Federerade analyser

Utkast Rättsliga överväganden

Rapport från Läkemedelsverket

Datum:2020-05-06
Dnr: 4.3.1-2020-017988

LÄKEMEDELSVERKET
SWEDISH MEDICAL PRODUCTS AGENCY

Förord

För att kunna studera misstankar om ovanliga biverkningar av läkemedel är det viktigt att ha tillgång till ett så stort antal exponerade individer som möjligt. Det är ofta svårt att utföra sådana studier på grund av att antalet individer som exponerats för läkemedlet och antalet händelser som studeras är litet. En lösning på problemet är att samla information om ett så stort antal exponerade individer som möjligt. Det är därför viktigt att kunna kombinera information från flera datakällor och flera länder för att få ett tillräckligt underlag för analysen.

Läkemedelsverket vill med den här rapporten beskriva och lyfta fram de rättsliga överväganden som uppkommer i förhållande till behandlingar av personuppgifter vid registerforskning med federerad analys. Federerad analys är metoder som gör det möjligt att åstadkomma statistiska analyser på flera olika datakällor med identiskt strukturerade individdata, utan att behöva fysiskt sammanföra individdata.

För att kunna ta ställning till användningen av federerad analys är det nödvändigt att förhålla sig till hur personuppgifter inom projektet behandlas. Skyddet för personuppgifter inom EU är långtgående och regleras på EU-nivå i och med dataskyddsförordningen och det finns krav på att minst en part tar ansvar för hur personuppgifter behandlas. Det personuppgiftsansvaret kan se olika ut beroende på hur ansvaret fördelas inom forskningsprojektet.

Projektet om federerade analyser har varit en del i Läkemedelsverkets särskilda uppdrag från regeringen att utveckla strukturerad uppföljning av läkemedel. Projektet består av flera delprojekt. Denna rapport fokuserar på de juridiska förutsättningarna för federerad analys utifrån behandling av personuppgifter. Andra delprojekt fokuserar på begränsningar och möjligheter avseende statistiska metoder, datortekniska aspekter och informationshantering samt verktyg för validering av implementering.

Rapporten har utformats av Läkemedelsverkets rättsenhet. Under arbetet med rapporten har även Karolinska institutets rättsenhet, Sveriges kommuner och regioners stödfunktion för nationella kvalitetsregister samt forskare vid Umeå universitet konsulterats.

Citera gärna Läkemedelsverkets rapporter, men kom ihåg att uppge källa:
Läkemedelsverket, rapportens namn och år.

Läkemedelsverket, december 2020
Diarienummer: xxxx
Postadress: Box 26, 751 03 Uppsala
Besöksadress: Dag Hammarskjölds väg 42, Uppsala
Telefon: 018-17 46 00
www.lakemedelsverket.se

Sammanfattning

Federerad analys är metoder som gör det möjligt att åstadkomma statistiska analyser på flera olika datakällor med identiskt strukturerade individdata, utan att behöva fysiskt sammanföra individdata. Tekniken ger ändå samma resultat som om individdata fysiskt hade slagits ihop till en enda datamängd.

Läkemedelsverket vill med den här delrapporten belysa några rättsliga frågeställningar som bör beaktas vid forskning som inbegriper federerade analyser. Rapporten tar i huvudsak upp frågeställningar med koppling till behandling av personuppgifter vid federerad analys och EU:s dataskyddsförordning. Rapporten har avgränsats till behandlingar som sker inom EU/EES. Målsättningen är att rapporten ska kunna fungera som underlag för jurister men även för intressenter utan expertkunskap inom juridik.

Principen för federerad analys är att själva analysen flyttar till platsen med data istället för att data samlas på platsen för analys. Det innebär att beräkningsfrågor skickas från en central analysdator till noder där data finns. Statistiska beräkningar utförs autonomt på varje nod och sedan returneras endast resultatet av beräkningen tillsammans med metadata som behövs för att sammanställa resultat från flera noder.

När federerad analys används för att analysera data inom forskning utför forskningshuvudmannen vid varje nod flera specifika behandlingar av personuppgifter i processtegen innan själva analysen. Den statistiska analysen som sker lokalt i noden är en behandling av personuppgifter. Den data som respektive nod levererar till den centrala analysdatorn är inte att betrakta som en behandling av personuppgifter, förutsatt att leveransen består av aggregerad data eller statistiska beräkningar.

Dataskyddsförordningen kräver att det finns minst en personuppgiftsansvarig för behandling av personuppgifter inom forskningsprojekt. Personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Ansvaret för personuppgifterna utgår från varje behandling av personuppgifter, det innebär att det kan finnas flera personuppgiftsansvariga för olika behandlingar inom ett och samma projekt.

Vid registerforskning med federerade analyser kan ansvaret för en behandling av personuppgifter helt eller delvis komma att flyttas mellan forskningshuvudmän utan att det sker någon överföring av personuppgifterna i fråga. Det är därför lämpligt att tidigt i forskningsprojektets planeringsfas fastställa om det rör sig om ett eller flera forskningsprojekt och fastställa ansvarsfördelning och roller. Avtal och överenskommelser bör vara skriftliga och reglera ansvar och roller samt ansvarsskyldighet för underlåtenhet att efterleva avtalet.

Rapporten presenterar tre olika modeller för hur personuppgiftsansvaret kan fördelas i ett forskningsprojekt med federerad analys. Det finns vissa skillnader mellan hur ansvaret fördelas mellan de tre olika modellerna som presenteras. Det är därför viktigt att beslutsfattare, forskare, tekniker, jurister och andra nyckelroller med koppling till ett forskningsprojekt är tillräckligt insatta i såväl hur en federerad analys går till som tillämpliga delar av dataskyddsregelverket och hur ansvaret flyttas och fördelas i det aktuella forskningsprojektet.

Projektet om federerade analyser består av flera delprojekt. Denna rapport fokuserar på de juridiska förutsättningarna för federerad analys utifrån behandling av personuppgifter. Andra delprojekt fokuserar på begränsningar och möjligheter avseende statistiska metoder, datortekniska aspekter och informationshantering samt verktyg för validering av implementering. Varje rapport ska kunna fungera som underlag för diskussioner mellan IT-experter, jurister, statistiker och forskare. Målet är att rapporterna tillsammans ska kunna underlätta för informationsägare att kunna fatta beslut om användande av federerade analyser.

Innehållsförteckning

1. Uppdraget

1.1 Bakgrund

För att Läkemedelsverket ska kunna identifiera och karaktärisera möjliga säkerhetsproblem med läkemedel används olika register för att göra epidemiologiska studier. När det handlar om läkemedel som ännu inte använts av så många individer eller det är ovanliga biverkningar man vill studera är det ofta nödvändigt att kombinera information från flera datakällor för att få ett tillräckligt underlag för analysen. Att slå samman olika datakällor är ofta en tidsödande och komplicerad process av både praktiska och juridiska skäl, inte minst när det gäller internationella samarbeten där data finns i olika länder. Ett alternativ är då att använda analysmetoder som bygger på federerad analys.

Federerad analys innebär i korthet att analysen flyttar till platsen med data istället för att data samlas på platsen för analys. Beräkningsfrågor skickas från en central analysdator till noder där data finns och sedan returneras resultatet av beräkningen tillsammans med metadata som behövs för att sammanställa resultat från flera noder.

Användandet av federerade analyser aktualiserar en rad juridiska frågor avseende skyddet för personuppgifter, särskilt om datakällorna finns i olika länder. Vilka behandlingar av personuppgifter sker? Vem är att anse som ansvarig för behandlingen av personuppgifterna? Hur ska ansvaret regleras? Påverkas denna ansvarsreglering av att det territoriella tillämpningsområdet för bestämmelser om etikprövning är nationellt medan dataskyddsregleringen är internationell?

1.2 Syfte och avgränsning

Denna delrapport syftar till att belysa vilka juridiska frågor som uppkommer i förhållande till behandling av personuppgifter vid federerad analys. Rapporten avgränsas till att omfatta personuppgifter som behandlas vid federerad analys och där behandlingen sker inom EU/EES. Målsättningen är att rapporten ska kunna fungera som underlag för jurister men även för intressenter utan expertkunskap inom juridik.

Rapporten är en del i Läkemedelsverkets särskilda uppdrag från regeringen att utveckla strukturerad uppföljning av läkemedel. Projektet om federerade analyser består av flera delprojekt. Rapporten avses kunna läsas självständigt eller tillsammans med de andra delprojekten som fokuserat på IT-arkitektur ”Federerade analyser – IT-arkitektur”, hjälpmedel för implementering och utvärdering av denna, ”Tutorial: Analysing simulated federated data with GLM using DataSHIELD” och möjligheter och begränsningar avseende statistiska metoder ”Statistical methods in federated analyses”.

2. Skydd för personuppgifter inom EU/EES

2.1 EU:s dataskyddsförordning

För att skydda den enskildes privatliv finns det EU-gemensamma regler om hur personuppgifter får behandlas. Dataskyddsförordningen, ofta förkortad GDPR [1], som tillämpas från och med den 25 maj 2018 är den primära rättsliga regleringen vid behandling av personuppgifter. Det innebar att tidigare gällande lagar inom skydd för personuppgifter, personuppgiftslagen[2] (PUL) och personuppgifts-

[1]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.
[2] Personuppgiftslagen (1998:204).

förordningen[3], slutade gälla och istället ersattes av dataskyddsförordningen och dess kompletterande bestämmelser i dataskyddslagen[4].

Dataskyddsförordningen är direkt tillämplig i varje medlemsland i EU. Syftet med dataskydds-förordningen är att skapa lika förutsättningar för skydd för personuppgifter i hela EU. Att dataskyddsförordningen är primär betyder att när personuppgifter behandlas måste i första hand dataskyddsförordningens bestämmelser om skydd för den personliga integriteten beaktas och därefter (med avseende på personuppgiftsbehandlingen) kompletterande nationell lagstiftning följas.

Dataskyddsförordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Från dataskyddsförordningens tillämpningsområde undantas behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som utförs av medlemsstaterna när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken.[5] Dataskyddsförordningen ska tillämpas på all behandling av personuppgifter som sker inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte.

Dataskyddsförordningen anger i artikel 5 ett antal grundläggande principer för behandling av personuppgifter, som alla som omfattas av förordningen och som hanterar personuppgifter måste följa. Principerna rör krav på laglighet, öppenhet, ändamålsbegränsning, korrekthet, uppgiftsminimering och lagringsminimering.[6]

En av de grundläggande principerna rör kravet på säkerhet och innebär att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av lämpliga tekniska eller organisatoriska åtgärder. Lämplig säkerhet ska säkerställa exempelvis skydd mot obehörig eller otillåten behandling, förlust, förstöring eller skada genom olyckshändelse.[7]

Även den personuppgiftsansvariges ansvar tydliggörs i dataskyddsförordningen. Den så kallade ansvarsskyldigheten innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna efterlevs.[8] Kravet avser dels att säkerställa att behandlingen av personuppgifterna utförs i enlighet med dataskyddsförordningen, dels att den personuppgiftsansvarige ska kunna visa att behandlingen av personuppgifterna utförs i enlighet med förordningen.

Vissa bestämmelser i dataskyddsförordningen berör särskilt förutsättningarna för att behandla personuppgifter för bl.a. vetenskapliga eller historiska forskningsändamål. I skäl 159 anges att behandling av personuppgifter för vetenskapliga forskningsändamål i förordningen bör ges en vid tolkning och omfatta till exempel teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. Vetenskapligt forskningsändamål bör också omfatta studier som utförs av ett allmänt intresse inom folkhälsoområdet. Bestämmelser om behandling av personuppgifter för forskningsändamål finns bl.a. i artikel 5 som innehåller principer för behandling av personuppgifter, artikel 6 som anger när behandling av personuppgifter är laglig, artikel 9 med reglering av behandling av särskilda kategorier av personuppgifter, artikel 12–20 om den registrerades rättigheter och artikel 89 med särskilda bestämmelser för behandling av personuppgifter för bl.a. vetenskapliga eller historiska forskningsändamål.

[3] Personuppgiftsförordningen (1998:1191).
[4] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[5] SOU 2017:39 s 74.
[6] Artikel 5.1 dataskyddsförordningen.
[7] Artikel 5.1 f dataskyddsförordningen.
[8] Artikel 5.2 dataskyddsförordningen.

2.2 Vad är en personuppgift

En personuppgift är varje uppgift som kan knytas till en levande person. Uppgifter som rör personer som är avlidna eller ännu inte är födda anses inte vara personuppgifter. Inte heller uppgifter som rör juridiska personer är personuppgifter. Uppgifterna kan vara direkt eller indirekt kopplade till en fysisk person. Det avgörande är om personen på något sätt kan identifieras av någon annan.[9] Typiska uppgifter som är personuppgifter är namn, adress och personnummer, men även fotografier eller ljudupptagningar som lagras elektroniskt kan klassas som personuppgifter. Det är tillräckligt att det är möjligt att knyta uppgifterna till en specifik person, t.ex. vaktmästaren på Lummelundaskolan eller ett registreringsnummer till en bil som nyttjas av en person. Även uppgifter som är krypterade och olika slags elektroniska identiteter som t.ex. e-postadresser eller IP-adresser är personuppgifter om de kan knytas till en person.

Vissa personuppgifter är extra känsliga personuppgifter. Dessa återfinns i artikel 9 i dataskyddsförordningen samt i 3 kap. 1 § dataskyddslagen och omfattar uppgifter som rör ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa, uppgifter om en fysisk persons sexualliv och sexuell läggning (känsliga personuppgifter).

Personnummer och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men personnummer och samordningsnummer anses extra skyddsvärda och får enligt 3 kap. 10 § dataskyddslagen behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

2.3 Behandling av personuppgifter

Med begreppet behandling avses i dataskyddsförordningen en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter.[10] Detta gäller oavsett om behandlingen sker elektroniskt eller på annat sätt. Exempel på behandling av personuppgifter är att lagra, samla in, skriva ut, radera, använda eller lämna ut personuppgifter till någon annan.

Den första principen om behandling av personuppgifter inom dataskyddsförordningen är att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.[11] Principen om laglighet utgör en hänvisning till de rättsliga grunderna i artikel 6.1. Den europeiska dataskyddsregleringen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund. Behandling av personuppgifter får därför bara ske under de omständigheter som särskilt anges i lagstiftningen. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1.[12] Behandling är enligt denna bestämmelse endast laglig om och i den mån som åtminstone ett av följande villkor föreligger: samtycke (a), avtal (b), rättslig förpliktelse (c), vitala intressen (d), myndighetsutövning (e), uppgift av allmänt intresse (e), eller berättigat intresse (f).[13] Uppräkningen i artikel 6.1 är uttömmande. Om inget av dessa villkor är uppfyllda är behandlingen inte laglig och får därmed inte utföras. Den omständigheten att behandlingen är laglig enligt artikel 6.1 i dataskyddsförordningen, dvs. att den är rättsligt grundad, innebär inte att behandling kan ske av vilka uppgifter som helst eller på valfritt sätt. Den personuppgiftsansvarige måste även uppfylla kraven i övriga bestämmelser i förordningen.[14] När

[9] Se artikel 4 dataskyddsförordningen.
[10] Se artikel 4.2 dataskyddsförodningen. Den svenska ordalydelsen ”åtgärder beträffande personuppgifter” och den tyska ordalydelsen ”im Zusammenhang mit personenbezogenen Daten” har rent språkligt ett något vidare tillämpningsområde än den engelska ordalydelsen ”operation […] which is performed on personal data”.
[11] Artikel 5.1 dataskyddsförordningen.
[12] SOU 2017:39 s 103.
[13] För de specifika villkor som föreligger se artikel 6.1 dataskyddsförordningen.
[14] SOU 2017:39 s 103.

det gäller behandling som avser känsliga personuppgifter anges ytterligare villkor i artiklarna 9 och 10 i dataskyddsförordningen.

Det är förbjudet enligt dataskyddsförordningen att behandla känsliga personuppgifter, bland annat uppgifter om en persons hälsa.[15] Det finns dock ett antal undantag från förbudet. Förbudet ska t.ex. inte tillämpas om behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter. Det måste ske på grundval av unionsrätten eller medlemsstaternas nationella rätt samt att lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs. [16] Begreppet folkhälsa bör tolkas, enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008, så att det avser alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso-och sjukvård, utgifter för och finansiering av hälso-och sjukvården samt dödsorsaker.[17] Studier som utförs av ett allmänt intresse inom folkhälsoområdet bör därmed omfattas av begreppet forskningsändamål.[18]

2.4 Behandling av känsliga personuppgifter i forskning

Förbudet mot behandling av känsliga personuppgifter i artikel 9 i och j är inte tillämpligt för behandling som är nödvändig, bl.a. vetenskapliga eller historiska forskningsändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt. Detta förutsatt att behandlingen står i proportion till det eftersträvade syftet samt att behandlingen ska vara förenligt med skyddet för personuppgifter samt innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.[19] Regeringen gör i propositionen ”Behandling för personuppgifter för forskningsändamål” bedömningen att etikprövning är en lämplig och särskild åtgärd vid all behandling av känsliga personuppgifter för andra forskningsändamål än kliniska läkemedelsprövningar. Etisk granskning är alltså en sådan i svensk rätt fastställd lämplig och särskild åtgärd som krävs enligt EU:s dataskyddsförordning för behandling av känsliga personuppgifter för forskningsändamål.[20] Det har kodifierats i etikprövningslagen[21], där det framgår att för att få utöva forskning som bedrivs inom Sverige och som innefattar behandling av känsliga personuppgifter krävs godkännande genom etikprövning.[22] Även tystnadsplikt erfordras vilket framgår direkt av dataskyddsförordningen.[23]

För ett forskningsprojekt som omfattar forskning även utanför Sverige prövas endast den del av forskningen som utförs inom Sverige, även om ansökan bedöms mot bakgrund i hela projektet. Det innebär att den forskning som i andra länder än Sverige måste prövas etiskt enligt respektive lands lag, medan hanteringen av personuppgifterna ska göras i enlighet med dataskyddsförordningen. Det kommer av att dataskyddsförordningen är direkt tillämplig och gäller i hela EU, medan etikprövningslagen endast har nationell tillämpning. Här kan det vara så att det andra landet har valt en annan form av extra skydd för att nå upp till dataskyddsförordningen än etikprövning. Det är därför viktigt att forsknings-huvudmännen i respektive land ser till att uppfylla kraven i dataskyddsförordningen vad det gäller att behandla känsliga personuppgifter i enlighet med dataskyddsförordningen. Om man tar ett samarbete mellan Danmark och Sverige som ett exempel måste det inom ett sådant samarbete regleras hur personuppgiftsansvaret ska fördelas inom projektet utifrån dataskyddsförordningen medan respektive

[15] Se artikel 9.1 i dataskyddsförordningen.
[16] Se artikel 9.2 i dataskyddsförordningen.
[17] Se skäl 54 i dataskyddsförordningen.
[18] Se skäl 159 dataskyddsförordningen samt prop. 2017/18:298 s 29.
[19] Prop. 2017/18:298 s 86f.
[20] Prop. 2017/18:298 s 95.
[21] Lagen (2003:460) om etikprövning av forskning som avser människor (etikprövningslagen).
[22] Se 3, 5, 6 §§ etikprövningslagen.
[23] Se artikel 9.1 i dataskyddsförordningen.

lands forskningshuvudman måste ansöka om etikgodkännande för sin del av projektet enligt sitt lands etikprövningslag.[24]

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 b–f måste den vara nödvändig för att fullgöra, skydda eller utföra den rättsliga grunden. Att en behandling är nödvändig innebär inte att den måste vara absolut nödvändig i ordets språkliga betydelse utan det är tillräckligt att användandet av personuppgifterna t.ex. ger en betydande effektivitetsvinst.

2.5 Begreppen forskningshuvudman och personuppgiftsansvarig

Forskningshuvudman är den fysiska eller juridiska person i vars verksamhet forskningen *utförs*, till exempel lärosäte, kommun, region, myndighet eller privat företag. Det är forskningshuvudmannen som har det yttersta ansvaret för forskningen och är den som ska ansöka om etikprövning. Forskningshuvudmannen är ansvarig för att forskning som omfattas av etikprövningslagen inte utförs utan godkännande.[25] . Samtidigt tar detta ansvar inte ifrån den enskilda forskaren hans eller hennes personliga ansvar för att utföra forskning i enlighet med etikprövningslagen. Både forskaren och forskningshuvudmannen har alltså ett ansvar för forskningens lagenlighet.[26]

Vid uppdragsforskning är det den som åtagit sig att i sin verksamhet utföra forskningen (uppdragstagaren) som är forskningshuvudman. Den som åtar sig att bedriva viss forskning för någon annans räkning kan alltså inte överlåta sitt ansvar som forskningshuvudman till beställaren (uppdragsgivaren).[27]

Etikprövningslagens geografiska tillämpningsområde är enligt 5 § forskning som ska utföras i Sverige. Om en svensk forskningshuvudman deltar i ett internationellt forskningsprojekt omfattar prövningen den del av projektet som ska utföras i Sverige. Bedömningen görs dock mot bakgrund av vad hela projektet avser.[28]

När flera forskningshuvudmän (inom Sverige) medverkar i ett och samma forskningsprojekt ska de gemensamt uppdra åt en av dem att ansöka om etikprövning av projektet för allas räkning och att informera de övriga om Etikprövningsmyndighetens beslut. En forskningshuvudman ansvarar för den del av projektet som utförs inom den egna verksamheten.[29]

Personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer *ändamålen* och *medlen* för behandlingen av personuppgifter.[30] Enligt dataskyddsförordningen gäller att om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt förordningen, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14 i förordningen, genom ett inbördes arrangemang. Detta gäller under förutsättning att de personuppgiftsansvarigas respektive skyldigheter inte fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för detta arrangemang får en gemensam kontaktpunkt för de personuppgiftsansvariga utses. Arrangemanget ska

[24] I Danmark prövas etikprövningsansökan av den danska myndigheten ”National videnskabsetisk komité” i enlighet med ” lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter nr. 593 af 14. juni 2011”. För en översikt av de nordiska ländernas nationella rätt för behandling av hälsodata för forskningsändmål se Nordforsk rapport, The Nordic Commons, bilaga 4.
[25] Se 2, 3 och 6 §§ etikprövningslagen.
[26] Se prop. 2018/19:165 s. 37.
[27] Se prop. 2002/03:50 s. 93 och s. 193.
[28] Se prop. 2002/03:50 s. 109.
[29] Se 23 § etikprövningslagen och prop. 2018/19:165 s 38 f.
[30] Se artikel 4.7 i dataskyddsförordningen.

på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot den registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade. Oavsett formerna för arrangemanget får den registrerade utöva sina rättigheter enligt förordningen med avseende på och emot var och en av de personuppgiftsansvariga.[31]

Enligt dataskyddsförordningen gäller vidare att varje personuppgiftsansvarig (eller personuppgiftsbiträde) som har medverkat vid en behandling kan hållas ansvarig för hela skadan, dvs det råder ett solidariskt ansvar för skadestånd när det finns flera personuppgiftsansvariga (eller personuppgiftsbiträden) som är ansvariga för samma behandling.[32]

När det gäller personuppgifter som behandlas i forskning är det i regel forskningshuvudmannen som bestämmer ändamålen och medlen för behandlingen av personuppgifter. Det är då forskningshuvudmannen som är personuppgiftsansvarig. Vid uppdragsforskning kan både beställaren (uppdragsgivaren) och uppdragstagaren vara ensamt eller gemensamt personuppgiftsansvarig, även om uppdragstagaren alltid är forskningshuvudman.[33]

2.6 Begreppen personuppgiftsbiträde och personuppgiftsbiträdesavtal

Ett personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.[34] Det är viktigt att personuppgiftsbiträdet endast utför personuppgiftsbehandling för den personuppgiftsansvariges räkning. Om denne går utöver sitt mandat eller får för stort inflytande över ändamål eller medel kan personuppgiftsbiträdet istället bli gemensamt personuppgiftsansvarig, se avsnitt 2.7 om gemensamt personuppgiftsansvar. Det är fakta som avgör ansvaret, det vill säga de faktiska förutsättningarna för vilken part som utövar bestämmanderätten över ändamål och medel, inte hur avtalet för ansvaret ser ut. En aktör som de facto har bestämmanderätt över ändamål och medel kan därför inte vara personuppgiftsbiträde. Det är därför viktigt att analysera externa parters roller och vilka risker det finns med att använda sig av personuppgiftsbiträden vid behandling av personuppgifter. [35,36]

Personuppgiftsansvarig och personuppgiftsbiträde är autonoma EU-rättsliga begrepp som ska tolkas huvudsakligen utifrån dataskyddsförordningen, även om andra rättsområden på både unionsnivå och nationell nivå kan hjälpa till att identifiera vem som är ansvarig för personuppgifterna. Det är således viktigt att inte blanda ihop begreppet personuppgiftsansvarig med koncept från andra områden inom juridiken som upphovsman eller rättighetsinnehavare av immateriella rättigheter eller konkurrensrätt.[37]

Om den personuppgiftsansvarige har utsett minst ett personuppgiftsbiträde ska detta regleras i ett avtal eller annan rättsakt.[38] Av artikel 28 framgår att avtalet ska vara bindande både för den personuppgiftsansvarige och personuppgiftsbiträdet. Av samma artikel framgår att personuppgiftsbiträdesavtalet ska

---

[31] Se artikel 26 i dataskyddsförordningen.
[32] Se skäl 146 och artikel 82 i dataskyddsförordningen.
[33] Se SOU 2017:104 s. 242, jämför prop. 2018/19:165 s. 39 och prop. 2002/03:50 s. 93.
[34] Se artikel 4.8 i dataskyddsförordningen
[35] GDPR juridik, organisation, säkerhet, D. Frydlinger, T. Edvardsson, C. Olstedt Carlström och S. Beyer, Norstedts juridik, 2018, s. 56f.
[36] Vid utredning av ansvar behöver de egentliga förhållandena analyseras på ett djupare plan än endast vad som framgår av avtal och andra dokument. Det handlar i hög grad om att avgöra vem som har sådan kontroll över en viss behandling att denna bör åläggas personuppgiftsansvar för att ge de registrerade fullgott skydd. Däremot ska man inte nödvändigtvis gå så långt att varje konsult är att anse som personuppgiftsbiträde. I det fall konsulten är en del av den personuppgiftsansvariges organisation och på andra sätt fungerar som en anställd så är konsulten att anse som del av den personuppgiftsansvarige.
[37] Europeiska dataskyddsstyrelsens vägledning, ”Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, version 1.0 a, antagen den 2 september 2020, s. 9.
[38] Se artikel 28.3 i dataskyddsförordningen.

vara skriftligt. Avtalet ska säkerställa att båda parter följer dataskyddsförordningen, att båda parter är medvetna om sina skyldigheter mot varandra och mot den registrerade, att båda parter skyddar de personuppgifter som behandlar tekniskt men även att de har konfidentialitet eller tystnadsplikt. Personuppgiftsbiträdesavtalet gör det även enklare för parterna att visa att de följer dataskydds-förordningen samt på vilket sätt ansvaret är fördelat.

Ett personuppgiftsavtal ska innehålla information om behandlingen av personuppgifter. Av avtalet ska det framgå: föremålet för behandlingen och dess varaktighet, behandlingens art och ändamål, vilka typer av personuppgifter och kategorier av registrerade som omfattas samt den personuppgiftsansvariges rättigheter och skyldigheter.[39] Det finns minimikrav för vad ett personuppgiftsbiträdesavtal ska innehålla vilket framgår av artikel 28.3 dataskyddsförordningen. Utöver minimikraven kan personuppgiftsansvarige och personuppgiftsbiträdet komplettera avtalet med mer utförliga avtalsvillkor. Normalt är personuppgiftsbiträdesavtalet indelat i två delar: allmänna bestämmelser och en mer detaljerad instruktion. Instruktionen läggs ofta av praktiska skäl i en bilaga då den normalt förändras oftare än den allmänna delen.[40]

Överenskommelsen eller avtalet ska dock inte endast återupprepa de villkor som ställs upp inom dataskyddsförordningen, utan det ska innehålla mer specifik och konkret information om hur villkoren ska uppnås och vilken nivå av säkerhet som krävs för behandlingen av personuppgifterna som omfattas av avtalet.[41] Den personuppgiftsansvarige har en skyldighet att endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller dataskyddsförordningens kraven och säkerställer att den registrerades rättigheter skyddas. .[42]

2.7 Begreppet gemensamt personuppgiftsansvar

Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamål och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt dataskyddsförordningen.[43]

Precis som med personuppgiftsbiträden är det de faktiska förhållandena som avgör om två eller fler parter är gemensamt personuppgiftsansvariga.[44] Varje part är ansvarig för att de följer dataskydds-förordningens regler och att de har rättslig grund för respektive behandling.[45]

Begreppet ”ansvarig” har en i sammanhanget förhållandevis vid definition där syftet är att säkerställa ett effektivt och komplett skydd för de berörda personerna. EU-domstolen har slagit fast att en fysisk eller juridisk person som för eget syfte *påverkar behandlingen av personuppgifter*, och därigenom bidrar till att bestämma ändamål och medel för behandlingen, kan anses vara ansvarig.[46] För att flera aktörer

[39] Se artikel 28.3 i dataskyddsförordningen och https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/personuppgiftsansvariga-och-personuppgiftsbitraden/personuppgiftsbitradesavtal/ (2020-10-08).
[40] GDPR juridik, organisation, säkerhet, D. Frydlinger, T. Edvardsson, C. Olstedt Carlström och S. Beyer, Norstedts juridik, 2018, s. 305.
[41] Europeiska dataskyddsstyrelsens vägledning, ”Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, version 1.0 a, antagen den 2 september 2020, s. 4.
[42] Se artikel 28.1 i dataskyddsförordningen.
[43] Se artikel 26.1 i dataskyddsförordningen.
[44] GDPR juridik, organisation, säkerhet, D. Frydlinger, T. Edvardsson, C. Olstedt Carlström och S. Beyer, Norstedts juridik, 2018, s. 55.
[45] Europeiska dataskyddsstyrelsens vägledning, ”Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, version 1.0 a, antagen den 2 september 2020, s. 4.
[46] Se EU-domstolens dom av den 10 juli 2018, Jehovan todistajat, C-25/17, ECLI: EU:C:2018:551, punkt 68.

ska anses ha ett gemensamt ansvar för samma behandling krävs inte att var och en av dessa har *tillgång* till de aktuella personuppgifterna.

En aktör kan välja att för sina egna ändamål använda ett verktyg eller ett system som utvecklats eller tillhandahålls av en annan aktör. Om den ena aktörens beslut att använda verktyget medför en behandling av personuppgifter hos den andra aktören som inte annars skulle vara möjlig, kan detta val medföra att aktörerna ska anses gemensamt bestämma över *medlen* för behandlingen.[47]

Vad gäller ändamålen för behandlingen av personuppgifter är det lämpligt att analysera aktörernas samtliga individuella och gemensamma intressen kopplade till genomförandet av en behandling. Gynnar en behandling gemensamma ekonomiska eller vetenskapliga intressen kan det medföra att aktörerna anses gemensamt bestämma över ändamålen med behandlingen, även om aktörerna har egna specifika syften i tidigare eller senare led. [48]

Det gemensamma ansvaret avgränsas till de behandlingar aktörerna faktiskt bestämmer ändamålen och medlen för tillsammans. En aktör ska således inte anses vara ansvarig för tidigare eller senare åtgärder i den övergripande behandlingskedjan.

Det är viktigt att fastställa vem eller vilka parter som är personuppgiftsansvariga och på vilket sätt enligt dataskyddsförordningen. Det finns inte något formkrav för hur ansvaret ska fördelas, men det är att rekommendera att göra detta skriftligen samt att respektive parter är väl insatta i överenskommelsen.[49] Om gemensamt personuppgiftsansvar föreligger ska de gemensamt personuppgiftsansvariga fastställa sitt respektive ansvar för att uppfylla förordningens regler. Detta särskilt med hänsyn till de registrerades rättigheter till insyn och information.[50]

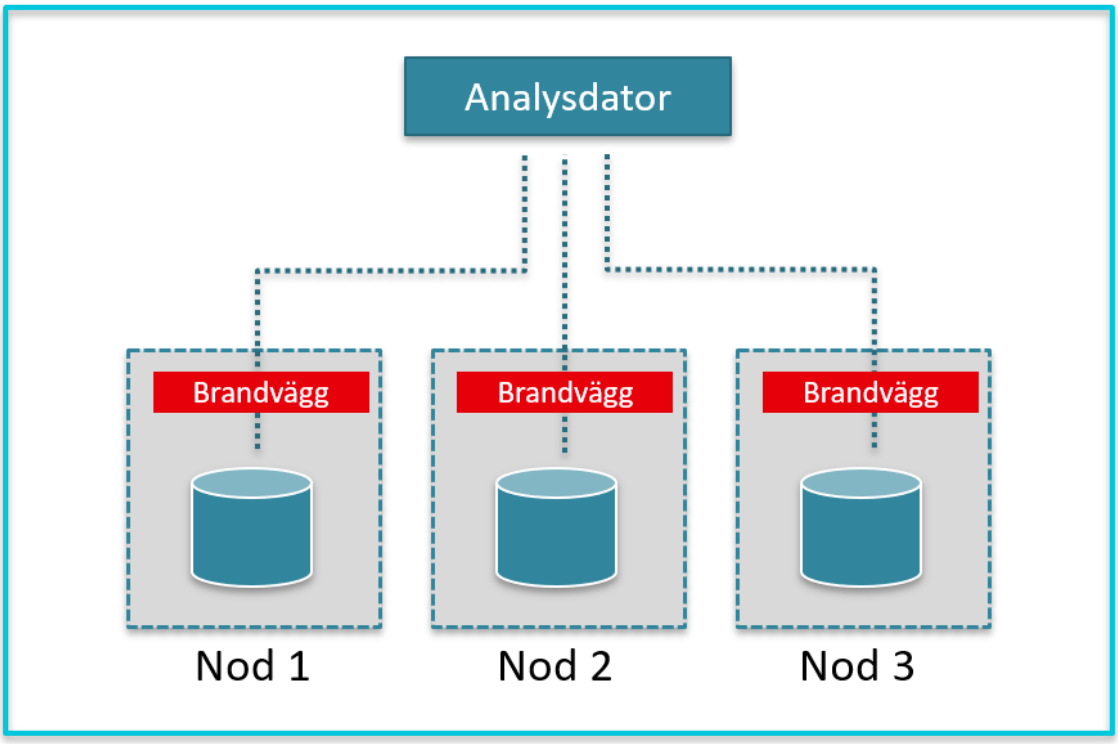
Fastställandet av ansvar ska enligt dataskyddsförordningen ske under öppna former genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.[51] Vad som avses med öppna former (”*a transparent manner*”) är inte fastställt i förordningen eller i praxis. Kravet på transparens torde innebära att det ska vara möjligt för de registrerade att ta del av fördelningen av skyldigheter som finns i arrangemanget.[52] Det kan göras genom att t.ex. publicera ansvarsfördelningen på en publik hemsida eller genom att upplysningar ges i samband med att information enligt artikel 13 eller 14 lämnas till de registrerade.[53] För exempel på vad som bör ingå i ett avtal för gemensamt personuppgiftsansvariga se bilaga 1 – Gemensamt personuppgiftsansvar.

[47] EU-domstolens dom av den 29 juli 2019, Fashion ID, C-40/17, ECLI:EU:2018:1039, punkterna 77-79.
[48] Jämför EU-domstolens dom Fashon ID, punkterna 80-81.
[49] Dataskyddsförordningen (GDPR) m.m. En kommentar, Sören Öman, Gula biblioteket, Norstedts juridik, 2019, s. 387.
[50] Se artikel 13 och 14 i dataskyddsförordningen samt GDPR juridik, organisation, säkerhet, D. Frydlinger, T. Edvardsson, C. Olstedt Carlström och S. Beyer, Norstedts juridik, 2018, s. 55.
[51] Se artikel 26.1 i dataskyddsfördordningen.
[52] Dataskyddsförordningen (GDPR) m.m. En kommentar, Sören Öman, Gula biblioteket, Norstedts juridik, 2019, s. 387.
[53] Se artikel 26.2 i dataskyddsförordningen samt Dataskyddsförordningen (GDPR) m.m. En kommentar, Sören Öman, Gula biblioteket, Norstedts juridik, 2019, s. 387.

3. Federerad analys

3.1 Vad är federerad analys?

Federerad analys innebär att analysen flyttar till platsen med data istället för att data samlas på platsen för analys. Det innebär att beräkningsfrågor skickas från analysdatorn till noder där den data som ska analyseras finns. Beräkningen utförs på varje nod och sedan returneras endast resultatet av beräkningen tillsammans med metadata som behövs för att sammanställa resultatet från flera noder (exempelvis antalet individer som legat till grund för en viss beräkning). För mer utförlig beskrivning av tekniken bakom federerad analys se delrapporten om IT-arkitekuren för federerade analyser – ”Federerade analyser – IT-arkitektur”.



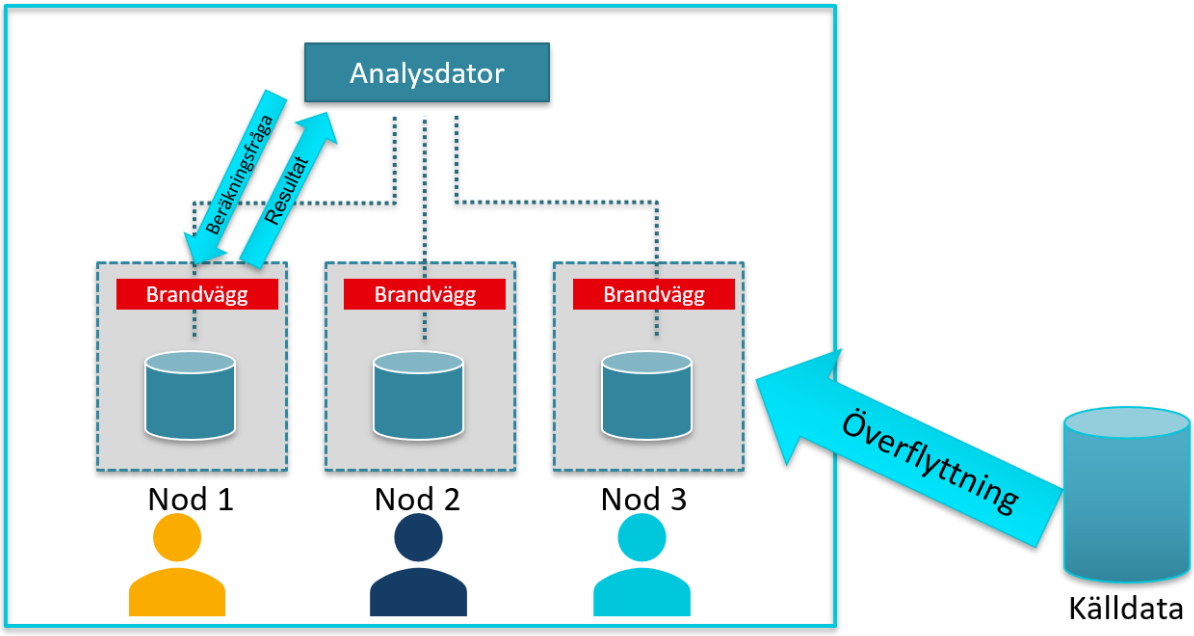
Figur 1
IT-arkitektur för federerad analys

3.2 Vilka specifika behandlingar av personuppgifter sker vid federerad analys?

Som anförts ovan avses med behandling en åtgärd eller kombination av åtgärder beträffande personuppgifter. Varje nod utför flera specifika behandlingar i processtegen innan själva analysen (beräkningarna), t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning och ändring.

Den beräkningsfråga som skickas från analysdatorn till noden utgör i sig inte en personuppgifts-behandling utan utgör instruktioner för en behandling. Den statistiska analysen som sker lokalt i nodens är en behandling (användning) av personuppgifter. Den data som respektive nod levererar till den centrala analysdatorn (resultatet) är inte heller att betrakta som en behandling av persondata, förutsatt att leveransen består av aggregerad data eller statistiska beräkningar (summor, antal, medelvärden, min,

max). Bedöms dessa tre åtgärder tillsammans som en kombination av åtgärder torde de anses utgöra behandling av personuppgifter.



Figur 2
Åtgärder i samband med federerad analys

3.3 Ansvar för personuppgifter vid federerad analys i forskning

Det ska, enligt dataskyddsförordningen, finnas en eller flera personuppgiftsansvariga för behandlingar av personuppgifter. Den personuppgiftsansvarige är den som bestämmer varför och hur personuppgifter ska behandlas, se avsnitt 2.5. för mer information om begreppet personuppgiftsansvarig. Det finns inte något krav i dataskyddsförordningen att det ska vara endast en person som är personuppgiftsansvarig.

Vid traditionell insamling av data vid registerforskning är det normalt forskningshuvudmannen som bestämmer ändamålen och medlen för behandlingen av personuppgifter i sin verksamhet. Vid federerad analys kan ansvaret se olika ut beroende på val av samarbetsform, men även vilken form av studie som ska företas. Eftersom ansvaret utgår från de faktiska förhållandena kring varje åtgärd eller kombination av åtgärder beträffande personuppgifter innebär det att det i ett forskningsprojekt kan finnas flera personuppgiftsansvariga för personuppgiftsbehandlingar både *inom* och *i anslutning till* en federerad analys.

Figur 3
Förenklad process av personuppgiftsbehandlingar i anslutning till federerad analys. Vilken eller vilka av forskningshuvudmännen som ansvarar för respektive processteg beror på det faktiska upplägget av ett forskningsprojekt.

Nedan presenteras tre modeller för fördelning av personuppgiftsansvar i ett forskningsprojekt där federerade analyser används. Modellerna illustrerar det inflytande en eller flera forskningshuvudmän har över åtgärder i den centrala analysdatorn och i noderna. Modellerna utgår ifrån antagandet att åtgärderna som beskrivs är att anse som personuppgiftsbehandlingar, ingår i ett led av åtgärder som tillsammans är att anse som behandlingar eller i vart fall har en stark koppling till sådana behandlingar att de ingår i det ansvar som regleras i dataskyddslagstiftningen (t.ex. säkerhetsåtgärder eller tekniska åtgärder som konfigurering av ett system eller av en systemkomponent).

De tre modellerna är:

Modell 1 - personuppgiftsbiträdesavtal,

Modell 2 - ensamt övergripande ansvar, samt

Modell 3 - gemensamt övergripande ansvar.

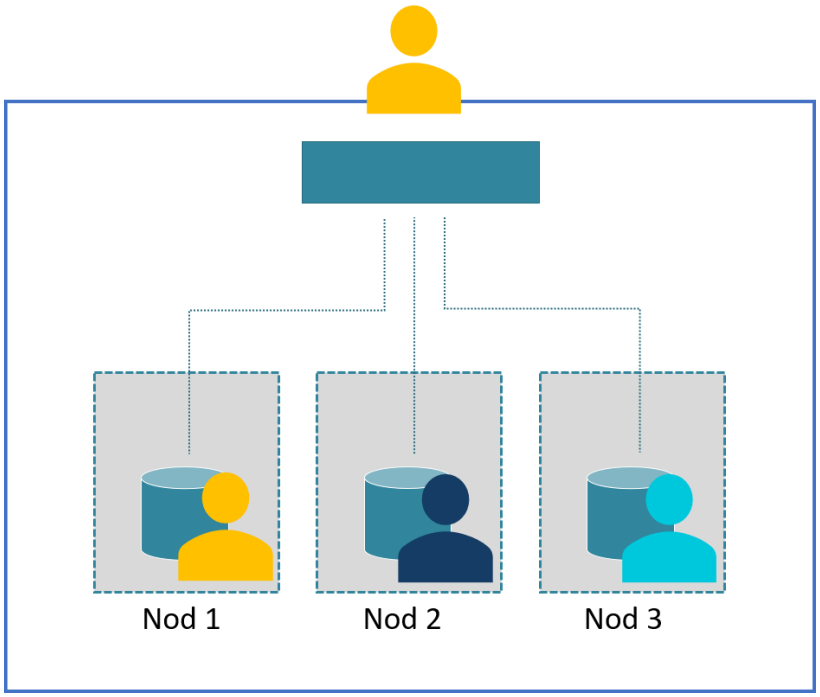
Ändamålet är själva syftet med behandlingen medan medlen är hur personuppgifterna behandlas. Om inget annat anges nedan så har analysen av ansvaret avgränsats till åtgärder och aktiviteter som sker inom den federerade analysen, det vill säga från att en fråga från analysdatorn ställs till noderna, noderna behandlar frågan och skickar tillbaka ett analyssvar till den centrala analysdatorn.

3.3.1. Modell 1 - Personuppgiftsbiträdesavtal vid federerad analys

Den första modellen utgår från att en forskningshuvudman (huvudmannen för nod 1) bestämmer över den centrala analysdatorn och är övergripande personuppgiftsansvarig för all personuppgiftsbehandling som sker inom den federerade analysen. Övriga forskningshuvudmän är då personuppgiftsbiträden för de specifika personuppgiftsbehandlingar som sker lokalt i noderna vid den statistiska analysen.

För att det de facto ska anses föreligga en biträdessituation får personuppgiftsbiträdena (forskningshuvudman 2 och forskningshuvudman 3) endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige (forskningshuvudman 1). Instruktionerna kan lämna ett visst handlingsutrymme för biträdet t.ex. vad gäller mest lämpliga tekniska och organisatoriska åtgärder för behandlingen.[54] För att det ska anses föreligga en biträdessituation ska den personuppgiftsansvarige faktiskt kunna åta sig ansvaret för behandlingarna av personuppgifterna som sker efter det att uppgifterna överförts till noden.

[54] Europeiska dataskyddsstyrelsens vägledning, ”Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, version 1.0 a, antagen den 2 september 2020.



Figur 4
Forskningshuvudmannen för nod 1 är personuppgiftsansvarig för all personuppgiftsbehandling som sker inom den federerade analysen. Forskningshuvudmännen för nod 2 och nod 3 är personuppgiftsbiträden.

Ändamålet för behandlingen är det man vill uppnå genom analyserna som ska göras på den specifika samling data som hanteras i noden. Arbetet med att definiera övergripande ändamål med forskningen och specifika ändamål för analyser kan ske under öppna former men det är de personuppgiftsansvariga som utövar den slutliga beslutanderätten (”*exercise of decision-making power*”) över både ändamål och medel. Ytterst är det den personuppgiftsansvarige (forskningshuvudman 1) som bestämmer att en specifik analys av en specifik samling data ska äga rum i en nod och varför den analysen är nödvändig för att uppnå det övergripande ändamålet med forskningen. Detta måste även tydligt återspeglas av personuppgiftsbiträdesavtalet.

Kan den personuppgiftsansvarige forskningshuvudmannen, inom ramen för sin verksamhet, åta sig ansvaret för ett biträdes analys av personuppgifter som biträdet samlat in i egenskap av personuppgiftsansvarig forskningshuvudman? Detta är en frågeställning som måste besvaras i det enskilda fallet. En rimlig utgångspunkt för bedömningen är situationer där det bedöms lagligt och lämpligt att överföra uppgifter mellan forskningshuvudmän inom ramen för ett traditionellt forskningssamarbete. Är det lagligt och lämpligt att överföra personuppgifter mellan forskningshuvudmännen torde det även vara lämpligt att överföra ansvaret för en personuppgiftsbehandling mellan två huvudmän.

En viktig observation är att de forskningshuvudmän som i denna modell är personuppgiftsbiträden är personuppgiftsansvariga för behandlingar i tidigare led för de uppgifter som ska föras över till noderna. Biträdet måste därför säkerställa att hanteringen som ska ske i noden inte är oförenlig med de ursprungliga ändamålen för vilka de samlades in eller en separat rättslig grund.[55]

Etikprövningslagen är territoriellt avgränsad till Sverige, se avsnitt 2.5. I exemplet utgår vi från att de andra ländernas lagstiftning är uppbyggda på samma sätt, dvs att de är avgränsade territoriellt. Det innebär att varje land som medverkar i studien behöver ansöka om etikprövning nationellt. Det är

[55] Se artikel 5.1 c och skäl 50 i dataskyddsförordningen angående ändamålsbegränsning.

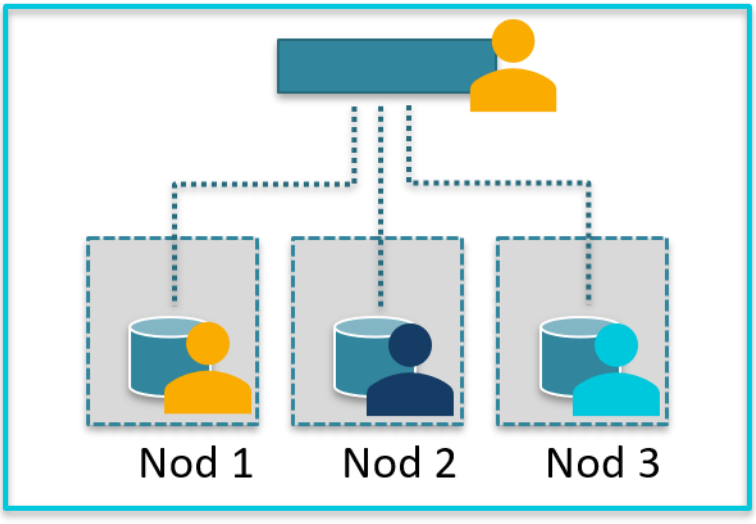
forskningshuvudman 1 som är personuppgiftsansvarig om denne ställer upp ändamål och medel med behandlingen av personuppgifterna. I federerad analys är analysfrågan att anse som ändamålet med behandling medan den konfigurering av noderna som krävs för att kunna utföra behandlingen är att ses som medel utifrån personuppgiftsansvaret. Noderna ska endast utföra de behandlingar som krävs för att besvara forskningshuvudmannens beräkningsfrågor. Det är då viktigt att, enligt ovan, avtala om förutsättningarna för behandlingen och hur fördelningen av ansvar ska se. Detta bör lämpligen göras redan i forskningsprojektets planeringsfas och ska dokumenteras i ett skriftligt avtal eller överenskommelse.[56]

När det rör sig om federerad analys är det viktigt att hålla isär den behandling som sker av personuppgifter inom forskningsprojektet med stöd av federerad analys och den som sker i noderna av forskningshuvudman 2 och forskningshuvudman 3 utanför projektet som t.ex. att samla in den registerdata som finns i noden eller att data behandlas av noderna. Forskningshuvudman 2 och forskningshuvudman 3 är alltid personuppgiftsansvarig för de personuppgifter som denne t.ex. samlar in, lagrar och behandlar utifrån egna ändamål och medel och ansvarar även för att ha laglig grund för att de insamlade uppgifterna får användas vidare i projektet, även om denne är att anse som personuppgiftsbiträde i forskningsprojektet i fråga.

3.3.2. Modell 2 - Ensamt övergripande personuppgiftsansvar vid federerad analys

Den andra modellen utgår ifrån att en av forskningshuvudmännen (huvudmannen för nod 1) ensam bestämmer över den centrala analysdatorn och de övergripande ändamålen och medlen för behandlingen av personuppgifterna inom den federerade analysen, med undantag för de specifika personuppgiftsbehandlingar som sker lokalt i noderna vid de statistiska beräkningarna.

I modell 2 är respektive forskningshuvudman (huvudmännen för nod 1, 2 och 3) personuppgiftsansvarig för de behandlingar som sker i noden. Varje deltagande forskningshuvudman ansvarar för att deras nod konfigureras i förhållande till ändamålet med den federerad analysen.



Figur 5
En övergripande ansvarig huvudman i kombination med självständigt ansvariga noder.

[56] Se artikel 28.3 i dataskyddsförordningen.

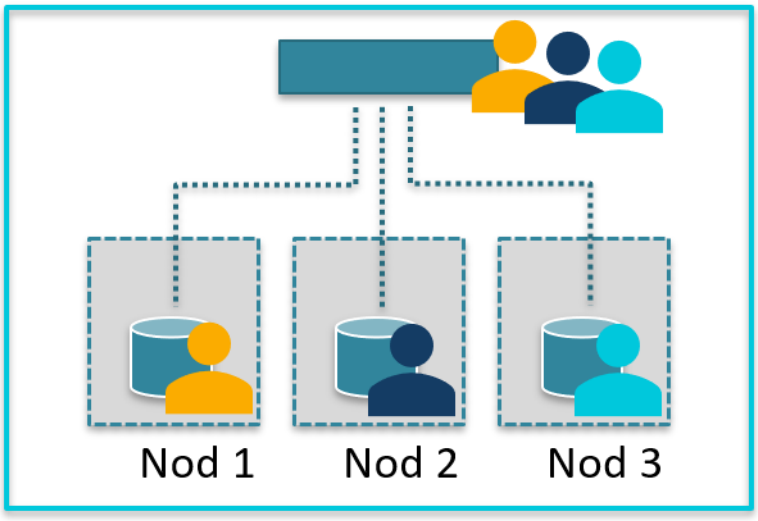
För att det de facto ska anses föreligga ensamt ansvar för forskningshuvudman 1 får övriga forskningshuvudmän inte delta organisatoriskt eller faktiskt i slutliga beslut kring övergripande frågor eller systemets övriga komponenter utanför den egna noden. Forskningssamarbetet kan ske under öppna former men det är de personuppgiftsansvariga som utövar den slutliga beslutanderätten (”*exercise of decision-making power*”). Det är den personuppgiftsansvarige (forskningshuvudman 1) som bestämmer att en specifik analys av en specifik samling data ska äga rum i en nod och varför den analysen är nödvändig för att uppnå det övergripande ändamålet med forskningen. Ytterst blir det dock den personuppgiftsansvarige forskningshuvudmannen (huvudmännen för nod 1, 2 och 3) för noden som beslutar om en specifik analysfråga ska få tillåtelse att köras på noden.

Modell 2 innebär i teorin tydligt avgränsade roller och ansvar. Det kan dock vara en pedagogisk utmaning att beskriva dessa i avtal och överenskommelser och även utmanande att hålla sig till dessa roller i det faktiska arbetet.

3.3.3 Modell 3 - Gemensamt övergripande personuppgiftsansvar vid federerad analys

Den tredje modellen utgår ifrån att forskningshuvudmännen (huvudmännen för nod 1, 2 och 3) bestämmer gemensamt de övergripande ändamålen och medlen för behandlingen av personuppgifterna i samarbetet där den federerade analysen äger rum (analysdatorn). Huvudmännen bestämmer gemensamt vad man vill uppnå genom analyserna som ska göras på den specifika samling data som hanteras i respektive deltagande nod.

I modell 3 är respektive forskningshuvudman (huvudmännen för nod 1, 2 och 3) personuppgiftsansvarig för de behandlingar som sker i noden. Varje deltagande forskningshuvudman ansvarar för att deras nod konfigureras i förhållande till ändamålet med den federerad analysen.



Figur 6
Gemensamt övergripande ansvar i kombination med självständigt ansvariga noder.

Vid gemensamt personuppgiftsansvar är parterna även gemensamt och solidariskt ansvariga för eventuell skada som uppkommer. Ett avtal som reglerar hur parterna ska förhålla sig till behandlingen av personuppgifterna bör därför vara tydligt utformat och ta upp alla behandlingar som sker inom samarbetet. Det är viktigt att avgränsa vilka behandlingar som ingår i det gemensamma ansvaret.

Ett forskningssamarbete med gemensamt personuppgiftsansvar uppställer större krav på tillit mellan deltagarna jämfört med andra modeller. Gemensamt ansvar innebär även särskilda krav på dokumentation av beslut och åtgärder i olika skeden av projektet.

3.4 Säkerhet

Det framgår av dataskyddsförordningen att personuppgiftsansvarig och personuppgiftsbiträde måste vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Åtgärderna ska tas med beaktande av den senaste utvecklingen, genomförandekostnaderna, behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.[57] Det krävs alltså tekniska och organisatoriska lösningar som står i proportion till risken för en personuppgiftsincident.

Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs om uppgiftsbehandlingen inbegriper en risk eller en hög risk. Faktorer som bör beaktas vid bedömningen av risken för forskningspersoners rättigheter och friheter är bland annat om det är frågan om personuppgifter som omfattas av tystnadsplikt, uppgifter om hälsa eller sexualliv, om det sker behandling av personuppgifter rörande sårbara fysiska personer – framför allt barn – eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade. Även skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier av uppgifter som kan kräva särskilda riskbedömningar.

Att ett forskningsprojekt använder sig av federerad analys istället för att på ett traditionellt sätt överföra personuppgifter för gemensam analys innebär inte att det är saknas riskelement i hanteringen av personuppgifter, även om vissa risker minskar i förhållande traditionella metoder. Antalet deltagande noder och vald teknisk plattform är några faktorer som påverkar riskbedömningarna. Det krävs att en riskanalys görs i ett tidigt stadie i planeringen av forskningen då riskanalyser är en viktig del i arbetet med dataskydd och informationssäkerhet.[58]

Riskbedömning bör ske innan etikprövningsansökan lämnas in och absolut senast innan noderna konfigureras för att ta emot och behandla analysfrågor. Det vill säga att hur noderna konfigureras måste utformas utifrån riskbedömningen och användas på ett sätt som stämmer överens med den faktiska behandlingen (användningen).[59] I och med att inga personuppgifter lämnar noderna, om behandlingen av data sker med hjälp av federerad analys, minskar detta betydligt risken för en personuppgiftsincident vid hanteringen av personuppgifterna inom forskningsstudien. Detta under förutsättning att alla komponenter i den centrala analysdatorn och i noderna konfigureras på ett säkert sätt.

3.5 Analys av personuppgiftsansvaret vid forskningssamarbete

Vid registerforskning med federerade analyser är det särskilt viktigt att redan i projektets planeringsfas bestämma och tydliggöra de olika roller som finns i projektet i förhållande till personuppgifterna som behandlas. Vid traditionell registerforskning följer normalt personuppgiftsansvaret med om personuppgifterna överförs mellan verksamheter och huvudmän. Vid registerforskning med federerade analyser kan ansvaret för en behandling flyttas mellan deltagande forskningshuvudmän utan att det sker

[57] Se artikel 24 och 32 i dataskyddsförordningen.
[58] Riskbedömningar bör göras kontinuerligt för alla behandlingar av personuppgifter. Om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter är det obligatoriskt att genomföra en konsekvensbedömning avseende dataskydd, se artikel 35 och skäl 89-93 i dataskyddsförordningen.
[59] Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram ett metodstöd för arbete med informationssäkerhet - https://www.informationssakerhet.se/metodstodet/.

någon överföring av personuppgifterna i fråga, se tabellen nedan. Det finns dock många andra relevanta faktorer som kan utgöra vägledning när det är svårt att utröna personuppgiftsansvaret ur ett informationsflöde.

Det är därför extra viktigt att bestämma rutiner, roller och relationer inom projektet. Det är även viktigt att alla parter inom projektet är införstådda i ansvarsfördelningen, annars finns det en risk för att någon part påverkar ändamål eller medel för behandlingen och att rollerna då förändras i och med att det faktiska ansvaret förändras. De två rollerna som personuppgiftsansvarig och personuppgiftsbiträde fördelas utifrån hur ansvaret för ändamål och medel för behandlingarna av personuppgifter ska ske inom projektet. Det beror på hur samarbetet inom projektet är tänkt att se ut samt vilket inflytande de deltagande forskningshuvudmännen ska ha på frågor och svar i den centrala analysdatorn och i förhållande till varandra. Ansvaret riktar sig i första hand mot de registrerade, men även mot parterna i projektet.

Vid en biträdessituation är det ett krav enligt dataskyddsförordningen att det ska finns ett skriftligt personuppgiftsbiträdesavtal.[60] Här kan det noteras att det inte finns något krav enligt dataskydds-förordningen på en skriftlig överenskommelse vid gemensamt personuppgiftsansvar eller vid ett samarbete mellan flera självständigt personuppgiftsansvariga huvudmän. Det är dock vår starka rekommendation att alltid dokumentera ansvar och avgränsningar i ett datadelningsavtal eller motsvarande.[61] Det ska vara tydligt och transparent hur fördelning av ansvaret samt behandlingen av personuppgifterna inom projektet ska ske. Tydlighet för de avtalande parterna för att det ska bli lättare att förhålla sig till och handla efter sin roll utifrån personuppgiftsansvaret eftersom ansvaret enligt dataskyddsförordningen utgår från de faktiska förutsättningarna, men även tydlighet mot de registrerade vars personuppgifter ligger till grund för forskningen och som behandlas av forskningshuvudmännen i respektive nod. Det finns alltså dels ett ansvar mot varandra som avtalspartner inom forskningsprojektet, dels ett ansvar för behandlingen av personuppgifterna mot den registrerade.[62]

Vem som är att anse som ansvarig för personuppgiftsbehandlingen är viktig utifrån att den ansvarige ska se till att dataskyddsförordningen efterlevs för alla behandlingar som faller under ansvaret. Det innebär bland annat att personuppgiftsansvarige ska se till att de registrerade ska tillhandahållas information om hur uppgifterna behandlas.[63] De registrerade har även rätt att begära rättelse eller radering av personuppgifter.[64] Personuppgiftsansvarig eller personuppgiftsbiträde ska ersätta all skada som en enskild individ kan komma att åsamkas till följd av personuppgiftsbehandling som strider mot GDPR. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör dock befrias från skadeståndsskyldighet om den kan visa att den inte på något sätt är ansvarig för skadan. Begreppet skada bör tolkas brett mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar dataskyddsförordningens mål. Den som har lidit skada har i princip rätt att få ersättning för hela skadan av antingen den personuppgiftsansvarige eller personuppgiftsbiträdet. Om en skadevållare betalt full ersättning till den registrerade har den rätt att inleda ett regressförfarande mot övriga skadevållare.[65] Om en personuppgiftsansvarig eller ett personuppgiftsbiträde har överträtt bestämmelserna i dataskyddsförordningen kan de även få betala kostsamma administrativa sanktionsavgifter som efterlevs av tillsynsmyndigheten.[66]

[60] Biträdesavtalet ska inte bara återupprepa innehållet i artikel 28 utan ge specifik, konkret information om hur kraven kommer uppnås, se EDPB:s vägledning punkt 109.
[61] Se bilaga 1 för exempel på vad som bör ingå i ett datadelningsavtal.
[62] Se artikel 1.2 i dataskyddsförordningen.
[63] Se artiklarna 12 till 14 i dataskyddsförordningen.
[64] Se artiklarna 16 och 17 i dataskyddsförordningen.
[65] Se skäl 146 och artikel 82 i dataskyddsförordningen.
[66] Se skäl 148-150 samt artikel 83 i dataskyddsförordningen.

I nedanstående tabell presenteras en jämförelse mellan de tre modellerna och ett traditionellt samarbete.

Tabell 1

	Traditionellt samarbete med biträdesavtal	**Modell 1** Federerad analys med biträdesavtal för noder	**Modell 2** Federerad analys med en ensamt ansvarig huvudman	**Modell 3** Federerad analys med gemensamt ansvar för den centrala analysdatorn
Överföring av data från ursprungskällan till noden	-	Ja	Ja	Ja
Överföring av personuppgifter mellan parterna.	Ja	Nej	Nej	Nej
Överföring av ansvar mellan parterna.	Ja	Ja	Nej	Nej
Solidariskt ansvar för en skadegenererande händelse i den centrala analysdatorn	-	Nej	Nej	Ja
Solidariskt ansvar för skadegenererande händelse i noden	-	Ja (För PA och berört biträde)	Nej	Nej

Oavsett vilken av modellerna för personuppgiftsansvar som tillämpas för personuppgiftsbehandlingen inom noderna sker det en överföring (eller ett tillgängliggörande) av personuppgifter från respektive ursprungskälla till respektive nod. Till skillnad från ett traditionellt samarbete sker vid federerad analys inte någon överföring av personuppgifter mellan de olika forskningshuvudmännen.

4. Slutsatser

Möjligheten att kunna använda sig av känsliga data i registerforskning från olika länder är en viktig framgångsfaktor inom uppföljning av läkemedel. Ett forskningssamarbete måste oavsett organisation och teknisk lösning vara förenligt med dataskyddsförordningen och tillämplig nationell lagstiftning. För att kunna tillvarata den mängd av data som finns tillgänglig genom samarbeten mellan olika länder krävs

det att det finns metoder för att samarbeta mellan länderna som är säkra utifrån såväl teknisk, statistisk som rättslig ståndpunkt.[67]

Rapporten tar upp hur behandling av personuppgifter i registerforskning regleras, huvudsakligen i dataskyddsförordningen, dataskyddslagen och till viss del av etikprövningslagen. I registerforskning som avser säkerhetsuppföljning av läkemedel analyseras data som normalt utgörs av känsliga personuppgifter. Denna typ av personuppgifter utgörs av hälsotillstånd eller andra integritetskänsliga uppgifter varför det krävs extra skyddsåtgärder enligt dataskyddsförordningen. Rapporten tar även upp begrepp som personuppgiftsansvarig, personuppgiftsbiträde och forskningshuvudman, vilka alla är vikt att känna till för att kunna fullgöra sina åtagande utifrån dataskyddsförordningen.

När federerad analys används för att analysera data inom forskning utför forskningshuvudmannen vid varje nod flera specifika behandlingar av personuppgifter i processtegen innan själva analysen. Den statistiska analysen som sker lokalt i noden utgör behandling av personuppgifter. Den data som respektive nod levererar till den centrala analysdatorn är däremot inte att betrakta som en behandling av personuppgifter, förutsatt att leveransen består av aggregerad data eller statistiska beräkningar.

Vid traditionell registerforskning följer normalt personuppgiftsansvaret med om personuppgifterna överförs från en verksamhet till en annan.

Vid registerforskning med federerade analyser kan ansvaret för personuppgifterna helt eller delvis komma att flyttas utan att det sker någon överföring av personuppgifterna i fråga. Det är därför lämpligt att tidigt i forskningsprojektets planeringsfas fastställa om det rör sig om ett eller flera forskningsprojekt och fastställa dess ansvarsfördelning och roller. Avtal och överenskommelser bör vara skriftliga och reglera ansvar och roller samt ansvarsskyldighet för underlåtenhet att efterleva avtalet. Här är det även lämpligt att parterna i avtal eller överenskommelser lämnar garantier om att deras personuppgiftsbehandlingar i noden uppfyller kraven i dataskyddsförordningen.

Det är inte givet vad som är den bästa modellen för fördelning av personuppgiftsansvaret i ett forskningsprojekt där federerad analys ingår. Det finns fördelar och nackdelar mellan de tre olika modellerna som presenterats i rapporten. Det är därför viktigt att beslutsfattare, forskare, tekniker, jurister och andra nyckelroller med koppling till ett forskningsprojekt är tillräckligt insatta såväl hur en federerad analys går till som tillämpliga delar av dataskyddsregelverket och hur ansvaret flyttas och fördelas i det aktuella forskningsprojektet.

Oavsett om samarbete kring registerforskning sker på traditionellt sätt eller med federerad analys ser vi inte att det uppstår några tydliga skillnader i förhållande till att den nationella regleringen i etikprövningslagen och dataskyddsförordningens territoriella tillämpningsområde.

Ur ett dataskyddsperspektiv är det positivt att tillämpningen av federerad analys ger större möjligheter till kontroll över personuppgiftsansvaret för respektive forskningshuvudman jämfört med att överföra personuppgifterna mellan huvudmännen utifrån de allmänna principerna om uppgiftsminimering och precisa ändamål utifrån dataskyddsförordningen. Ökade möjligheter till kontroll över personuppgifterna kan göra det lättare att ingå samarbeten över landsgränserna och därmed få tillgång till större datamängder till underlag för forskningen och på så sätt få mer tillförlitligt resultat. Det som vi ser som den största utmaningen med federerad analys är att det kan vara mer komplicerat att utreda hur personuppgiftsansvaret förflyttas beroende på val av samarbetsform.

[67] Utgångspunkten i rapporten är främst de nordiska länderna då dessa länder har en liknande lagstiftning vad det gäller både dataskydd och etikprövning, men även andra länder inom EU/EES är möjliga.

En intressant lösning för att underlätta användningen av federerad analys är att upprätta en uppförandekod enligt artiklarna 40-43 i dataskyddsförordningen. En uppförandekod bidrar till en korrekt och effektiv tillämpning av dataskyddsförordningen.[68]

5. Definitioner och förkortningar

I artikel 4 i dataskyddsförordningen räknas en rad olika begrepp eller definitioner upp. Dessa kan vara användbara för att förstå vad som menas med begreppet i förhållande till förordningen. Nedan finns ett urval av de definitioner som anges i artikeln uppräknade.

Personuppgift: är varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Behandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Register: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

Personuppgiftsansvarig: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning

Gränsöverskridande behandling:

a) behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller

b) behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat.

[68] Se t.ex. Nordiska ministerrådet rapport från 2019, NordForsk, ”A vision of a Nordic secure digital infrastructure for health data: The Nordic Commons“s. 27. Rapporten innehåller flera förslag, bl.a. ett som avser uppförandekod.

6. Litteraturlista

6.1 Författningar

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

Personuppgiftslagen (1998:204) – upphävd

Personuppgiftsförordningen (1998:1191) - upphävd

Lagen (2003:460) om etikprövning av forskning som avser människor

Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

6.2 Förarbeten

Proposition 2002/03:50 – Etikprövning i forskning

Proposition 2017/18:298 – Behandling av personuppgifter för forskningsändamål

SOU 2017:39 – Dataskyddsutredning

6.3 Doktrin

GDPR juridik, organisation, säkerhet, D. Frydlinger, T. Edvardsson, C. Olstedt Carlström och S. Beyer, Norstedts juridik, 2018

Dataskyddsförordningen (GDOR) m.m. En kommentar, Sören Öman, Gula biblioteket, Norstedts juridik, 2019

6.4 Artiklar/vägledningar

Europeiska dataskyddsstyrelsens vägledning, ”Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, version 1.0 a, antagen den 2 september 2020

Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram ett metodstöd för arbete med informationssäkerhet - https://www.informationssakerhet.se/metodstodet/.

6.5 Rättsfall

EU-domstolens dom (andra avdelningen) av den 29 juli 2019
”Fashion ID GmbH & Co.KG mot Verbraucherzentrale NRW eV”, målnummer C-40/17

EU-domstolens dom av den 10 juli 2018 ”Jehovan todistajat”, målnummer C-25/17

7. Bilagor

Bilaga 1 – Gemensamt personuppgiftsansvar (datadelningsavtal)

Ett avtal för gemensamt personuppgiftsansvariga kan inkludera (denna lista är varken slutgiltig eller fullständig)[1]:

– ändamål med personuppgiftsdelning/det gemensamma personuppgiftsansvaret

– identitet för de organisationer (personuppgiftsansvariga) som är parter i det gemensamma personuppgiftsansvaret

– kategorier av personuppgifter som kan delas och/eller överföras och behandlas enligt avtalet

– översikt över behandlingsåtgärderna (t.ex. överföring, användning)

– beskrivning av de respektive rollerna och ansvarsområdena i det gemensamma personuppgiftsansvaret

– ansvar för genomförandet av tekniska och organisatoriska säkerhetsåtgärder för personuppgiftsskydd

– definition av ansvar vid en personuppgiftsincident (t.ex. vem som kommer att informera, när det skall ske och eventuell ömsesidig information)

– villkor för bevarande och/eller radering av personuppgifter

– ansvarsskyldighet för underlåtenhet att efterleva avtalet

– hur förpliktelserna gentemot de registrerade uppfylls

– hur de registrerade förses med information om innebörden av förhållandet mellan de gemensamt personuppgiftsansvariga

– hur de registrerade kan få annan information de har rätt att få och en kontaktpunkt för de registrerade.

Adress: Läkemedelsverket, Box 26, 751 03 Uppsala
Besöksadress: Dag Hammarskjölds väg 42
Telefon: 018-17 46 00 Fax: 018-54 58 66
E-post: registrator@lakemedelsverket.se
www.lakemedelsverket.se