat på den personuppgiftsansvarigas berättigade intresse men detta inte väger tyngre än den enskildes intresse. Detta gäller även om den personuppgiftsansvarige utför en uppgift av allmänt intresse.<sup>214</sup> Alltså innebär detta att om den personuppgiftsansvarige inte kan påvisa tyngre vägande skäl än de som den registrerade anför ska personuppgifterna raderas. Det kan bland annat röra sig om ekonomiska skäl eller allmänhetens informationsintresse men även andra skäl kan presenteras.<sup>215</sup> Även historiska, vetenskapliga, statistiska eller forskningsändamål lär kunna anföras. Forskning avseende folkhälsa kan i vissa situationer anses utgöra ett allmänt intresse.<sup>216</sup>

Det är oklart vilka åtgärder den personuppgiftsansvarige bör vidta för att upptäcka och bedöma den enskildes motstående intressen. Utgångspunkt får emellertid tas i den registrerades specifika situation och huruvida informationen skadar den registrerades rättigheter och intressen, bland annat den personliga integriteten. I bedömningen får därmed ett antal faktorer vägas in som exempelvis mängden personuppgifter som behandlas och vilken sorts information som framkommer av dessa.<sup>217</sup> Trots att det saknas en allmängiltig definition av personlig integritet betraktas det ofta grundas i den enskildes självbestämmande och kontroll gällande när, hur och i vilken omfattning deras

---

<sup>208</sup> Art. 6.1 a GDPR.

<sup>209</sup> EDPB-riktlinjer 05/2020 p. 11.

<sup>210</sup> Skäl 32 GDPR; EDPB-riktlinjer 05/2020 p. 55–61.

<sup>211</sup> Krzysztofek (2021) s. 106.

<sup>212</sup> Jfr C-136/17 *Commission nationale de l'informatique et des libertés (CNIL) v. Google LLC* p. 61–62.

<sup>213</sup> Art. 7.3 GDPR.

<sup>214</sup> Art. 17.1 c GDPR.

<sup>215</sup> Ausloos (2020) s. 212–214; jfr C-131/12.

<sup>216</sup> Slokenberga m.fl. (2021) s. 24.

<sup>217</sup> Wendleby (2021) s. 475 ff.

personliga information kan kommuniceras till andra.<sup>218</sup> Alltså en rätt att själv förfoga över information om den egna personen och att ha rätt att behålla vissa saker för sig själv.<sup>219</sup> Emellertid har det även hävdats att rätten till integritet varken är en rätt till sekretess eller en rätt till kontroll utan en rätt till ett lämpligt flöde av personlig information.<sup>220</sup> Enskildas integritet skyddas även i EU-stadgan, bland annat artikel 3 som anger att var och en har rätt till fysisk och psykisk integritet, artikel 7 som fastslår rätten till privatliv och artikel 8 där skydd för behandling av personuppgifter återfinns. Dessa rättigheter är dock inte absoluta då en inskränkning i vissa fall kan motiveras enligt lag eller om det anses nödvändigt i ett demokratiskt samhälle. Därmed kan rätten till radering delvis förstärka rätten till personlig integritet i ett samhälle som präglas av teknologiska framsteg med ständigt bevarad och lättillgänglig information. Emellertid har det även framförts att rättigheten inte tillhandahåller ett effektivt skydd för personlig integritet i vårt digitala samhälle och att nya angreppssätt krävs.<sup>221</sup>

Följaktligen blir det på denna grund relevant att först se till i vilket syfte den personuppgiftsansvarige behandlar personuppgifterna i den specifika situationen. Därefter är det upp till den personuppgiftsansvarige att presentera berättigade intressen som denne anser väger tyngre än den enskildes intressen. Sedan får personuppgiftsansvarige göra en bedömning kring vilket intresse som väger tyngst. I intresseavvägningen ska även åtgärder som den personuppgiftsansvarige avser vidta för att skydda personuppgifterna vägas in såsom användning av anonymiseringstekniker, transparens i förhållande till de registrerade om vilka uppgifter som används och en generell och ovillkorad opt-out rätt, dvs en rätt att begära att behandlingen upphör.<sup>222</sup>

#### 3.2.2.4 *Olaglig behandling*

Rätt till radering föreligger också om personuppgifterna olagligen behandlas.<sup>223</sup> Detta är en extensiv grund som kan omfatta en rad situationer. Olaglig behandling kan dels tolkas utifrån artikel 6 GDPR avseende giltig behandling av personuppgifter och andra i GDPR fastställda principer såsom de som anges i artikel 5 GDPR. Dels kan olaglig behandling tolkas brett som behandling i strid med en annan lagbestämmelse än GDPR. Sistnämnda tolkning måste utföras objektivt av tillsynsmyndigheter enligt nationell rätt eller ett

---

<sup>218</sup> Westin (2015) s. 7.

<sup>219</sup> Smer, *Integritet*.

<sup>220</sup> Nissenbaum (2009) s. 127 f.

<sup>221</sup> Kocharyan, Vardanyan, Hamulák, Kerikmäe (2022) s. 96–115.

<sup>222</sup> Artikel 29-gruppens yttrande 6/2014, s. 35–45.

<sup>223</sup> Art. 17.1 d GDPR.

domstolsbeslut. Exempelvis kan radering aktualiseras om personuppgiftsbehandlingen förbjudits genom ett domstolsbeslut.<sup>224</sup>

När det kommer till särskilda kategorier av personuppgifter, såsom personlig e-hälsodata, åtnjuter dessa ett högre juridiskt skydd vilket ställer särskilda krav på dess hantering. Utgångspunkten är därför att det är förbjudet att behandla sådana känsliga personuppgifter. Det är endast tillåtet att behandla sådana uppgifter i de undantagsfall som anges i artikel 9.2 GDPR.<sup>225</sup> Majoriteten av dessa undantag relaterar antingen till den enskildes samtycke till behandling eller samhällets intresse av att behandla uppgifterna. EHDS-förordningen relaterar till det sistnämnda och utgör sådan unionsrätt som tillhandahåller en rättslig grund i enlighet med GDPR för den sekundära användningen av personlig e-hälsodata enligt artikel 9.2 punkterna g), h), i) och j) GDPR. Utöver artikel 9.2 GDPR bör en av de lagliga grunderna för behandling som anges i artikel 6 föreligga när e-hälsodata behandlas för sekundär användning. Det är upp till hälsodatainnehavare, hälsodataåtkomstorgan eller hälsodataanvändare som vill behandla uppgifter att visa att detta föreligger.<sup>226</sup> Här bör även tilläggas att förslaget till EHDS anger att medlemsstater inte får upprätthålla eller införa ytterligare villkor, såsom att begära samtycke från fysiska personer, avseende behandling för sekundär användning av personliga e-hälsodata. Det får enbart införas striktare bestämmelser när det kommer till genetisk information, biobanker, hälsoappar eller andra uppgifter som anges i artikel 33.5 EHDS.<sup>227</sup>

### 3.2.2.5 Rättslig förpliktelse

Om radering krävs för att uppfylla en rättslig skyldighet kan rätten till radering tillämpas.<sup>228</sup> Här tas sikte på förpliktelser att radera personuppgifter som antingen kan hänföras till EU-rätt eller medlemsstaternas nationella rätt.<sup>229</sup> Exempelvis kan datalagringsreglering falla under den här punkten som anger att uppgifter får behandlas ett maximalt antal år.

## 3.2.3 Begränsningar av rätten till radering

### 3.2.3.1 Utövande av yttrande- och informationsfrihet

Om behandlingen är nödvändig för att tillgodose rätten till yttrande- och informationsfrihet kan radering nekas.<sup>230</sup> Denna punkt går att härleda till Coste-jadomen och den avvägning som gjordes mellan å ena sidan den enskildes

---

<sup>224</sup> Vrabc (2021) s. 145.

<sup>225</sup> Art. 9 GDPR.

<sup>226</sup> Skäl 37 EHDS; jfr Kjellman & Värmon (2022) s. 40.

<sup>227</sup> Skäl 37 EHDS.

<sup>228</sup> Art. 17.1 e GDPR.

<sup>229</sup> Skäl 73 GDPR.

<sup>230</sup> Art. 17.3 a GDPR.

personliga integritet och å andra sida yttrande- och informationsfrihet. Här får därmed en bedömning göras kring hur en radering av informationen skulle påverka dessa rättigheter.<sup>231</sup>

### 3.2.3.2 *Uppfyllelse av rättslig förpliktelse, utförande av uppgift av allmänt intresse eller led i myndighetsutövning*

Radering kan nekas om behandling krävs för att uppfylla en rättslig förpliktelse enligt EU-rätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Alltså om den personuppgiftsansvarige måste behandla en viss information på grund av en rättslig förpliktelse. Dessutom kan radering nekas om behandling krävs för att utföra en uppgift av allmänt intresse eller utförs som ett led i den personuppgiftsansvariges myndighetsutövning.<sup>232</sup> Personuppgifter behöver således inte raderas vid behandling av personuppgifter när en myndighet genom författning ålagts att föra ett offentligt register eller där tillsyn av myndigheter och dokumentationsarbete av den enskilde är en förutsättning.<sup>233</sup> Exempelvis finns ofta dokumentationskrav inom hälso- och sjukvård och krav att bevara personuppgifter i journalhandlingar ett visst antal år.<sup>234</sup> Således är rätten till radering inte tillämplig på patientjournaler när dessa behöver behandlas till följd av en rättslig förpliktelse. På så vis undantas behandling av personuppgifter som utförs inom den offentliga sektorn för fastställda allmänna intressen i stor utsträckning från rätten till radering.<sup>235</sup>

Det är emellertid upp till medlemsstater att närmare precisera vad som avses med allmänt intresse och myndighetsutövning.<sup>236</sup> Vad som avses med uppgift av allmänt intresse kan rent språkligt innebära något som är av intresse för eller berör många människor rent allmänt, i motsats till ett enskilt intresse.<sup>237</sup> Allmänintresset inkluderar hälso- och sjukvårdsändamål, folkhälsa, socialt skydd och förvaltning av hälso- och sjukvårdstjänster. Även arkivändamål kan vara av allmänt intresse.<sup>238</sup> Kampen mot Covid-19 är generellt sett att anse som ett viktigt allmänintresse då pandemin orsakat en exceptionell sanitär kris av aldrig tidigare skådad karaktär och omfattning.<sup>239</sup>

---

<sup>231</sup> Se Ausloos (2020) s. 254–259.

<sup>232</sup> Art. 17.3 b GDPR.

<sup>233</sup> Krzysztofek (2021) s. 166.

<sup>234</sup> Jfr 3 kap. 17 och 18 §§ PDL.

<sup>235</sup> Öman (2023), kommentaren till artikel 17 GDPR.

<sup>236</sup> Ausloos (2020) s. 261–262.

<sup>237</sup> Öman (2023), kommentaren till artikel 6 GDPR under rubriken *Arbetsuppgift av allmänt intresse*.

<sup>238</sup> Skäl 45, 52–56, 112 och 154 GDPR. Se även art. 5.1 b GDPR.

<sup>239</sup> EDPB-riktlinjer 03/2020 p. 63–66; skäl 46 och 112 GDPR.

Arbetsuppgifter som utgör ett led i myndighetsutövning lär även vara arbetsuppgifter av allmänt intresse samt bero på en rättslig förpliktelse. Myndighetsutövning karaktäriseras av ensidiga beslut eller andra åtgärder som ger uttryck för samhällets maktbefogenheter gentemot medborgarna.<sup>240</sup> Att en myndighet förvarar uppgifter i en databas som bolag enligt lag är skyldiga att lämna till myndigheten och ger personer möjlighet att ta del och tillhandahålla dem kopior av dessa uppgifter utgör myndighetsutövning.<sup>241</sup>

### 3.2.3.3 *Viktigt allmänt intresse på folkhälsoområdet*

En personuppgiftsansvarig kan även neka radering om personuppgiftsbehandlingen är nödvändig för att utföra en uppgift av allmänt intresse på folkhälsoområdet.<sup>242</sup> Här balanseras alltså den enskildes rätt till integritet med samhällets intresse av att hantera frågor som rör folkhälsa. Detta kan tänkas omfatta sjukdomsövervakning, smittspårning och andra hälsoinsatser. Huruvida personuppgiftsbehandlingen är nödvändig får bedömas utifrån EU-rätt eller medlemsstatens nationella rätt.

### 3.2.3.4 *Arkivändamål av allmänt intresse eller av vetenskapliga, historiska eller statistiska ändamål*

Radering kan nekas vid behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, som omfattas av lämpliga skyddsåtgärder enligt artikel 89.1 GDPR, om en rätt till radering hade omöjliggjort eller avsevärt försvårat uppnåendet av behandlingens syfte.<sup>243</sup> Detta undantag blir ofta aktuellt om den personuppgiftsansvariga är en myndighet eller utför en uppgift av allmänt intresse och har en lagstiftad skyldighet att spara och inneha personuppgifter. Exempelvis föreligger ofta en lagstiftad skyldighet för vårdgivare att under en viss period spara och inneha personuppgifter via arkivering.<sup>244</sup> Om personuppgiftsansvarige nekar radering till följd av vetenskapliga ändamål måste denne kunna visa att en radering förhindrar eller äventyrar den planerade forskningen. Det har anförts att det är osannolikt att radering eller anonymisering av enstaka data självständigt skulle påverka ett forskningsprojekt. Upprepade begäranden om radering från olika individer riskerar dock att försvaga relevansen av ett dataset.<sup>245</sup>

---

<sup>240</sup> Öman (2023), kommentaren till artikel 6 GDPR under rubriken *Myndighetsutövning*.

<sup>241</sup> C-138/11 *Compass-Datenbank* p. 40–41; C-398/15 *Salvatore Manni*, p. 43.

<sup>242</sup> Art. 17.3 c GDPR; jfr art. 9.2 h och j och art. 9.3 GDPR.

<sup>243</sup> Art. 17.3 d GDPR.

<sup>244</sup> Ausloos (2020) s. 267 f.

<sup>245</sup> Slokenberga m.fl. (2021) s. 112.

### 3.2.3.5 *För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.*

Om behandling krävs för att kunna fastställa, göra gällande eller försvara rättsliga anspråk kan radering nekas.<sup>246</sup> Att radering kan nekas på denna grund har betydelse i säkerställandet av ett effektivt rättsmedel då det ger en möjlighet för organisationer och enskilda att behålla personuppgifter om det behövs för att skydda sina rättigheter i rättsliga sammanhang, såsom vid tvister eller rättsliga processer.<sup>247</sup>

### 3.2.4 Bedömning och genomförande av radering

Den personuppgiftsansvarige ska efter en enskilds begäran om radering bedöma huruvida rätten till radering gäller i det enskilda fallet och därmed om personuppgifter ska raderas eller inte.<sup>248</sup> Den initiala bedömningen som görs avseende uppgiftsbehandlingslagligheten skiljer sig alltså från en prövning av om uppgifterna ska raderas. På så vis kan personuppgiftsbehandlingen ha varit laglig men bli otillåten efter en begäran om radering som kräver prövning i det enskilda fallet.<sup>249</sup> Omfattningen av den personuppgiftsansvariges utredning baseras på begärens innehåll samt om den är mer allmän eller om konkreta anmärkningar lämnats.<sup>250</sup> Om personuppgiftsansvarige beslutar att uppgifterna ska raderas ska detta ske utan dröjsmål, senast inom tre månader efter begäran mottagits.<sup>251</sup>

Utöver detta åläggs personuppgiftsansvariga en meddelandeskyldighet.<sup>252</sup> Detta innebär att den personuppgiftsansvarige, efter att personuppgifter raderats på den enskildes begäran, ska informera dem de lämnat ut uppgifterna till om raderingen. De åläggs därmed en skyldighet att vidta åtgärder, inklusive tekniska åtgärder, för att informera tredje part om begäran från den registrerade och för att radera alla länkar eller kopior eller replikeringar av sådana personuppgifter. Detta gäller dock inte om det skulle vara en alltför betungande insats eller visa sig vara omöjligt. Meddelandeskyldigheten avser framför allt att stärka rätten till radering i nätmiljö.<sup>253</sup> Emellertid har skyldigheten ansetts göra för lite för den enskildes kontroll och en effektiv applicering av rätten till att bli bortglömd. Tredje parter kan vara svåra att nå och det saknas garanti på att data hos dem faktiskt kommer att raderas.<sup>254</sup>

---

<sup>246</sup> Art. 17.3 e GDPR.

<sup>247</sup> Ausloos (2020) s. 268 f.

<sup>248</sup> Wendleby & Wetterberg (2019) s. 230 ff.

<sup>249</sup> Axberger (2022) s. 240.

<sup>250</sup> Öman (2023), kommentaren till artikel 17 GDPR.

<sup>251</sup> Öman (2023), kommentaren till artikel 17 GDPR.

<sup>252</sup> Art. 17.2 GDPR.

<sup>253</sup> Skäl 66 GDPR.

<sup>254</sup> Vrabc (2021) s. 157.

### 3.2.5 Utmaningar

#### 3.2.5.1 *Rättighetens tolkning och implementering*

Bedömningen avseende om det föreligger en rätt till radering är komplex och kräver en noggrann analys utifrån det specifika fallet. Att det dessutom finns olika tolkningar av lagstiftningen och att oenighet råder angående rättighetens räckvidd försvårar bedömningen och ger upphov till ett tolkningsutrymme som skapar rättsosäkerhet på området.<sup>255</sup> Visserligen har enskilda som samtyckt till behandling av data för ett visst ändamål rätt att få dessa uppgifter raderade från systemet om grund för radering föreligger. Detta innebär dock inte att varje begäran resulterar i att all personlig data raderas. Det kan föreligga en rad undantag som ger organisationen en fortsatt rätt att behandla uppgifterna. Hur långtgående dessa undantag ska anses vara och när de kan komma att aktualiseras blir en bedömning i det enskilda fallet. Exempelvis får det nödvändighetskriterium som genomsyrar samtliga undantag bedömas i varje enskilt fall. Det saknas även riktlinjer över hur raderingen mer specifikt ska utföras vilket resulterar i att varje organisation till viss del självständigt får besluta hur de ska implementera rättigheten.

Medlemsstater kan också genom nationell rätt begränsa rätten till radering, något som belyser systemets komplexitet.<sup>256</sup> Exempelvis är rätten till radering i Sverige inte tillämplig på vårdgivares och kvalitetsregisters behandling av personuppgifter då PDL innehåller en motsvarande rätt att få bli utplånad i och med journalförstöring. Sådan journalförstöring gäller dock enbart radering av uppgifter i en patientjournal som har samlats in inom offentlig eller privat hälso- och sjukvård.<sup>257</sup> Att olika medlemsstater kan ha olika regelverk och normer kring dataskydd och rätten till radering kan leda till harmoniseringsvårigheter. Något som även kan försvåra att rätten till radering respekteras likvärdigt i samtliga medlemsstater. Förutom bestämmelserna om registrerades rätt till radering i GDPR behöver alltså nationella bestämmelser och praxis beaktas vid tillämpningen av rätten till radering.

#### 3.2.5.2 *Privat aktör bedömer rättigheten*

Att det åligger den personuppgiftsansvarige att bedöma huruvida rätten till radering föreligger eller inte har ifrågasatts med hänsyn till rättssäkerheten.<sup>258</sup> Visserligen medför bedömningen att utsedda myndigheter inte belastas med arbete och att en större mängd förfrågningar kan hanteras. Dock kan exempelvis ett företag ha ett eget intresse av att minimera rätten till radering vilket kan utgöra en risk för godtyckligt maktutövande. Emellertid kan det

---

<sup>255</sup> Andersson (2019) s. 38 f.

<sup>256</sup> Art. 23 EHDS; skäl 156 GDPR.

<sup>257</sup> Jfr 1 kap. 3 och 4 § PDL.

<sup>258</sup> Wendleby (2021) s. 399 f.



motsatsvis tänkas att det personuppgiftsansvariga vill att rätt beslut fattas då den registrerade har möjlighet att utkräva skadestånd från dem.<sup>259</sup> Att beakta är att olika företag och myndigheter kan ha tillgång till skilda resurser och expertis på området. Exempelvis har mindre företag möjligtvis sämre tekniska och juridiska förutsättningar än ett större företag att bedöma huruvida uppgifterna ska raderas. Att rätten till radering ska bedömas av olika företag, myndigheter, organisationer och så vidare utan samarbete eller kommunikation sinsemellan kan onekligen medföra brister i hur den registrerades rättigheter behandlas och bedöms.<sup>260</sup> En personuppgiftsansvarig myndighet som har att bedöma rätten till radering ska dessutom ta avstamp i förvaltningsrättsliga principer som till exempel likabehandlings- och objektivitetsprincipen samt motiveringsskyldigheten. Detta för att säkerställa att myndighetens beslutsfattande är sakligt och förenlig med tidigare beslut.<sup>261</sup>

### 3.2.5.3 *Intresseavvägningar*

En av de största utmaningarna är hur den registrerades rätt till radering ska balanseras med andra berättigade intressen, såsom yttrandefrihet, offentligt intresse och rätten till information. Ibland kan det finnas ett allmänintresse av att behålla viss information för medicinsk forskning eller historiska arkiv.<sup>262</sup> Exempelvis kan uppgifter rörande hälsa behöva behållas under långa tidsperioder av lagstadgade skäl, såsom medicinsk historik och forskningsändamål. Att uppfylla krav på datalagring samtidigt som man respekterar rätten till radering kan vara komplicerat. Här kan också nämnas att det fördes diskussioner vid utvecklingen av GDPR om dess eventuella påverkan på medicinsk forskning. Forskare och organisationer lyfte sin oro över en tänkbar negativ påverkan på personuppgiftsrelaterad forskning. Det går till exempel att tänka sig att forskning, innovation och beslutsfattande riskerar att drabbas negativt om enskilda ges möjlighet att nyttja rätten till radering i allt för många fall då de tillgängliga personuppgifterna isåfall reduceras.<sup>263</sup>

### 3.2.5.4 *Tekniska utmaningar*

Rätten till radering kan även kompliceras till följd av tekniska utmaningar. Personuppgifter kan bland annat vara lagrade i ett flertal system, på olika platser samt i olika former vilket kan försvåra identifiering och radering. Att fullständigt radera e-hälsodata från komplexa hälsoinformationssystem eller att säkerställa att data inte längre kan återskapas kan således vara problematiskt.<sup>264</sup>

---

<sup>259</sup> Art. 82 GDPR.

<sup>260</sup> Ausloos (2020) s. 413–415.

<sup>261</sup> Karlsson Alverhill (2023) s. 108 f.

<sup>262</sup> Ausloos (2020) s. 298–301.

<sup>263</sup> Ploem M. C., Essink-Bot M. L., Stronks K (2013) s. 3534; Rumbold J. M. & Pierscionek B (2017) s. 47.

<sup>264</sup> Ausloos (2020) s. 459–462.

## 4 Radering av e-hälsodata vid sekundär användning

### 4.1 E-hälsodata som känslig personuppgift

För att rätten till radering ska kunna tillämpas krävs först och främst att det överhuvudtaget är tal om behandling av personuppgifter då det utan en sådan gränsdragning hade varit omöjligt att avgöra vilken data som behöver raderas.<sup>265</sup> Samtliga minimikategorier av e-hälsodata som hälsodatainnehavare ska tillgängliggöra för sekundär användning är i grund och botten uppgifter om hälsa eller genetiska uppgifter som direkt eller indirekt går att koppla till en levande fysisk person. Personlig e-hälsodata utgör på så vis en så kallad känslig kategori av personuppgifter enligt GDPR.<sup>266</sup>

Trots att rätten till radering enligt praxis främst har tillämpats avseende information på internet kan den, såsom den beskrivs i GDPR, även appliceras på hälsodata som behandlas för sekundär användning. Detta då rätten omfattar samtliga situationer där personuppgiftsansvariga kan bli skyldiga att radera personuppgifter.<sup>267</sup> I förslaget till EHDS anges även att förordningen avser att specificera och komplettera fysiska personers rättigheter enligt GDPR i relation till sekundär användning av deras personliga e-hälsodata. Alltså ska de i GDPR angivna rättigheterna fortsätta gälla oavsett i vilken medlemsstat data behandlas, typ av vårdgivare, källor till data eller den fysiska personens hemvistland.<sup>268</sup> Här görs emellertid ingen notering kring rättigheternas eventuella giltighet eller ogiltighet i kontexten av datadelning för sekundär användning.

Vid sekundär användning av e-hälsodata enligt EHDS ska hälsodataåtkomstorgan eller hälsodatainnehavare anonymisera eller pseudonymisera e-hälsodata så att identifiering av den enskilde förhindras. Detta ska ske tidigt i processen efter en ansökan eller begäran om hälsodata.<sup>269</sup> E-hälsodata som blivit anonymiserad utgör icke-personlig e-hälsodata och faller därmed utanför GDPR.<sup>270</sup> Således utesluts en rätt till radering vid sekundär användning av dessa oberoende vilken eventuell skada en sådan behandling kan orsaka och hur önskvärd en radering än kan tänkas vara. Så fort data anonymiseras förlorar alltså den enskilde sina rättigheter till denna.<sup>271</sup> Det har på så vis även framförts att korrekt anonymisering motsvarar radering och därmed att rätten

---

<sup>265</sup> Ausloos (2020) s. 128.

<sup>266</sup> Art. 2.2a EHDS och art. 9 GDPR.

<sup>267</sup> Jfr art. 17 GDPR.

<sup>268</sup> Art. 1.2a EHDS och skäl 8 EHDS.

<sup>269</sup> Se avsnitt 2.3.5.2.

<sup>270</sup> Art. 2.2 b EHDS.

<sup>271</sup> Vrabc (2021) s. 147 f.

till radering möjligtvis kan tillgodoses genom att data anonymiseras.<sup>272</sup> Här har dock oro framförts över att anonymisering kan användas på ett kontra-intuitivt sätt för att försätta den enskilde i en maktlös position. Detta då en anonymisering förhindrar enskilda från att förstå, granska och ifrågasätta hur data används samtidigt som den personuppgiftsansvarige har att bedöma huruvida anonymiseringen är adekvat. Den personuppgiftsansvarige kan på så vis hävda att den enskildes rättigheter är omöjliga att tillgodose eftersom de påstås sakna möjlighet att återidentifiera datasubjektet.<sup>273</sup> Samtidigt anses ofta en tillförlitlig avidentifiering av e-hälsodata vara svår att uppnå, särskilt då tillräcklig information måste behållas för att kunna användas för de ändamål som avses uppfyllas i samband med sekundär användning. Här får även vägas in att tillräckligt anonymiserade personuppgifter dessutom ofta anses göra data mindre användbar alternativt värdelös.<sup>274</sup>

Om däremot pseudonymiserad e-hälsodata behandlas är de dock fortfarande att betrakta som personuppgifter då möjligheten till identifiering, om än lägre, kvarstår.<sup>275</sup> Särskilt då det inte heller ställs något krav på att all information som möjliggör identifieringen av den registrerade behöver innehas av en och samma person.<sup>276</sup> Här har även angetts att pseudonymisering inte bör utgöra ett verktyg för personuppgiftsansvariga att undanta sig själva från GDPR:s tillämpningsområde.<sup>277</sup>

Möjligheten att identifiera en person utifrån viss e-hälsodata kräver att hänsyn tas till de specifika omständigheterna i fallet och samtliga rimliga medel som kan tänkas användas, antingen av den personuppgiftsansvariga eller av någon annan person.<sup>278</sup> Dessa rimliga medel kan bland annat innebära att det inte får vara för kostsamt, tidskrävande eller praktiskt taget omöjligt eller olagligt att identifiera en person genom uppgifterna.<sup>279</sup> Här kan även faktorer såsom med vem anonymiserade data kommer delas med, hur den kommer behandlas och vilken annan data den kommer eller kan bli kombinerad med beaktas.<sup>280</sup> Enbart en hypotetisk identifiering räcker således inte för att en person ska anses identifierbar enligt GDPR. Därmed kan samma dataset anses utgöra personuppgifter inom en behandlingskontext men inte inom en annan. Förutom att bedömningen beror på de aktuella omständigheterna behöver även hänsyn tas till risken för återidentifiering över tid.<sup>281</sup> Något som problematiseras av att

---

<sup>272</sup> Ausloos (2020) s. 141.

<sup>273</sup> Ausloos (2020) s. 143.

<sup>274</sup> Ausloos (2020) s. 142.

<sup>275</sup> Skäl 26 GDPR; Ausloos (2020) s. 143.

<sup>276</sup> Artikel 29-gruppens yttrande 4/2007, p s. 18 ff.

<sup>277</sup> Ausloos (2020) s. 144.

<sup>278</sup> Artikel 29-gruppens yttrande 4/2007, s.15; Artikel 29-gruppens yttrande 05/2014 s. 5.

<sup>279</sup> Förslag till avgörande av generaladvokat Campos Sánchez-Bordona i mål C-582/14 p. 68.

<sup>280</sup> Artikel 29-gruppens yttrande 05/2014 s. 10.

<sup>281</sup> Ausloos (2020) s. 141 f.

svårigheter avseende anonymisering av personuppgifter bedöms öka i takt med dagens teknikutveckling.<sup>282</sup>

I förslaget till EHDS förbjuds hälsodataanvändare att försöka återidentifiera den enskilde bakom pseudonymiserad e-hälsodata.<sup>283</sup> Dock verkar inte återidentifieringsförbudet täcka andra aktörer, vilka med rimliga medel kan tänkas återidentifiera en person såsom hälsodataåtkomstorganet. Andra tekniska och organisatoriska åtgärder vidtas dock för att förhindra återidentifiering vilket kan resultera i att pseudonymiserad e-hälsodata trots allt inte anses utgöra personuppgifter. Förutsatt att dessa åtgärder är lämpliga.<sup>284</sup> Exempelvis kan medicinska forskningsdata som pseudonymiserats genom kodning fortfarande betraktas som identifierbar personlig data. Om denna data dock överförs till en tredje part, såsom ett läkemedelsföretag, som inte har möjlighet att få tillgång till kodnyckeln kan denna data övergå till att inte anses utgöra personlig data.<sup>285</sup>

På så vis lär rätten till radering inte vara möjlig att tillämpa vid sekundär användning om e-hälsodata väl har anonymiserats eller överförs till en hälsodataanvändare i pseudonymiserat format. Sistnämnda är under förutsättningen att hälsodataanvändare inte kan få åtkomst till informationen som krävs för att avpseudonymisera data. Enligt förslaget till EHDS ska sådan information innehas av hälsodataåtkomstorganet eller en myndighet som agerar som betrodd tredje part enligt nationell rätt, alltså antas hälsodataanvändaren inte kunna få åtkomst till informationen.<sup>286</sup>

Hur som helst kan rätten till radering tänkas vara applicerbar avseende e-hälsodata om denna inte bedöms lämpligen anonymiserad. Att betona är att anonymisering kan vara svårt när man har att göra med särskilt känsliga e-hälsodata såsom de avseende sällsynta sjukdomar, uppgifter från biobanker och självgenererad e-hälsodata via exempelvis hälsoapplikationer.<sup>287</sup> Utöver detta bör rätten till radering kunna tillämpas avseende icke-anonymiserad e-hälsodata som innehas av hälsodatainnehavare eller hälsodataåtkomstorganet innan en överföring sker till hälsodataanvändare.

---

<sup>282</sup> Ausloos (2020) s. 142.

<sup>283</sup> Art. 2.1a EHDS.

<sup>284</sup> Ausloos (2020) s. 132.

<sup>285</sup> Artikel 29-gruppens yttrande 05/2014 s. 20 f.

<sup>286</sup> Art. 44 EHDS.

<sup>287</sup> Skäl 64 EHDS.

## 4.2 Begära radering

För att begära radering av personlig e-hälsodata måste den enskilde vända sig till den personuppgiftsansvariga för databehandlingen. Detta förutsätter givetvis att den enskilde dels överhuvudtaget är medveten om att dennes personliga e-hälsodata behandlas, dels att data i fråga fortfarande är att betrakta som en personuppgift.<sup>288</sup> Eftersom e-hälsodata behandlas i flera olika led efter ett beviljat datatillstånd eller begäran om hälsodata för sekundär användning blir därmed även olika aktörer ansvariga för behandlingen. Både hälsodatainnehavare, eventuellt betrodda hälsodatainnehavare, hälsodataåtkomstorgan, hälsodataanvändare och nationella kontaktpunkter är personuppgiftsansvariga i sina respektive roller i de olika stegen. Vem den enskilde ska vända sig till med en raderingsbegäran beror alltså på hos vem e-hälsodata behandlas.<sup>289</sup>

Till följd av ett beviljat datatillstånd eller en begäran om hälsodata skickar hälsodataåtkomstorganet en åtkomstbegäran till hälsodatainnehavaren. När hälsodatainnehavaren sedan delar den personliga e-hälsodatan med organet är hälsodatainnehavaren att anse som personuppgiftsansvarig för denna delning. Sedan är hälsodataåtkomstorganet personuppgiftsansvarig för behandlingen av personlig e-hälsodata när organet samlar in, förbereder och sedan tillgängliggör data för hälsodataanvändaren.<sup>290</sup>

Hälsodataanvändaren är i sin tur personuppgiftsansvarig för behandlingen av personlig e-hälsodata i pseudonymiserat format i hälsodataåtkomstorganets säkra behandlingsmiljö enligt sitt datatillstånd.<sup>291</sup> På uppdrag av hälsodataanvändaren är hälsodataåtkomstorganet personuppgiftsbiträde för denna behandling samt för behandling för att besvara en begäran om hälsodata.<sup>292</sup>

Om en betrodd hälsodatainnehavare behandlar personlig e-hälsodata relaterad till tillhandahållandet av e-hälsodata till hälsodataanvändaren enligt ett datatillstånd eller begäran om hälsodata är denne personuppgiftsansvarig för behandlingen. Den betrodda hälsodatainnehavaren är också personuppgiftsbiträde för hälsodataanvändaren när denne tillhandahåller data genom en säker behandlingsmiljö.<sup>293</sup> Vid delning av e-hälsodata genom Hälsodata@EU anses de nationella kontaktpunkterna gemensamt personuppgiftsansvariga för den behandling de utför på plattformen. EU-kommissionen är kontaktpunkternas personuppgiftsbiträde vid sådan behandling.<sup>294</sup>

---

<sup>288</sup> Slokenberga m.fl. (2021) s. 97; Ausloos (2020) s. 446.

<sup>289</sup> Jfr art. 51 EHDS; skäl 55 EHDS.

<sup>290</sup> Art. 51.1a EHDS; skäl 55 EHDS.

<sup>291</sup> Skäl 49 EHDS.

<sup>292</sup> Art. 51.1a EHDS; skäl 55 EHDS.

<sup>293</sup> Art. 51.1a EHDS; skäl 55 EHDS.

<sup>294</sup> Art. 52 EHDS.

### 4.3 Grunder för rätt till radering

Sekundär användning grundar sig i att e-hälsodata som samlats in för ett ändamål används för ett annat. Om hälsodataanvändare således beviljas åtkomst till e-hälsodata för sekundär användning kommer den enskildes data behandlas för andra ändamål än för vilka de samlades in för. Således kan detta antas utgöra en grund för radering förutsatt att behandlingen inte anses förenlig med de ursprungliga ändamålen för insamling.<sup>295</sup> Här får en bedömning av respektive sorts e-hälsodata ske med beaktande av de ändamål för vilka de samlades in. Exempelvis har elektroniska patientjournaler som upprättats inom hälso- och sjukvården behandlats för tillhandahållandet av den enskildes hälso- och sjukvård. Data som individer själva genererar genom hälsoappar får antas ha behandlats för att tillhandahålla information om enskilda personers hälsa eller för leverans av vård för andra ändamål än just tillhandahållande av hälso- och sjukvård.<sup>296</sup>

När e-hälsodata väl behandlas av hälsodataåtkomstorgan görs detta i syfte att tillgängliggöra data för sekundär användning. Sådan behandling bör enbart ske i den utsträckning det är nödvändigt för detta ändamål. Samma gäller när pseudonymiserad e-hälsodata behandlas av hälsodataanvändare i hälsodataåtkomstorganets säkra behandlingsmiljö. Om den inte längre anses nödvändig för sekundär användning enligt de ändamål som ligger bakom en godkänd ansökan eller begäran så bör e-hälsodata kunna raderas.<sup>297</sup> Dock ligger bedömningen kring behandlingens fortsatta nödvändighet på den personuppgiftsansvarige vilket ger ett stort skönsmässigt utrymme avseende informationens relevans, speciellt då bedömningskriterier på området saknas.

Sekundär användning av e-hälsodata baseras inte på samtycke som grund för behandlingen. Ett återkallande av samtycke som grund för radering kan således inte bli aktuellt. Hur som helst är det möjligt att samtycke ligger som grund för den ursprungliga inhämtningen och behandlingen hos hälsodatainnehavaren. Till exempel innebär ett samtycke till vård och behandling även att känsliga uppgifter får dokumenteras i en patientjournal.<sup>298</sup> Att enskilda, beroende på om samtycke är den legala basen för insamling av e-hälsodata, kan begära rätt till radering hos hälsodatainnehavaren innan denne mottagit en åtkomstförfrågan från hälsodataåtkomstorganet faller dock utanför uppsatsen då data inte behandlas för sekundär användning ännu.

Radering kan även aktualiseras om den enskilde invänder mot att dennes personliga e-hälsodata behandlas för sekundär användning och den enskildes intresse av att få uppgifterna raderade väger tyngre än den

---

<sup>295</sup> Art. 17.1 a GDPR.

<sup>296</sup> Jfr art. 2.2 aca EHDS.

<sup>297</sup> Art. 17.1 a GDPR.

<sup>298</sup> Wendel & Mattsson (2022) s. 136.

personuppgiftsansvariges intresse av att behandla uppgifterna.<sup>299</sup> E-hälsodata ska därmed raderas förutsatt att den personuppgiftsansvarige inte kan påvisa berättigade intressen som väger tyngre än den enskildes intresse av radering. Vid sekundär användning behandlas e-hälsodata för de accepterade ändamål som ligger bakom ett godkänt datatillstånd eller begäran om hälsodata. Dessa ändamål anknyter i stor del till folkhälsan och utvecklingen av hälso- och sjukvården.<sup>300</sup> Den personuppgiftsansvariges berättigade intresse att behandla e-hälsodata kan således hänföras till folkhälsan och allmän intresset. Det är dock inte ovanligt att folkhälsoändamål kan stå i konflikt med den enskilda individens rättigheter.<sup>301</sup> Något som föranleder en diskussion om vid vilka tillfällen det kollektiva allmänna intresset ska anses väga tyngre än individuella rättigheter.

Rätten till radering kan anses del av enskildas rätt till integritet och den enskildes intresse av radering kan därför baseras på skydd för den egna integriteten. På så vis blir det relevant att kartlägga när rätt till integritet avseende hälsoinformation ska anses sekundärt i förhållande till samhällets intresse. Exempelvis kan tillgängliggörande av hälsodata avseende smittbara sjukdomar såsom Covid-19 anses ha ett stort samhällligt värde och motivera att enskildas integritet påverkas.<sup>302</sup> Att e-hälsodata består av känsliga hälsorelaterade personuppgifter kan föranleda att den enskilde vill förhindra ytterligare behandling av dessa då denne kan komma att drabbas negativt om informationen skulle missbrukas. Uppgifter om hälsotillstånd kan upplevas som mycket integritetskänsliga för enskilda då de är nära förknippade med många individers identitet och självbild samt deras fri- och rättigheter.<sup>303</sup> Bland annat kan vissa hälsorelaterade uppgifter än idag orsaka stigma, till exempel om en enskild har en viss sjukdom eller inte. Stigmatisering till följd av sådan information riskerar att resultera i negativa konsekvenser avseende mental hälsa, familjeliv, arbete, banklån, hälsa och livförsäkringar.<sup>304</sup> Till exempel kan e-hälsodata innehålla information som skulle kunna påverka den enskildes sociala eller professionella framtid, bland annat den enskildes jobb- och möjligheter. Dessutom kan möjligheterna att genom maktutövning kränka enskildas integritet genom användning av dessa uppgifter anses stora. Integritetsintrång och incidenter inom hälso- och sjukvården är vidare inte ovanligt.<sup>305</sup>

---

<sup>299</sup> Se avsnitt 3.2.2.3.

<sup>300</sup> Se avsnitt 2.3.3.

<sup>301</sup> Ausloos (2020) s. 413 och 265 f.

<sup>302</sup> Correia, Rego & Nunes (2021) s. 63.

<sup>303</sup> Wendel & Mattsson (2022) s. 162; skäl 51 GDPR.

<sup>304</sup> Correia, Rego & Nunes (2021) s. 62.

<sup>305</sup> TT, *Staten brister i att skydds personuppgifter*, Dagens medicin, 18-04-2024; Jesper Cederberg, *Uppgifter till salu på darknet efter attacken mot Sophiahemmet*, Läkartidningen, 04-03-2024.

Avvägningen mellan å ena sidan den enskildes integritet och å andra sidan samhällets intresse av att e-hälsodata behandlas för sekundär användning måste dessutom utföras av den personuppgiftsansvarige i varje enskilt fall. Det är här tänkbart att avvägningen till viss del varierar beroende på vilken kategori av e-hälsodata som behandlas för sekundär användning och för vilket ändamål. Här kan diskuteras om den enskildes intresse av integritetsskydd generellt sätt bör bedömas högre vid behandling av de datakategorier som enligt EHDS-förordningen bedöms vara mer känsliga, såsom genetisk data, data från biobankar och data från hälsoappar.<sup>306</sup> Eller om vissa ändamål för sekundär användning ska anses väga tyngre än andra i avvägningen mot intrång i enskildas integritet, såsom till exempel att behandling sker på grund av ett allmänintresse inom folkhälsa jämfört med i utbildningssyfte. Dessutom ska vissa ändamål för sekundär användning enbart vara tillåtna för offentliga myndigheter och EU vilket skulle kunna antyda att dessa bör anses väga tyngre än de resterande ändamålen.

EHDS-förordningen tillhandahåller en rättslig grund i enlighet med GDPR för den sekundära användningen av personlig e-hälsodata.<sup>307</sup> Förutsatt att de i artikel 6 GDPR angivna lagliga grunder för behandling också uppfylls har e-hälsodata inte behandlats olagligen och radering på den här grunden tycks därmed uteslutas. Förutsatt att hälsodatainnehavare, hälsodataåtkomstorgan eller hälsodataanvändare som vill behandla uppgifter kan visa att detta föreligger i det enskilda fallet.

Någon rättslig förpliktelse som anger att e-hälsodata endast får behandlas en viss tid existerar inte. Här kan dock nämnas att för de fall hälsodataanvändare beviljats ett datatillstånd är tillståndet tidsbegränsat, med möjlighet att ansöka om förlängning.<sup>308</sup>

I kontexten av sekundär användning av e-hälsodata är därmed rätten till radering mest sannolik att aktualiseras under grunderna i artikel 17.1 a) och c), alltså att behandling av e-hälsodata inte längre är nödvändig för de ändamål som de samlades in för eller att den enskilde motsätter sig behandlingen och den personuppgiftsansvarige inte har tyngre vägande skäl att fortsätta behandlingen. Om e-hälsodata väl har behandlats och publicerats är det dock svårare att radera data, om inte omöjligt, då tidigare gjorda användningar av data inte kan göras ogjorda.<sup>309</sup>

---

<sup>306</sup> Jfr art. 33.5 EHDS.

<sup>307</sup> Se avsnitt 3.2.2.4.

<sup>308</sup> Se avsnitt 2.3.4.1.

<sup>309</sup> Slokenberga m.fl. (2021) s. 96 f.



## 4.4 Begränsningar av rätt till radering

Trots att en grund för radering föreligger kan e-hälsodata likväl fortsätta att behandlas om den personuppgiftsansvarige bedömer att en begränsning enligt artikel 17.3 GDPR aktualiseras. Att yttrande- och informationsfrihet skulle påverkas vid en radering av e-hälsodata som behandlas för sekundär användning eller att aktörer bakom sekundär användning ska anses utöva en rätt till yttrande- och informationsfrihet och därmed hindra radering på denna grund är osannolikt. Det blir inte heller relevant att begränsa radering för att ha möjlighet att fastställa, göra gällande eller försvara rättsliga anspråk när det kommer till sekundär användning av e-hälsodata. De begränsningar som dock kan antas göra sig gällande när e-hälsodata behandlas för sekundär användning är dels uppfyllande av rättslig förpliktelse, utförande av uppgift av allmänt intresse eller led i myndighetsutövning och dels viktigt allmänt intresse på folkhälsoområdet.

Hälsodatainnehavare kan ha en lagstiftad skyldighet att under en viss period spara och inneha personuppgifter via arkivering och har därigenom möjlighet att neka radering till följd av detta. Så kan exempelvis vara fallet för vårdgivare. Det föreligger dock ingen sådan skyldighet för hälsodataåtkomstorgan eller hälsodataanvändare. Emellertid är det möjligt att hälsodataanvändare kan neka radering till följd av vetenskapliga ändamål. Dock måste hälsodataanvändaren kunna visa att en radering förhindrar eller äventyrar den planerade forskningen. Att radering eller anonymisering av data självständigt skulle påverka ett forskningsprojekt är osannolikt. Upprepade begäranden om borttagning från olika individer kan däremot riskera att försvaga ett datasets relevans. Att radering av e-hälsodata vid sekundär användning skulle hindras på denna punkt är på så vis inte troligt.

Hälsodatainnehavare, eventuellt betrodda hälsodatainnehavare, hälsodataåtkomstorgan och hälsodataanvändare har en rättslig förpliktelse enligt EU-rätten genom EHDS-förordningen att behandla vissa kategorier av e-hälsodata för sekundär användning. När exempelvis hälsodataåtkomstorganet samlar in, förbereder och delar e-hälsodata till hälsodataanvändare får behandlingen anses krävas för att uppfylla organets rättsliga förpliktelse att efter en godkänd åtkomstansökan göra e-hälsodata tillgänglig för sekundär användning i en säker behandlingsmiljö. När hälsodataanvändare får laglig tillgång till pseudonymiserad e-hälsodata inom hälsodataåtkomstorganets behandlingsmiljö sker inte behandlingen till följd av en rättslig förpliktelse. Hälsodataanvändare är inte förpliktad att ansöka om åtkomst till e-hälsodata utan detta sker frivilligt.

Att radering kan nekas om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse på folkhälsoområdet är särskilt relevant i samband med

sekundär användning av e-hälsodata.<sup>310</sup> På så vis gäller rätten till radering inte för e-hälsodata om behandlingen är nödvändig för folkhälsans intresse. Huruvida personuppgiftsbehandlingen är nödvändig får bedömas utifrån EU-rätt eller nationell rätt. Exempelvis om behandling är nödvändig för att förhindra allvarliga gränsöverskridande hälsohot, såsom under Covid-19 pandemin. Både hälsodatainnehavare, inklusive betrodda, hälsodataåtkomstorgan och hälsodatainnehavare kan enligt denna punkt ha rätt att, oavsett en begäran om radering, behandla e-hälsodata för sekundär användning om det fyller ett allmänt intresse på folkhälsoområdet. Således kan en hälsodataanvändare neka radering om forskningen syftar till förebyggande eller yrkesmedicin, skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga standarder för kvalitet och säkerhet inom hälso- och sjukvård, läkemedel eller medicintekniska produkter.<sup>311</sup>

Här kan dock argumenteras att ett orsakssamband mellan behovet att begränsa den grundläggande rätten till dataskydd och värdet av folkhälsan är nödvändigt att fastställa. Att all hälsodata i samtliga fall kan omfattas av detta undantag från rätten till radering utan att ett konkret orsakssamband fastställs mellan den datan och folkhälsan är diskutabelt. Att utesluta rätten till radering enbart för att hälsodata kan ha en potentiell relevans bör inte kunna ske utan hälsodata bör anses vara av aktuell relevans för folkhälsan.<sup>312</sup> Om samtliga e-hälsodata som ska tillgängliggöras för sekundär användning enligt EHDS-förordningen förutsätts ha relevans för folkhälsan utan att en bedömning görs i det enskilda fallet riskerar en begränsning av rätten till radering bli en regel snarare än ett undantag. Det är upp till den personuppgiftsansvarige, som vill fortsätta behandla och behålla hälsodata, att bevisa att en begränsning föreligger i det enskilda fallet och att det bör finnas en rätt till radering för enskilda om det saknas konkreta folkhälsoskäl.

## 4.5 Sammanfattande kommentarer

En hälsodatainnehavare åläggs att göra e-hälsodata tillgänglig till hälsodataåtkomstorgan. Denne ska i sin tur göra denna e-hälsodata tillgänglig i ett anonymiserat eller pseudonymiserat format genom en säker behandlingsmiljö till hälsodataanvändare. Huruvida den enskilde har rätt till radering av e-hälsodata i det specifika fallet får den personuppgiftsansvarige i varje steg bedöma mot bakgrund av de i artikel 17 GDPR angivna förutsättningarna.

Den enskilde har en rätt till radering av sin e-hälsodata som behandlas för sekundär användning om den inte är avidentifierad i den grad de inte utgör en personuppgift och en grund för radering enligt artikel 17.1 GDPR föreligger

---

<sup>310</sup> Art. 17.3 c GDPR; se avsnitt 3.2.3.3.

<sup>311</sup> Correia, Rego & Nunes (2021) s. 64.

<sup>312</sup> Correia, Rego & Nunes (2021) s. 64.

i dennes specifika fall. En risk för återidentifiering av den enskilda bör motivera en rätt till radering, särskilt när det gäller känsliga personliga e-hälsodata där fullständig anonymisering eller pseudonymisering kan vara utmanande. Om en grund föreligger kan inte hälsodatainnehavare, hälsodataåtkomstorgan eller hälsodataanvändare fortsätta behandla data efter en begäran om radering om de inte kan visa att en begränsning av rätten till radering enligt artikel 17.3 GDPR gör sig gällande. Något som, baserat på ovanstående analys, är mycket troligt vid sekundär användning av e-hälsodata då behandling utifrån de accepterade ändamålen för sekundär användning relaterar till samhällsintresset av att behandla uppgifterna.

## 5 Avslutande diskussion

Rätten till radering är komplex i förhållande till e-hälsodata och måste förstås i kontexten av hälso- och sjukvård samt hälsorelaterad forskning och innovation. Medlemsstaters ojämna implementering av GDPR gör dessutom att rätten till radering kan skilja sig inom och mellan medlemsstater. Emellertid bedöms rätten till radering generellt sett mycket begränsad vid sekundär användning av e-hälsodata. Dels till följd av anonymisering, dels då behandling kan anses uppfylla folkhälsoändamål och ligga i allmänhetens intresse samt väga mer än den enskildes intresse av att uppgifterna raderas. Oavsett om radering vidtas eller nekas i det enskilda fallet ska den personuppgiftsansvarige kommunicera detta med den enskilde vilket främjar transparens.

Här kan man även ställa sig frågande huruvida rätten till radering överhuvudtaget bör kunna tillämpas vid sekundär användning av e-hälsodata. Givetvis måste enskildas e-hälsodata och integritet värnas vid sekundär användning och därmed individens rättigheter, däribland rätten till radering, respekteras. Dessutom kan rätten till radering anses ännu viktigare att respektera och upprätthålla i samband med digitalisering och teknologiska framsteg som tillåter en ökad spridning och bevarande av information. Vilket hälsodataområdet onekligen bidrar till genom nationell och gränsöverskridande sekundär användning av e-hälsodata. Risker kan onekligen göra sig gällande för individer vars information används om inte lämpliga säkerhetsåtgärder föreligger. Att ett undantag från rätten till radering skulle förutsättas föreligga i samtliga fall och för samtliga kategorier av e-hälsodata eller ändamål för sekundär användning kan därmed ifrågasättas.

Hur som helst är det av yttersta vikt att en balans existerar mellan å ena sidan individens integritet och å andra sidan behovet av att använda e-hälsodata för samhällets bästa i varje enskilt fall. Huruvida allmänhetens intresse av sekundär användning bör anses stå över den enskildas integritet är dock oklart. Genom att rätten till radering utifrån artikel 17 GDPR har begränsad tillämplighet avseende samhällsgagnande ändamål får så inte anses vara fallet. Det går inte heller att förneka att sekundär användning av e-hälsodata kan medföra stora samhällsfördelar inom hälso- och sjukvårdssektorn. Något som även kan vägas mot att rätten till integritet, liksom rätten till radering, inte är absoluta och kan inskränkas i vissa fall.

Det kan även ifrågasättas om rätten till radering i praktiken överhuvudtaget skulle kunna genomföras i kontexten av sekundär användning av e-hälsodata. Eftersom rätten till radering ska bedömas i varje enskilt fall är även frågan om åtkomst kan beviljas avseende samma e-hälsodata för andra ändamål eller för andra hälsodataanvändare. Om e-hälsodata dessutom inte kan raderas från ursprungskällan på grund av datalagringskrav kan den enskildes möjlighet att

förhindra att dennes e-hälsodata behandlas för sekundär användning i praktiken anses illusorisk.

Det är dock viktigt att ha i åtanke de personer som kan komma att se sin integritet kränkt när hälsodataanvändare beviljas åtkomst till deras e-hälsodata, om än under anonymiserad eller pseudonymiserad form. Exempelvis de personer i samhället som lever med vissa medicinska tillstånd och sällsynta sjukdomar som ser sig särskilt utsatta för stigmatisering. Uppgifter gällande psykiska sjukdomar, vissa smittsamma sjukdomar såsom HIV, missbruk och beroendesjukdomar kan också antas vara särskilt känsliga i sammanhanget. Som vi har sett bygger emellertid hälsodataområdet på ett flertal skyddsåtgärder, utöver anonymisering och pseudonymisering, som avser att förhindra missbruk av e-hälsodata. Något som även kan tala för att rätten till radering bör kunna begränsas utan att för den skull riskera den enskildes integritet.

Genom den opt-out möjlighet som införts i artikel 35f EHDS ska enskilda dessutom när som helst och utan att ange skäl kunna välja att avstå från att deras e-hälsodata används för sekundär användning. Om en enskild väljer att inte delta får e-hälsodata inte delas med hälsodataanvändare, inte ens i anonym form. På så vis grundar sig opt-out mekanismen och rätten till radering sig delvis i samma tanke om att EU-medborgare ska skyddas från att inte förekomma i sammanhang där de inte vill delta. För att därigenom främja enskildas integritet samt självbestämmande och kontroll över användning av deras e-hälsodata. Särskilt då sekundär användning kan genomföras utan informerat samtycke.

Enskilda ska kunna nyttja opt-out mekanismen både innan och under tiden deras uppgifter behandlas för sekundär användning. Därmed tillåts enskilda att avstå från att deras e-hälsodata överhuvudtaget behandlas för sekundär användning vilket även belyser opt-out förfarandets vikt som säkerhetsåtgärd. Motsatsvis kan rätten till radering först tillämpas efter att den personuppgiftsansvarige inom processen för sekundär användning väl har behandlat uppgifterna. Att enskilda har möjlighet att använda opt-out rätten innan behandlingen kan på sätt och vis liknas vid ett samtycke. Opt-out rätten bör då avse ett specifikt syfte med den sekundära användningen och inte enbart sekundär användning i sin helhet. Opt-out presumerar att ett samtycke föreligger och lägger över på den enskilde att aktivt avstå behandling och på så vis självständigt tillvarata sin rättighet.

Medlemsstaterna kan anta undantag från opt-out rätten och därmed tillåta sekundär användning av e-hälsodata trots att en enskild valt att inte delta. Detta får dock endast ske till förmån för viss sekundär användning av offentliga organ på nationell och EU-nivå och under strikta villkor. Något som betonar nödvändigheten av sekundär användning för att uppnå fördelar för samhället

i stort samtidigt som det ska ske under kontrollerade former för att minimera risker. Här kan det dock ifrågasättas om det är lämpligt för medlemsstater att införa ett undantag till opt-out för vetenskaplig forskning avseende studier om ovanliga sjukdomar. Detta då e-hälsodata rörande ovanliga sjukdomar kan vara problematisk att anonymisera eller pseudonymisera på ett lämpligt sätt vilket gör att individer därmed löper risk att identifieras. Oaktat om skyddet för individens integritet, särskilt återidentifieringsförbudet, kommer att fortsätta gälla när undantaget används. Förordningen anger även att eventuella undantag ska respektera individens grundläggande rättigheter och vara proportionerliga i förhållande till det allmänna intresset. Hur den här proportionalitetsbedömningen ska ske och hur olika allmänna intressen ska bedömas framkommer inte. Alltså bedöms vissa ändamål som rör allmänintresset kunna ligga till grund för tillgång till data från personer som valt att inte delta.

Vidare är det tänkbart att vissa länder väljer att införa undantag till opt-out medan andra inte gör det. Skillnader mellan medlemsstaterna kan resultera i att personer i olika EU-länder ges skilda möjligheter att invända mot användningen av sina personuppgifter. På så vis kan det även leda till en ojämlig behandling av registrerade personer i olika medlemsstater. Något som även riskerar att reproducera den nuvarande fragmenterade situationen som orsakats medlemsstaternas tolkning och ojämna implementering av GDPR. Att vissa medlemsstater antar strängare lagstiftning än andra kan möjligtvis leda till bias i datamängderna och på sikt utgöra ett hinder för sekundär användning.

Opt-out möjligheten är som sagt obegränsad, förutom de eventuella undantag en medlemsstat antagit, och den enskilde behöver inte ange skäl för sitt avstående. När det däremot gäller rätten till radering måste den personuppgiftsansvariga bedöma om grund för radering föreligger i det enskilda fallet. Dessutom kan radering nekas om den personuppgiftsansvarige bedömer att en begränsning av rättigheten är motiverad. På så sätt kan personuppgiftsansvarens bedömning huruvida rätten till radering kan utövas leda till oförutsägbara resultat för enskilda, särskilt när det saknas tydlig praxis. Något som förhindras om enskilda tillåts avstå i förhand från att deras e-hälsodata används.

Genom EHDS-förordningen framkommer det inte om opt-out rätten kan begränsas att enbart gälla en viss sorts data eller om det handlar om att godkänna delning av allt eller inget. Det även oklart hur möjligheten till opt-out kommer att hanteras och av vilken aktör, om medlemsstater inte väljer att hälsodataåtkomstorganet ska göra detta. Hur opt-out mekanismen kommer att fungera och hanteras i praktiken, liksom hur reversibiliteten ska genomföras, får antas besvaras genom vägledning och praxis när EHDS har trätt i kraft. Det kan dock tänkas lämpligt att en samordning mellan och inom medlemsstaterna bör ske för att förhindra avvikelser i tillvägagångssätt så att samtliga EU-

medborgare ges samma möjlighet att avstå behandling. Dessutom bör det diskuteras hur opt-out rätten kommer fungera för data som samlats in före ikraftträdandet av EHDS. Särskilt sådan data där det saknas en tydlig länk till individerna, såsom pseudonymiserad data.

En enskilds e-hälsodata, inklusive anonym sådan, får alltså inte delas med hälsodataanvändare om den enskilde valt att opt-out. Att data inte får behandlas gäller från den tidpunkt den enskilde valt att inte delta. På så vis tycks det innebära att även om en person sagt nej till framtida användning av sina data så kommer tidigare beviljade datatillstånd eller begäran att fortsätta gälla för behandlingen av deras data för sekundär användning. Således kan man i och för sig ställa sig frågan om rätten till radering kan eller bör kunna tillämpas här då den enskilde inte ges möjlighet att välja att inte få sina uppgifter behandlade om ett tillstånd eller begäran redan godkänts.

Sammantaget kan opt-out mekanismen anses exkludera rätten till radering vid sekundär användning av e-hälsodata enligt EHDS. Detta då möjligheten för enskilda att opt-out när som helst utesluter en rätt till radering eftersom e-hälsodata isåfall inte kan behandlas längre och därmed finns ingen data att radera. Dock kan man även se rätten till radering som ett komplement till opt-out mekanismen genom att ge individer ytterligare kontroll över hur deras e-hälsodata används och utöka skyddet för deras integritet och självbestämmande.

Det har framförts tankar att opt-out mekanismen riskerar att leda till negativa effekter för den sekundära användningen då den öppnar upp för enskilda att avstå. Något som kan leda till att de tilltänkta fördelarna med hälsodataområdet inte uppnås eftersom en lika stor andel data inte finns att tillgå. Exempelvis kan man tänka sig att en person kan vara mer tveksam till att dennes e-hälsodata används för sekundär användning om data avser sällsynta sjukdomar. Särskilt då behandling och skapande av e-hälsodata vid sekundär användning enligt EHDS kommer inkludera privata aktörer och aktörer som är verksamma utanför den traditionella konfidentiella relationen mellan en patient och en inom hälso- och sjukvården verksam person eller en medicinsk forskare. Allt detta kan riskera att människor med sådana sjukdomar eller andra minoritetsgrupper kan komma att använda opt-out möjligheten i större utsträckning. Något som troligen kan leda till en viss snedvridning i data då e-hälsodata från dessa individer inte kommer representeras i den datamängd som behandlas för sekundär användning för till exempel forskning, nya behandlingar, mediciner och så vidare. Det är även möjligt att enskilda helt enkelt motsätter sig delning av sin e-hälsodata i vissa fall men inte i andra till följd av andra personliga orsaker.

Det europeiska hälsodataområdet bygger givetvis på tillgång till enskildas e-hälsodata. På så vis är befolkningens förtroende för systemet grundläggande. En möjlighet för enskilda att opt-out kan, i motsats till tidigare stycke, även tänkas bidra till att bygga tillit hos EU-medborgare för delning av e-hälsodata. Detta då individer ges möjlighet att kontrollera och bestämma huruvida deras e-hälsodata ska kunna användas för sekundär användning. Dock förutsätter detta att samhällsmedborgare har kunskap om sekundär användning samt de skyddsåtgärder som EHDS-förordningen tillhandahåller för att lämpligen skydda deras e-hälsodata. Något som hälsodataåtkomstorgan bland annat åläggs att göra genom EHDS då organet ska ge generell information kring processen, enskildas rättigheter och hur e-hälsodata används. Här är det viktigt att sådan information tillgängliggörs på ett transparent sätt som är lättåtkomligt för samtliga invånare, oavsett ålder eller kognitiva eller andra funktionsvariationer. På så vis kan även tillit byggas upp till att personuppgifter inte missbrukas.

Här bör erhållas att behandling av e-hälsodata för sekundär användning endast är möjlig för de i EHDS specifikt angivna ändamålen, baserat på datatillstånd eller begäran utfärdad av ett hälsodataåtkomstorgan. Tydliga regler finns för vad hälsodataanvändare kan och inte kan göra med data. Dessutom kommer behandlingen enbart att kunna ske genom statliga säkra behandlingsmiljöer och ingen personlig e-hälsodata ska kunna laddas ner från dessa miljöer. Hälsodataanvändare kan härigenom högst få tillgång till pseudonymiserad data, om syftet inte kan uppnås med anonymiserad data. Vidare är det förbjudet för hälsodataanvändare att ens försöka återidentifiera enskilda.

Vidare forskning krävs för att förstå de komplexa lagliga och tekniska aspekterna av sekundär användning av e-hälsodata inom EU. Det är viktigt att utreda hur enskildas rättigheter enligt GDPR ska tillgodoses för olika behandlingar som genomförs med stöd av bestämmelser i EHDS. Uppsatsen försöker bidra till detta men givetvis kommer många aspekter förbli obesvarade tills vägledande praxis skapats. På så vis behöver rättsliga frågor fortsätta att utredas och besvaras i takt med att tolkningen och tillämpningen av EHDS:s bestämmelser avgörs av nationella domstolar och i sista hand EU-domstolen efter EHDS genomförande. Att tekniken oftast ligger före juridiken bidrar till att hälsodataområdet fortlöpande behöver granskas så att enskildas integritet och kontroll säkerställs. Nationell lagstiftning avseende rätten till radering av e-hälsodata bör även analyseras för att identifiera eventuella möjligheter och utmaningar kopplade till införandet av EHDS och även en opt-out klausul.

Sammanfattningsvis råder det ingen tvekan om att det finns stora fördelar med sekundär användning av e-hälsodata som kan stärka hälso- och sjukvården inom och mellan EU-medlemsstater. Detta hänger dock på att enskildas



rättigheter respekteras och att ett förtroende skapas för EHDS. Rätten till radering är begränsad vid sekundär användning men genom en introduktion av en opt-out möjlighet främjas enskildas kontroll över sin e-hälsodata vilket i kombination med övriga säkerhetsåtgärder lägger grunden för tillit. Något som kan möjliggöra den önskade effekten med EHDS. Hur opt-out möjligheten kommer att hanteras i praktiken samt huruvida den hjälper eller stjälper hälsodataområdet återstår att se om eller när EHDS antas.

# Käll- och litteraturförteckning

## Offentligt tryck

*Sverige*

### Utredningsbetänkanden

SOU 2023:76 Vidareanvändning av hälsodata för vård och klinisk forskning

SOU 1997:39 Integritet, offentlighet, informationsteknik

Dir. 2022:41 Hälsodata som nationell resurs för framtidens hälso- och sjukvård

### Rapporter

eHälsomyndigheten, *Förslag till färdplan för genomförandet av en nationell digital infrastruktur för hälso- och sjukvården (S2023/02108)*, september 2023.

Myndigheten för digital förvaltning (Digg), *Uppdrag att fortsatt etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte*, januari 2023.

Socialdepartementet och Sveriges Kommuner och Landsting, *Vision e-hälsa 2025 – gemensamma utgångspunkter för digitalisering i socialtjänst och hälso- och sjukvård*, Stockholm, 2016.

Socialstyrelsen, *Kartläggning av datamängder av nationellt intresse på hälsodataområdet – slutrapport*, oktober 2022.

Socialstyrelsen, *Socialstyrelsen och European Health Data Space (EHDS), (1369/2023) Förstudie om förordningens potentiella påverkan på Socialstyrelsens verksamhet*, 2023.

Vinnova, *Patientens röst om hälsodata*, maj 2022.

### Övrigt

En nationell strategi för life science (N2019/03157).

## *Europeiska unionen*

Amendments adopted by the European Parliament on 13 December 2023 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)).

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

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.

Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsförordningen).

Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen).

Europeiska unionen, Meddelande från kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén En EU-strategi för data, Bryssel, 19.2.2020, COM(2020) 66 final (europeiska datastrategin).

Förslag till avgörande av generaladvokat Jääskinen i mål C-131/12, Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González, EU:C:2013:424.

Förslag till avgörande av generaladvokat Campos Sánchez-Bordona i mål C-582/14, Patrick Breyer mot Bundesrepublik Deutschland, EU:C:2016:339.

Förslag till Europaparlamentets och Rådets förordning om ett europeiskt hälsodataområde, COM (2022) 197 final av den 3 maj 2022.

Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

Regulation (EU) 2024/... of the European parliament and of the council on the European health data space, 2022/0140(COD), 7553/24, Bryssel, 18 mars 2024.

Rådets slutsatser om individualiserad behandling för patienter (2015/C 421/03).

### EDPB

Riktlinjer 03/2020 om behandling av uppgifter om hälsa för vetenskapliga forskningsändamål i samband med covid-19 utbrottet, antagna den 21 april 2020 (EDPB-riktlinjer 03/2020).

Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, Version 1.1, antagna den 4 maj 2020 (EDPB-riktlinjer 05/2020).

### Artikel 29-gruppen

Artikel 29-gruppen, Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, antaget den 9 april 2014 (Artikel 29-gruppens yttrande 6/2014).

Artikel 29-gruppen, Yttrande 05/2014 om avidentifieringsmetoder, antaget den 10 april 2014 (Artikel 29-gruppens yttrande 05/2014).

Artikel 29-gruppen, Yttrande 4/2007 om begreppet personuppgifter, WP136, antaget den 20 juni 2007 (Artikel 29-gruppens yttrande 4/2007).

## Litteratur

Andersson, Elina (2019), *Rätten att bli bortglömd, ur ett rättighets- och rättssäkerhetsperspektiv*, *Insolvensrättslig Tidskrift*, Nr 1 2019.

Ausloos, Jef (2020), *The right to erasure in EU data protection law – From individual rights to effective protection*, Oxford University press, Oxford, 30-04-2020.

Axberger, Elisabeth (2022), *Rätt till radering av personuppgifter – Grundläggande fri- och rättigheter i en digital union*, *Europarättslig tidskrift*, nr 2, 2022, s. 233–247.

Brinnen, Martin *Allmänna dataskyddsförordningen (GDPR)*, Karnov, 11-04-2024 (JUNO), kommentaren till artikel 17.

Cederberg, Jesper, *Smer kritiskt till förslag om område för hälsodata i Europeiska unionen*, *Läkartidningen*, 11-12-2023.

Cederberg, Jesper, *Uppgifter till salu på darknet efter attacken mot Sophiahemmet*, *Läkartidningen*, 04-03-2024.

Chikwetu, Lucy, Miao, Yu, K. Woldetensae, Melat, Bell, Diarra, M. Goldenholz, Daniel, Dunn, Jessilyn (2023), *Does deidentification of data from wearable devices give us a false sense of security? A systematic review*, *Lancet Digit Health*, april 2023.

Correia, Mónica, Rego, Guilhermina, Nunes, Rui (2021), *The right to be forgotten and Covid-19: Privacy versus public interest*, *Acta Bioethica*, 2021.

Daniel, Groos och Evert-Ben, van Veen (2020), *Anonymised Data and the Rule of Law*, EDPL, 2020.

D. Wilkinson, Mark, Dumontier, Michel, Aalbersberg, Ijsabrand Jan, Appleton, Gabrielle, Axton, Myles, Baak, Arie et al. (2016), *The FAIR Guiding Principles for scientific data management and stewardship*, *Scientific Data*, 15 mars 2016.

EU-kommissionen (2021), *Assessment of the EU Member States' rules on health data in the light of GDPR*, DG Health and Food Safety, 2021.

EU-kommissionen (2018), *Ethics and data protection*, 14 november 2018.

Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline, Beyer, Sandra (2018), *GDPR – juridik, organisation och säkerhet enligt dataskyddsförordningen* (2018, JUNO).

Gorska, Carrara, Anna, Joanna Davis, Elena, Bonten, Ruth, W.Friedrich, Marc Alex et al. (2022), *Challenges of data sharing in European Covid-19 projects: A learning opportunity for advancing pandemic preparedness and response*, The Lancet, 4 augusti 2022.

Hettne, Jörgen och Otken-Eriksson, Ida (2011), (red.): *EU-rättslig metod: Teori och genomslag i svensk rättstillämpning*, 2 uppl., Nordstedts Juridik, Stockholm, 2011.

*Hundratusen i protest mot delad patientdata i EU*, Dagens Nyheter, 13-09-2023.

Karlsson Alverhill, Rikard (2023), *Dataskyddsförordningen (GDPR) för offentlig sektor – en introduktion*, 03-01-2023.

Kjellman, Hanna & Värmon, Didrik (2022), *GDPR-guiden – Handbok för verkligheten*, JUNO, Norstedts Juridik, 22-12-2022.

Kleineman, Jan (2018), *Rättsdogmatisk metod i: Nääv, Maria och Zamboni, Mauro (red.), Juridisk metodlära*, 2. uppl., Studentlitteratur, Lund, 2018.

Kocharyan, Hovsep, Vardanyan, Lusine, Hamulák, Ondrej, Kerikmäe, Tanel (2022), *Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy?*, International and comparative law review, 29 mars 2022.

Krzysztofek, Mariusz (2021), *GDPR: Personal Data Protection in the European Union*, 07-04-2021.

Nakayama, Luis F., de Matos, Joao Carlos Ramos Goncalves, U. Stewart, Isabelle et al. (2023), *Retinal scans and data sharing: the privacy and scientific development equilibrium*. Mayo clinic proceedings, Digital Health, mars, 2023.

Nissenbaum, Helena (2009), *Privacy in context Technology, Policy, and the Integrity of Social Life*, Stanford university press, 24 november 2009.

Nordberg, Anna (2020), *Big Data, e-health and the right to be forgotten*, i: Anne Kjersti Befring & Inger-Johanne Sand (red), *Kunstig. Intelligens og big data I helsesektoren: Reettslige perspektiver*, Gyldendal, 2020.

- Ploem M. C., Essink-Bot M. L., Stronks K (2013), *Proposed EU data protection regulation is a threat to medical research*, British Medical Journal, Nr. 346, 2013.
- Reichel, Jane (2018), *EU-rättslig metod* i: Nääv, Maria & Zamboni, Mauro (red.), *Juridisk metodlära*, 2. uppl., Studentlitteratur, Lund, 2018.
- Rumbold, John Mark Michael & Pierscionek, Barbara (2017), *The Effect of the General Data Protection Regulation on Medical Research*, Journal of Medical Internet Research, Nr. 19(2), 2017.
- Sartor, Giovanni (2015), *The right to be forgotten in the Draft Data Protection Regulation*, International data privacy law, 2015, Vol. 5, No. 1, 13 december 2014.
- Slokenberga, Santa, Reichel, Jane, Tzortzatou, Olga (2021), *GDPR and biobanking – Individual rights, public interest and research regulation across Europe*, Springer International Publishing, 05-01-2021, E-Bok.
- Statens medicinsk-etiska råd (Smer), *Kort om hälsodata*, december 2022, (Smer 2022:4).
- Tehdas (2022), *Report on secondary use of health data through European case studies*, 28 februari 2022.
- Trysell, Katrin, *Brist på hälsodata pekas ut som hinder för precisionsmedicin*, Läkartidningen, 2023-11-17.
- TT, *Staten brister i att skydds personuppgifter*, Dagens medicin, 18-04-2024.
- Vrabec, Helena U. (2021), *Data Subject Rights under the GDPR*, Oxford University press, Oxford, 13-05-2021.
- Wendel, Lotta, & Mattsson, Titti (2022), *Informationshantering och integritetsskydd inom hälso- och sjukvården*, i: Zillén, Kavot, Mattsson, Titti och Slokenberga, Santa (red.), *Medicinsk rätt*, 2. uppl., Norstedts Juridik, Stockholm, 2022.
- Wendleby, Monika (2021), *GDPR: Hantera registrerades rättigheter*, 2021-01-21.
- Wendleby, Monika & Wetterberg, Dag (2019), *Dataskyddsförordningen GDPR: förstå och tillämpa i praktiken*, 2019-09-23.

Westin, Alan F. (2015), *Privacy and freedom*, Ig publishing, 1 november 2015.

Öman, Sören (2023) *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, (27 sept 2023, JUNO).

## Övrigt

Connecting European international cohorts to increase common and effective response to SARS-CoV2 Pandemic (ORCHESTRA)

<https://orchestra-cohort.eu/>

(hämtad 28-03-2024)

EDPB, *EDPB:s ordförandeskap*.

[https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board\\_sv](https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_sv)

(hämtad 18-04-2024)

EDPB, *Föregångare: Artikel 29-arbetsgruppen*.

[https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party\\_sv](https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_sv)

(hämtad 18-04-2024)

EU-kommissionen, *Commission welcomes political agreement on European Health Data Space*, pressmeddelande, Bryssel, 15 mars 2024.

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_1346](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1346)

(hämtad 15-04-2024)

EU-kommissionen, *European cancer information system (ECIS)*.

<https://ecis.jrc.ec.europa.eu/>

(hämtad 30-03-2024)

EU-kommissionen, *European Health Union: A European Health Data Space for people and science*, pressmeddelande, Bryssel, 3 maj 2022.

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_2711](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711)

(hämtad 30-03-2024)

EU-kommissionen, *European platform on rare disease registration (EU RD platform)*.

[https://eu-rd-platform.jrc.ec.europa.eu/\\_en](https://eu-rd-platform.jrc.ec.europa.eu/_en)

(hämtad 30-03-2024)



EU-kommissionen, *Personalised medicine*.

[https://research-and-innovation.ec.europa.eu/research-area/health/personalised-medicine\\_en](https://research-and-innovation.ec.europa.eu/research-area/health/personalised-medicine_en)

(hämtad 30-03-2024)

EU-kommissionen, *Remarks by Vice-President Margaritis Schinas at the press conference on the European Health Data Space*, Strasbourg, 3 maj 2022.

[https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_22\\_2788](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_2788)

(hämtad 19-03-2024)

EU-kommissionen, *Vad betyder "grundat på berättigat intresse"?*

[https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean\\_sv](https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_sv)

(hämtad 15-04-2024)

EU-parlamentet, *EU Health Data Space: more efficient treatments and life-saving research*, pressmeddelande, 24 april 2024.

<https://www.europarl.europa.eu/news/sv/press-room/20240419IPR20573/eu-health-data-space-more-efficient-treatments-and-life-saving-research>

(hämtad 26-04-2024)

EU-parlamentet, *EU Health Data Space to support patients and research*, pressmeddelande, 15 mars 2024.

<https://www.europarl.europa.eu/news/en/press-room/20240304IPR18765/eu-health-data-space-to-support-patients-and-research>

(hämtad 18-04-2024)

Europeiska rådet, *Det europeiska hälsodataområdet: rådet och parlamentet överens*, pressmeddelande, 15 mars 2024.

<https://www.consilium.europa.eu/sv/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/>

(hämtad 18-04-2024)

Finnish Social and Health Data Permit Authority Findata (Findata)

<https://findata.fi/en/>

(hämtad 15-04-2024)

Health Data Hub

<https://www.health-data-hub.fr/>

(hämtad 15-04-2024)

Patrick Breyer, *European Health Data Space (EHDS): Patients risk losing control over their data*, 8 mars 2024.

<https://www.patrick-breyer.de/en/european-health-data-space-ehds-patients-risk-losing-control-over-their-data/>

(hämtad 15-04-2024)

Reconciliation of Cohort data in Infectious Diseases (ReCoDID)

<https://recodid.eu/>

(hämtad 28-03-2024)

Statens medicinsketiska råd (Smer), Några medicinsk-etiska begrepp, *Integritet*.

<https://smer.se/etik/nagra-medicinsk-etiska-begrepp>

(hämtad 29-04-2024)

SYnergies for Cohorts in Health: integrating the ROle of all Stakeholders. (SYNCHROS).

<https://synchros.eu/>

(hämtad 28-03-2024)

Tehdas, *Results*.

<https://tehdas.eu/results/>

(hämtad 28-03-2024)

The Danish Health Data Authority

<https://sundhedsdatastyrelsen.dk/da>

(hämtad 15-04-2024)

Unravelling Data for Rapid Evidence-Based Response to COVID-19 (unCoVer)

<https://uncover-eu.net/>

(hämtad 28-03-2024)

World health organization (WHO), *Meeting on secondary use of health data*, 13 december 2022.

<https://www.who.int/europe/news-room/events/item/2022/12/13/default-calendar/meeting-on-secondary-use-of-health-data>.

(hämtad 15-04-2024)

World Health Organization (WHO), *Occupational health*.

<https://www.who.int/health-topics/occupational-health>

(hämtad 30-03-2024)

# Rättsfallsförteckning

## EU-domstolen

Dom av den 11 december 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064.

Domstolens dom av den 14 februari 2019, *Buivids*, C-345/17, EU:C:2019:122.

Dom av den 24 september 2019, *Commission nationale de l'informatique et des libertés (CNIL) v. Google LLC*, EU:C:2019:773.

Dom av den 12 juli 2012, *Compass-Datenbank*, C-138/11, EU:C:2012:449.

Domstolens dom av den 13 maj 2014, *Google Spain SL, Google Inc. v. Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317.

Domstolens dom av den 22 juni 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504.

Domstolen dom av den 6 november 2003, *Lindqvist*, C-101/01, EU:C:2003:596.

Domstolens dom av den 4 juli 2023, *Meta Platforms m.fl.*, C-252/21, EU:C:2023:537.

Domstolens dom av den 6 mars 2001, *P. Connolly mot Kommissionen*, C-274/99, EU:C:2001:127.

Dom av den 9 mars 2017, *Salvatore Manni*, C-398/15, EU:C:2017:197.

Domstolens dom den 20 maj 2003, *Österreichischer Rundfunk m.fl.*, I de förenade målen C-465/00, C-138/01 och C-139/01, EU C:2003:294.