Personuppgiftsansvar vid klinisk forskning

Version 1.2
2022-02-08

Rapporten sammanställd av
Per Bergstrand, Secure State Cyber

Per Bergstrand, Secure State Cyber, 2022-02-08

Innehållsförteckning

Revisionshistorik

Version	Datum	Författare	Beskrivning
1.0	2021-05-01	Per Bergstrand, Secure State Cyber	Rapport framtagen.
1.1	2021-06-17	Per Bergstrand, Secure State Cyber	Rapport uppdaterad.
1.2	2021-09-30	Per Bergstrand, Secure State Cyber	Rapport uppdaterad utifrån remissvar från Noderna.

1 Inledning

1.1 Bakgrund

En klinisk studie som ska genomföras korrekt styrs av lagar, författningar och riktlinjer. En del av dessa lagar och riktlinjer är nationella (svenska) medan andra är internationella, till exempel EU-förordningar. En EU-förordning innebär att den rättsliga regleringen ser likadan ut inom hela EU. En EU-förordning som berör kliniska studier är EU:s allmänna dataskyddsförordning (GDPR)[1] vilken utgör ramlagen för all behandling av personuppgifter inom EU.

I och med att GDPR började gälla maj 2018 har det uppmärksammats särskilt hur personuppgifter behandlas inom ramen för kliniska studier samt de forskningsdata som ska ligga till grund för analys och slutsatser. Tolkningen av vilken organisation som enligt GDPR ska vara personuppgiftsansvarig inom ramen för olika scenarier har visat sig skilja sig mellan Kliniska Studier Sveriges olika noder/regioner. Det föreligger därför ett behov av att skapa förutsättningar för att uppnå en nationell samsyn när det gäller tolkningen av GDPR och de ansvar som följer av denna lag så att alla forskare, oavsett forskningshuvudman, får samma förutsättningar att genomföra kliniska studier.

1.2 Syfte

Syftet med denna rapport är att besvara följande frågor utifrån scenariobeskrivningarna i avsnitt 5: (1) vilken aktör, eller vilka aktörer, är (a) personuppgiftsansvarig, (b) gemensamt personuppgiftsansvarig, eller (c) personuppgiftsbiträde för vilken behandling, och (2) vilka avtal avseende personuppgifter ska eller bör tecknas mellan ingående parter?

Det ska tilläggas att det finns många aspekter av GDPR som har betydelse för genomförandet av kliniska studier, till exempel den rättsliga grunden för behandlingen. Dessa och andra frågor är dock inte föremål för just denna rapport utan får behandlas vid ett senare tillfälle.

1.3 Utförande

Rapporten har tagits fram dels genom en juridisk analys, dels genom en tillämpning av den juridiska analysen på ett antal olika personuppgiftsbehandlingssituationer med olika partskonstellationer.

Dessa situationer utgår utifrån ett antal på förhand definierade scenarios kring klinisk forskning. Dessa scenarios har konstruerats och redovisats genom samverkan med samtliga noder i Kliniska Studier Sverige för att motsvara de vanligaste situationerna för inblandade parter inom ramen för olika typer av klinisk forskning.

Utifrån dessa scenarios har workshops hållits där det deltagit både jurister och kliniskt aktiv personal. I dessa workshops har man utgått från de frågeställningar kring personuppgiftsansvar som redogjorts för i rapporten och utifrån dessa bedömts på vilket sätt de olika parterna i respektive scenario direkt eller indirekt innehar ett faktiskt inflytande på olika delar av behandlingen av personuppgifter. Slutsatserna från genomförda workshops redovisas i denna rapport inom ramen för beskrivningen av respektive scenario.

Varje scenarioavsnitt är skrivet på ett sådant sätt att ett avsnitt ska kunna läsas helt fristående. Det innebär att en viss upprepning mellan de olika scenarierna för att sammanhanget ska blir så förståeligt som möjligt.

[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 (allmän dataskyddsförordning).

1.4 Terminologi

I följande avsnitt detaljeras central terminologi för rapporten. Se fullständig lista över använda termer och dess betydelse i bilaga 2.

1.4.1 Begreppen *forskning* och *forskningshuvudman*

Begreppet forskning har över tid definierats på flera olika sätt beroende på sammanhang. I den forskningspolitiska propositionen från 2016[2] använder regeringen en definition av forskning och utveckling som hämtats från Statistiska centralbyrån:

> ett systematiskt arbete för att söka efter ny kunskap eller nya idéer med eller utan en bestämd tillämpning i sikte. Här ingår också systematiskt arbete som utnyttjar forskningsresultat, vetenskaplig kunskap eller nya idéer för att åstadkomma nya material, varor, tjänster, processer, system och metoder, eller väsentliga förbättringar av redan existerande sådana.

I syfte att förtydliga Etikprövningslagen[3] och kodifiera praxis från Etikprövningsmyndigheten gäller sedan den 1 januari 2020 följande definitioner av begreppen forskning och forskningshuvudman.

Med forskning avses i 2 § etikprövningslagen:

> vetenskapligt experimentellt eller teoretiskt arbete eller vetenskapliga studier genom observation, om arbetet eller studierna görs för att hämta in ny kunskap, och utvecklingsarbete på vetenskaplig grund, dock inte sådant arbete eller sådana studier som utförs endast inom ramen för högskoleutbildning på grundnivå eller på avancerad nivå.[4]

Med forskningshuvudman avses i 2 § samma lag:

> en statlig myndighet eller en fysisk eller juridisk person i vars verksamhet forskningen utförs.

Av förarbetsuttalanden framgår att vid forskningsprojekt, där vissa delar av forskningen utförs på patienter inom sjukvården, är vårdgivaren forskningshuvudman för den delen av forskningsprojektet. Vårdgivaren har därmed ansvar för att etikprövningslagens regler efterlevs i forskningen, samtidigt som vårdgivaren har ansvar för patientens vård. Andra forskningshuvudmän är ansvariga för de moment av forskningsprojektet som utförs i deras regi.[5]

I forskningsprojekt där forskning utförs både inom ramen för en vårdgivarens verksamhet och en annan aktörs verksamhet är respektive part ansvarig för den del av projektet som utförs i den egna verksamheten. Det är därför viktigt att alla parter anges som forskningshuvudmän i ansökan till Etikprövningsmyndigheten och att det tydligt redogörs för vilka delar av forskningen som ska utföras i respektive verksamhet.

Vid ansökan om etikprövning till Etikprövningsmyndigheten görs en åtskillnad mellan den forskningshuvudman som ansöker om etikprövning (huvudansvarig forskningshuvudman), och andra forskningshuvudmän som deltar i forskningen (medverkande forskningshuvudmän). Varje forskningshuvudman ansvarar fortfarande för den del av forskningen som bedrivs i den egna verksamheten. Etikprövningen omfattar hela projektet och samtliga medverkande forskningshuvudmän.

[2] Prop. 2016/17:50.
[3] lag (2003:460) om etikprövning av forskning som avser människor (Etikprövningslagen).
[4] 2 § Lag (2003:460) om etikprövning av forskning som avser människor.
[5] Prop. 2018/19:165 s. 40 f.

1.4.2 Begreppen *klinisk forskning* och *kliniska studier*

Klinisk forskning är ett begrepp som ofta används, men som saknar en tydligt fastslagen definition. I Utbildningsdepartementets utredning om klinisk forskning 2007[6] menades att det saknas entydig beskrivning av vad klinisk forskning är, och att definitionen över tid har påverkats av avgränsningar i den medicinska forskningens finansieringssystem. Utredningen valde att definiera klinisk forskning som:

> forskning som förutsätter vårdens strukturer och resurser och som har som mål att lösa ett ohälsoproblem eller att identifiera faktorer som leder till ökad hälsa.

Denna utgångspunkt har fått spridning och återkommer till exempel i efterföljande utredningar, bland annat vid ändringar av etikprövningslagen.

Vetenskapsrådet ska enligt instruktion (2009:975) stödja och utveckla förutsättningarna för kliniska studier i Sverige. Vetenskapsrådet använder sedan april 2021 följande definition av klinisk forskning respektive kliniska studier:[7]

> *Klinisk forskning*
>
> Klinisk forskning är medicinsk och hälsovetenskaplig forskning som förutsätter vårdens strukturer och resurser och har som mål att lösa ett ohälsoproblem eller att identifiera faktorer som leder till ökad hälsa.
>
> *Kliniska studier*
>
> Kliniska studier genomförs på människor för att studera medicinska eller hälsorelaterade frågeställningar.

1.4.3 Begreppet *klinisk läkemedelsprövning*

En klinisk läkemedelsprövning definieras enligt 2 kap. 1 § Läkemedelslagen (2015:315) som:

> *En klinisk undersökning på människor eller djur av ett läkemedels egenskaper.*

Läkemedelslagen kommer att ändras där begreppet klinisk läkemedelsprövning utgår och ersätts med begreppet klinisk läkemedelsprövning på människor, vilket kommer definieras i 2 kap. 1 § genom en hänvisning till artikel 2.2.2 CTR:

> En klinisk prövning enligt definitionen i artikel 2.2.2 i Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av human-läkemedel och om upphävande av direktiv 2001/20/EG.
>
> *Som lyder:*
>
> En klinisk prövning är en klinisk studie där
>
> a) den behandlingsstrategi som ska tillämpas på försökspersonen fastställs i förväg och avviker från normal klinisk praxis i den berörda medlemsstaten,
>
> b) beslutet att förskriva prövningsläkemedlet fattas samtidigt som beslutet att inkludera försökspersonen i den kliniska studien, eller
>
> c) förfaranden för diagnostik eller övervakning utöver normal klinisk praxis tillämpas på försökspersonerna.

[6] Utredningen om den kliniska forskningens behov och villkor samt förslag till åtgärdsplan (U 2007:04).
[7] Vetenskapsrådet dnr. 1.2.4-2021-03621.

1.4.4 Begreppen *samtycke* och *informerat samtycke*

Inom ramen för forskning finns det åtminstone sex *typer av samtycke* som aktualiseras:

(1) samtycke till behandling av personuppgifter enligt artikel 4.11 GDPR,[8]
(2) informerat samtycke till forskning enligt 13-17 §§ etikprövningslagen,
(3) informerat samtycke till klinisk läkemedelsprövning enligt 7 kap. 3-4 §§ läkemedelslagen,
(4) samtycke och information enligt 3 kap. Biobankslagen (2002:297),[9]
(5) samtycke enligt 4 kap. Patientlagen (2014:821),[10] och;
(6) samtycke till hävande av sekretess enligt 12 kap. 2 § Offentlighets- och sekretesslagen (2009:400).[11]

De är olika typer av samtycken så till vida att de är definierade på olika sätt i olika lagstiftningar och således måste bedömas utifrån sin egen kontext.

Gemensamt för samtliga är att ett samtycke måste vara en frivillig viljeyttring som innebär att den som avger viljeyttringen samtycker till en viss i förväg beskriven och för den samtyckande parten känd hantering samt att den samtyckande parten tagit del av viss information. Ett samtycke ska också alltid kunna tas tillbaka av den samtyckande parten.

Området är juridiskt komplext eftersom det i den praktiken vid tillämpning av samtycke inte alltid är tydligt om ett givet samtycke avser den rättsliga grunden för behandlingen av personuppgifter enligt GDPR i sig eller om det istället är en viljeyttring för att godkänna en hävning av sekretess eller andra legala säkerhetsmekanismer, till exempel i de lagstiftningar som exemplifierats ovan.[12]

Mot bakgrund av ovanstående är det alltid viktigt att begreppet samtycke används på ett tydligt sätt och att det är klart beskrivet vilka legala mekanismer samtycket är tänkt att uppnå i den givna situationen.

[8] Notera att samtycke här avser samtycke som en rättslig grund att behandla personuppgifter, såsom redogörs för översiktligt i styckena nedan anses den rättsliga grunden för att behandla personuppgifter inom ramen för forskning normalt vara att behandlingen av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse.
[9] Lag (2002:297) om biobanker i hälso- och sjukvården m.m.
[10] Patientlag (2014:821).
[11] Offentlighets- och sekretesslag (2009:400).
[12] Notera att den rättsliga grunden för att behandla personuppgifter inom ramen för forskning normalt utgår från att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

2 Tillämplig lagstiftning

Förutom GDPR, som är den centrala lagstiftningen för att besvara frågeställningarna i denna rapport, har följande lagar också betydelse för bedömning kring ansvar vad gäller hanteringen av information inom ramen för ett forskningsprojekt.

Lagen (2003:460) om etikprövning av forskning som avser människor (etikprövningslagen). I syfte att bland annat uppfylla de krav som ställdes i Europarådets konvention om mänskliga rättigheter och biomedicin[13] infördes den 1 januari 2004 etikprövningslagen. Lagen syftar även till att anpassa svensk lag utifrån direktiv 2001/20/EG om tillnärmning av god klinisk sed vid kliniska prövningar av humanläkemedel. Etikprövningslagen innehåller bestämmelser om etikprövning av forskning som avser människor och biologiskt material från människor. Den innehåller också bestämmelser om samtycke till sådan forskning. I etikprövningslagen definieras olika aktörer inom forskningsområdet.

Klinisk läkemedelsprövning regleras idag genom läkemedelslagen (2015:315) och Läkemedelsverkets föreskrifter och allmänna råd (LVFS 2011:19) om kliniska läkemedelsprövningar på människor, vilka införlivar EU-direktivet 2001/20 om kliniska prövningar av humanläkemedel. Direktivet ska ersättas av EU-förordningen 536/2014 om kliniska prövningar av humanläkemedel (CTR) vilket kommer medföra även ändringar i läkemedelslagen. CTR trädde i kraft 2014 och ska börja gälla 31 januari 2022.[14]

Slutligen gäller även direktivet 2005/28/EG om fastställande av principer och detaljerade riktlinjer för god klinisk sed (GCP **(**Good Clinical Practice) - direktivet).

[13] ETS 164 och tilläggsprotokollet ETS 168.
[14] CTR trädde i kraft 2014 men tidpunkten för att den faktiskt ska tillämpas är avhängigt upprättandet av CTIS-databasen (Clinical Trial Information System). När förordningen väl börjar tillämpas kommer det tidigare direktivet och nationell lagstiftning som följt av direktivet inte längre att gälla. Se mer info https://www.ema.europa.eu/en/human-regulatory/research-development/clinical-trials/clinical-trial-regulation.

3 Personuppgiftsansvar i GDPR

3.1 Inledning

Huvudansvaret att tillse fysiska personer skydd genom GDPR samt nationella registerförfattningar ligger på den eller de (en eller flera) parter som är *personuppgiftsansvarig* eller *personuppgiftsansvariga*. Det finns alltid minst en personuppgiftsansvarig för varje behandling av personuppgifter. En personuppgiftsansvarig kan ge en annan part i uppdrag att utföra vissa delar av behandlingen och den som i sådant fall får detta uppdrag kallas personuppgiftsbiträde. Ett begränsat ansvar för delar av behandlingen (huvudsakligen att hanteringen sker på ett säkert sätt) bärs även av detta personuppgiftsbiträde. Anställda personer och andra fysiska personer som arbetar för en personuppgiftsansvarig eller ett personuppgiftsbiträde bär normalt inget eget ansvar enligt GDPR för den behandling som de utför åt sin arbets- eller uppdragsgivare utan det är i första hand en organisation (juridisk person) som är personuppgiftsansvarig. En forskare som arbetar för en vårdgivare, eller en akademisk institution har alltså i sin roll som prövare inget eget personuppgiftsansvar för den behandling av personuppgifter som sker, utan det är normalt den juridiska organisationen denne representerar som är personuppgiftsansvarig. Det är av detta skäl alltid väldigt viktigt att vara medveten om vilken organisation man representerar i varje given situation, särskilt i de fall en person arbetar för flera olika organisationer.

Om det är endast en aktör som är personuppgiftsansvarig så uttrycks detta ibland som ett *enskilt* personuppgiftsansvar för att understryka att den är en aktör som innehar det (i motsats till gemensamt personuppgiftsansvar). I följande avsnitt beskrivs de olika ansvarsrollerna i GDPR samt vilka kännetecken som är associerade till respektive roll. I ett senare avsnitt beskrivs sedan en modell för att genomföra själva bedömningen av vilken aktör som har vilken roll.

3.2 Personuppgiftsansvarig – en redogörelse för begreppet

Den *personuppgiftsansvarige* (engelska: *data controller*) är den aktör, eller de aktörer, som bestämmer ändamål och medel med behandling av personuppgifter. Personuppgiftsansvarig kan vara en fysisk person men som huvudregel är det en juridisk person; en myndighet, en nämnd eller ett företag. Verksamhet som omfattas av författningsreglering eller yrkesetiska regler som begränsar möjligheten att agera enligt annans instruktion bär som regel eget personuppgiftsansvar. Det är nödvändigt att göra en prövning i det enskilda fallet eftersom det kan finnas ett utrymme att ta emot instruktioner avseende personuppgiftsbehandling och samtidigt efterleva regulatoriska skyldigheter.

Enligt legaldefinitionen har den personuppgiftsansvarige bestämmanderätt över ändamål och medel men har förvisso möjligheten att delegera valet av tekniska och organisatoriska medel för behandlingen till en annan part (som då utgör ett personuppgiftsbiträde). Med ändamål avses *varför* behandlingen utförs. Med medel avses *hur* behandlingen utförs. Personuppgiftsansvaret syftar till att etablera en tydlig ansvarsfördelning som är ändamålsenlig utifrån principerna för dataskydd. Med det menas att det är den som är personuppgiftsansvarig som ska se till att de rättigheter och krav som följer av GDPR också tillämpas och att det därför är avgörande att det är den parten som faktiskt har möjlighet och kapacitet att tillse detta som är den som innehar rollen.

Vissa medel har så stor påverkan för behandlingen, så kallade *avgörande medel*, att de anses vara sådana medel som bör bestämmas av den personuppgiftsansvarige, till exempel:

- vilka personuppgifter som ska samlas in och behandlas,
- hur länge personuppgifterna ska sparas,
- vilka aktörer som får ha åtkomst till personuppgifter eller som personuppgifter får utlämnas till.

Andra medel anses vara *mindre avgörande* och kan beslutas av någon annan aktör än den personuppgifts-ansvarige (men fortfarande på uppdrag av denne). Dessa mindre avgörande medel kan omfatta:

- vilka programvaror som ska användas,
- mer konkret hur hanteringen ska fungera,
- vilka typer av säkerhetsåtgärder som ska väljas.

Utifrån den Europeiska dataskyddsombudsmannens (EDPS) riktlinje kan en aktör vara person-uppgiftsansvarig på en av följande tre grunder: (1) uttrycklig behörighet, (2) underförstådd behörighet samt (3) faktiskt inflytande.[15]

Med **uttrycklig behörighet** avses bestämmanderätt som framgår av författning (lag) eller är en direkt följd av författning. Ett sådant exempel är Patientdatalagen (2008:355) (PDL) som reglerar vem som är den personuppgiftsansvarige för behandling av personuppgifter inom ramen för hälso- och sjukvård (vilket inte innefattar forskning) samt en uttömmande lista över vilka ändamål som personuppgifter får behandlas för inom ramen för PDL. När PDL är tillämplig är det uppenbart vilken part som tilldelats en uttrycklig behörighet att förfoga över ändamålen och medlen eftersom det direkt framgår av lag.

Med **underförstådd behörighet** avses att personuppgiftsansvaret härrör från etablerad praxis eller partsbruk på ett område. Ett sådant exempel är presumtionen för att en arbetsgivare är personuppgiftsansvarig för arbetstagares behandling av personuppgifter som denne utför i sitt arbete.

Med **faktiskt inflytande** avses vem som har faktiskt bestämmande över en behandling. Vem som har faktiskt inflytande över behandlingens ändamål är inte lika lätt att identifiera som uttrycklig eller under-förstådd behörighet. Avtal och annan dokumentation kan användas för att bedöma en aktörs faktiska inflytande, men detta behöver inte vara avgörande. Även om avtal förekommer som pekar ut en aktör är det den faktiska hanteringen som ska vara avgörande varför en bedömning alltid bör fokusera på hur hanteringen fungerar i verkligheten. I tveksamma fall kan även den registrerade personens (den vars personuppgifter är föremål för behandling) rimliga förväntningar påverka bedömningen.

Omständigheter som tyder på *faktiskt inflytande* och därmed personuppgiftsansvar:

- Parten får intäkter av, eller har ett intresse i behandlingen av personuppgifter utöver ren ersättning för den tjänst denne utför,
- Parten fattar beslut som påverkar de registrerade, besluten påverkas av eller resulterar i behandlingen av personuppgifter (till exempel registrerade utgörs av dennes anställda),
- Behandlingen av personuppgifter är naturligt anknuten till partens organisations roll och uppgift (utifrån sedvänja, handelsbruk eller förpliktelse i lag),
- Behandlingen av personuppgifter avser partens etablerade och formaliserade relation med de registrerade i form av kunder, anställda, medlemmar etcetera,
- Parten har ett ensamt inflytande över beslut kring hur behandlingen av personuppgifter ska gå till,
- Parten har på eget initiativ överlåtit behandlingen eller delar av behandlingen av personuppgifter till en annan organisation,
- Parten är den som kommer att avgöra om personuppgifterna ska sparar eller raderas när behandlingen är avslutad.

En viktig aspekt är att det mycket väl kan vara så att en behandling av personuppgifter som kanske av parterna från början inte var avsedd men trotts detta genomförs. Det är då *de facto* den part som haft ett bestämmande inflytande över denna ytterligare behandling som är personuppgiftsansvarig för den. Det uppstår helt enkelt en ny behandling och det är den som är personuppgiftsansvarig för denna som är ansvarig att efterleva alla tillämpliga skyldigheter i GDPR. Det kan vara värt att notera att den som utför

[15] EDPS Guidelines on the concepts of controller, processor, and joint controllership under Regulation (EU) 2018/1725, sida 7. Motsvarande beskrivning återfinns i Europeiska Dataskyddsstyrelsens (EDPB) förslag till riktlinjer ”Guidelines 07/2020 on the concepts of controller and processor in the GDPR” sid 10 ff.

den nye behandlingen kan ha brutit mot ett ingånget personuppgiftsbiträdesavtal[16] eller avtal om gemensamt personuppgiftsansvar[17] när denna vidtagit en ny behandling som inte var avsedd från början och därtill kan sakna rättslig grund för den nya behandlingen som denne nu är ansvarig för och därför potentiellt också kan drabbas av sanktionsavgifter eftersom denne brutit mot GDPR.

En annan viktig aspekt att beakta är att personuppgiftsansvar i sig inte innebär en rättighet att behandla personuppgifter. Tvärtom innebär ett personuppgiftsansvar att denne part är den som har ansvaret att se till att det finns en korrekt rättslig grund för behandlingen och att övriga skyldigheter i GDPR efterlevs. Det är den som faktiskt, med eller utan rätt därtill, har bestämt över behandlingen som är personuppgiftsansvarig. Det är således inte så att en part baserat på att denne har ett personuppgiftsansvar kan hävda rätten att få bestämma över ändamål eller medel, om det de facto inte är den parten som gör det. Detta faktum bör snarare vara ett tydligt tecken på att denne part inte är personuppgiftsansvarig. Endast förekomsten av ett avtal som reglerar ansvarsförhållandet avgör därmed inte ansvarsfrågan, det krävs dessutom att avtalet faktiskt är omsatt i verkligheten.

3.3 Gemensamt personuppgiftsansvar

Om flera aktörer gemensamt bestämmer ändamål och medel för behandlingen kan de vara gemensamt personuppgiftsansvariga (engelska: *joint controllers*).

Kravet på gemensam bestämmanderätt medför inte att de inblandade aktörerna behöver ha lika stor inverkan på beslut om ändamål och medel med behandlingen. Det är tillräckligt att en aktör *i eget syfte* påverkar behandlingen av personuppgifter och därigenom bestämmer ändamål och medel.[18] Det är inte heller ett krav att samtliga inblandade aktörer har åtkomst till personuppgifter.[19] En aktör som organiserar och samordnar andra aktörers behandling av personuppgifter kan därigenom få ett personuppgiftsansvar. En förutsättning för gemensamt personuppgiftsansvar är dock alltid att ändamålet med behandlingen är gemensamt (även om aktörerna kan ha olika stort intresse i behandlingen).

Om två eller flera aktörer är gemensamt personuppgiftsansvariga finns det enligt GDPR ett krav på ett *inbördes arrangemang*.[20] Av detta inbördes arrangemang ska särskilt former och ansvar för utövande av den registrerade personens (försökspersonens) rättigheter samt förpliktelsen att lämna information till registrerade personer framgå. Därtill ska det inbördes arrangemanget på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållande till de registrerade personerna. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för de registrerade personerna.

GDPR ger inte en uttömmande lista över vad som ska regleras genom ett inbördes arrangemang. Exempel på andra frågor som kan vara lämpliga att reglera genom ett inbördes arrangemang är bevarande och gallring av personuppgifter, säkerhet för behandling, tystnadsplikt samt kontroll av den eller de andra parternas regelefterlevnad. Det är inte ett strikt krav enligt GDPR att detta inbördes arrangemang regleras genom ett skriftligt avtal mellan parterna (i motsats till kravet på ett så kallad personuppgiftsbiträdesavtal mellan en personuppgiftsansvarig och ett personuppgiftsbiträde) men det torde dock vara *mycket lämpligt* att så sker för att tydligt dokumentera vad parterna inom det gemensamma personuppgiftansvaret har för gemensam uppfattning kring arrangemanget. Ett sådant avtal kan kallas avtal för gemensamt personuppgiftsansvar.

EU-domstolen, som ytterst tolkar GDPR, har publicerat två avgöranden som kan tolkas som att domstolen gör bedömningen att gemensamt personuppgiftsansvar är att föredra när gränsdragningen

[16] Så kallad PUB-avtal där ett personuppgiftsbiträde erhåller sitt uppdrag från en personuppgiftsansvarig enligt artikel 28.3 GDPR.
[17] Ett avtal mellan flera parter som gemensamt har ett personuppgiftsansvar över en viss behandling enligt artikel 26.1 GDPR (”inbördes arrangemang”).
[18] Mål C-25/17 Jehovas vittnen, punkt 68.
[19] Mål C-25/17 Jehovas vittnen, punkt 69.
[20] Artikel 26 GDPR.

mellan personuppgiftsansvaret är svår att göra.[21] Även EDPB:s riktlinje antyder att det finns flera tillfällen när ett gemensamt personuppgiftansvar förekommer än vad som tidigare ansetts, alltså att praxis går mot en större acceptans för gemensamt personuppgiftsansvar. Generellt är det vår slutsats att rättsutvecklingen som skett på området tyder på att det finns ett större tillämpningsområde för gemensamt personuppgiftsansvar idag än under personuppgiftslagen som föregick GDPR.

Omständigheter som tyder på gemensamt inflytande och därmed gemensamt personuppgiftsansvar:

- Att två eller flera organisationer tillsammans bestämmer ändamålet med behandlingen,
- Att två eller fler organisationer bestämmer *och enas* kring ett ändamål och medlen för detta (se avsnitt om EDPB:s riktlinjer, nedan),
- Att ingen av organisationerna är utbytbara inom ramen för behandlingen,
- Att ingen av organisationerna ensamt kan besluta om förändringar i behandlingen i stort,
- Att ingen av organisationerna dikterar villkoren för väsentliga delar av samarbetet för den andra organisationen.

3.4 Separat personuppgiftsansvar

Ibland används uttrycket separat personuppgiftsansvar för att understryka att flera olika aktörer har ett eget, enskilt, personuppgiftsansvar i motsats till ett gemensamt. Så kan till exempel vara fallet när personuppgifter utlämnas från en part till en annan men den utlämnande parten inte kommer att ha något inflytande eller bestämma något över ändamålen eller medlen som den mottagande parten har med behandlingen av personuppgifter. I ett sådant fall uttrycks att parterna har ett separat personuppgiftsansvar. Det ska dock understrykas att det inte finns någon legal definition av begreppet.

3.5 Personuppgiftsbiträde – en redogörelse för begreppet

Ett personuppgiftsbiträde (*engelska: data processor*) är en aktör som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde är precis som personuppgiftsansvarig som regel en juridisk person även om det inte utesluter att det i undantagsfall kan vara en fysisk person. Ett personuppgiftsbiträde grundar sin rätt att behandla personuppgifter helt på det uppdrag denne fått från den personuppgiftsansvarige. Ett personuppgiftsbiträde kan alltså inte ha en egen rättslig grund för behandling av personuppgifter och får inte heller vara den som fastställer ändamålet med behandlingen av personuppgifter (detta ansvar faller exklusivt på den personuppgiftsansvarige).

Ett vanligt missförstånd är att en leverantör som utför ett uppdrag åt en uppdragsgivare alltid är ett personuppgiftsbiträde till uppdragsgivaren. Genom detta synsätt blir själva konstellationen beställare – utförare avgörande för bedömningen vilket är ett alltför förenklat synsätt. Det avgörande är snarare att en leverantör som behandlar personuppgifter och helt saknar ett eget ändamål med den aktuella behandlingen är ett personuppgiftsbiträde.

Om ett personuppgiftsbiträde anlitas ska den behandling som personuppgiftsbiträdet utför regleras genom ett avtal eller en annan rättsakt; vanligtvis ett så kallad *personuppgiftsbiträdesavtal (PUB-avtal)*.[22] Vad som ska regleras i ett personuppgiftsbiträdesavtal regleras i förhållandevis stor detalj i GDPR. Genom personuppgiftsbiträdesavtalet ger den personuppgiftsansvarige skriftliga instruktioner om ändamålet för personuppgiftsbiträdets behandling samt reglerar närmare hur behandlingen ska genomföras.

En rättslig förpliktelse som åvilar ett personuppgiftsbiträde kan medföra att denne behöver behandla personuppgifter utan instruktion, eller i strid med instruktion, från en personuppgiftsansvarig.

[21] Se bl.a. Mål C-210/16 Wirtschaftsakademie Schleswig-Holstein (cookies med statistik) och Mål C-40/17 Fashion ID (FB Like-knapp).
[22] Artikel 28 GDPR.

Personuppgiftsbiträdet blir då personuppgiftsansvarig för den aktuella behandlingen eftersom den genomförts av personuppgiftsbiträdet i eget syfte (att följa en rättslig förpliktelse).

Omständigheter som tyder på att parten inte har ett faktiskt inflytande över behandlingen av personuppgifter och därmed ska betraktas som ett personuppgiftsbiträde:

- Parten behandlar personuppgifter för någon annan parts ändamål och i enlighet med givna instruktioner,
- Parten har inget eget ändamål med behandlingen av personuppgifterna (utöver att utföra en specifikt erbjuden tjänst som inte är ändamålet med behandlingen i sig). Som exempel kan nämnas ett företag som levererar översättning behandlar information och bland annat personuppgifter när det levererar sin tjänst, men företaget har inget intresse i slutresultatet av behandlingen mer än att leverera resultatet de ska få ersättning för,
- En annan organisation övervakar partens behandling för att kontrollera att parten utför den i enlighet med givna instruktioner och/eller villkor,
- Parten har inget mandat att besluta vad personuppgifterna ska användas till eller att förändra tidigare fattade beslut,
- När den aktuella behandlingen är avslutad kommer parten inte att bevara personuppgifterna; de kommer raderas eller lämnas till någon annan.

3.6 Andra rättskällor som påverkar bedömningen kring ansvar

I detta avsnitt redogörs för ytterligare rättskällor som kan ha betydelse för bedömningen av personuppgiftsansvaret när det gäller just området klinisk forskning.

3.6.1 Ansvar enligt Clinical trial regulation (CTR)

I bilaga 3 finns en mer omfattande redogörelse för den kommande förordningen för klinisk läkemedelsprövning som kommer vara gällande inom EU. I artikel 2 i CTR definieras (i) sponsorn som den aktör som ansvarar för att inleda, leda och ordna med finansieringen av en klinisk prövning,[23] och (ii) prövaren som den som ansvarar för genomförandet av en klinisk prövning på ett prövningsställe. En part som är sponsor enligt CTR bär också huvudansvaret enligt förordningen för fullgörandet av skyldigheterna i CTR. Denna reglering torde vara av betydelse vid beaktande av den så kallade uttryckliga behörigheten till behandling av personuppgifter. Ett ansvar utpekat i lag om att utföra viss verksamhet torde innebära att presumtion ligger för att denne part även är personuppgiftsansvarig för behandlingen som verksamheten innebär.

3.6.2 Ändamålet ”vetenskaplig forskning” och dess betydelse i GDPR

När behandling av personuppgifter sker inom ramen för hälso- och sjukvård är det vårdgivaren som är personuppgiftsansvarig för behandlingen. Detta följer av 2 kap 6 § PDL. Forskning är dock inte ett ändamål för behandling av personuppgifter som omfattas av PDL:s ändamålskatalog i 2 kap. 4 §. Denna ändamålskatalog är uttömmande och ger uttryck för den yttre ramen när personuppgifter får behandlas inom ramen för hälso- och sjukvård med stöd av PDL.[24]

Mot bakgrund av att forskning inte ingår i ändamålskatalogen är därmed PDL inte tillämplig på behandling av personuppgifter för forskningsändamål. Det innebär i sin tur att det inte per automatik finns en uttrycklig behörighet för vårdgivaren att vara personuppgiftsansvarig för den behandling av personuppgifter som sker inom ramen för ett forskningsprojekt.

[23] Sponsor är inte ett begrepp som ännu förekommer i Läkemedelslagen, men kommer att göra det när CTR träder i kraft (se föreslagen 2 kap 1 § läkemedelslagen, länk).
[24] Det kan dock noteras att personuppgifter även enligt PDL får behandlas för andra ändamål efter att patienten uttryckligen samtyckt till detta enligt 2 kap. 3 § PDL.

Det blir istället GDPR som tillsammans med den svenska lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) blir tillämplig på behandling av personuppgifter för forskningsändamål, förutsatt att behandlingen sker inom ramen för ett verksamhetsställe i Sverige enligt 1 kap. 5 § dataskyddslagen.

Genom utredningen *Personuppgiftsbehandling vid antalsberäkning inför klinisk forskning*[25] finns ett förslag att behandling av personuppgifter som görs på förfrågan för att beräkna hur många personer som uppfyller på förväg uppställda kriterier och därmed kan komma att ingå i forskning inom hälso- och sjukvården, ska vara ett godkänt ändamål enligt PDL.

Enligt förslaget bör sådan antalsberäkning omfattas av begreppet *vetenskapliga forskningsändamål* enligt GDPR. Vårdgivaren, eller den myndighet som bedriver hälso- och sjukvård, föreslås vara den personuppgiftsansvarige för den behandling av personuppgifter som är nödvändig för ändamålet antalsberäkning. Utredningen föreslår med andra ord *inte* att forskningshuvudmannen är den personuppgiftsansvarige för hanteringen av antalsberäkning. Utredningen berör heller egentligen inte den vidare innebörden av att forskningsändamål på sätt och vis introduceras i PDL:s ändamålskatalog genom lagändringen.

Utredningen har i skrivande stund inte utmynnat i en proposition.

3.6.3 Europeiska dataskyddsstyrelsens vägledningar och dess påverkan på klinisk läkemedelsprövning

Den Europeiska dataskyddsstyrelsen[26] (EDPB) är en sammanslutning av nationella tillsynsmyndigheter; däribland den svenska tillsynsmyndigheten Integritetsskyddsmyndigheten. EDPB har till syfte att verka för en enhetlig tillämpning av GDPR inom EU och utfärdar, mot denna bakgrund, bland annat råd, riktlinjer och vägledning. EDPB har utfärdat tre yttranden och riktlinjer som berör klinisk läkemedelsprövning samt forskning på uppgifter om hälsa.

3.6.4 EDPB:s riktlinje 07/2020 v 2.0 om begreppen personuppgiftsansvarig och personuppgiftsbiträde[27]

Genom riktlinje 07/2020 (fastställd som v 2.0), som ersätter den tidigare Artikel 29-arbetsgruppens vägledning 1/2010, har EDPB gett vägledning om begreppen *personuppgiftsansvarig, gemensamt personuppgiftsansvarig och personuppgiftsbiträden* och hur de ska tillämpas.

Denna riktlinje presenterar bland annat ett exempel kring forskning och ett exempel kring kliniska studier och återges i sin helhet nedan. Dessa två exempel har tagits upp i riktlinjen som förenklade scenarion vilka används i ett pedagogiskt syfte att förklara begreppen. Mot den bakgrunden bör försiktighet iakttas vid tolkning av exemplen för att avgöra vilken vägledning som det är möjligt att generalisera utifrån dem. Det kan konstateras att exemplen är översiktligt beskrivna och inte tar hänsyn till alla roller och den komplexitet som detta kan innebära. Vidare nämner exemplen också väldigt översiktligt att ett forskningsprojekt kan innebära flera olika behandlingar men går egentligen inte in något mer på denna fråga. Klart är dock att inriktningen på rekommendationen tydligt verkar röra sig i riktning mot att flera aktörer som är inblandade i ett arbete som på något sätt har ett slutmål med ett delat intresse, det vill säga där samtliga aktörer är investerade i att få ut något av slutresultatet också ska betraktas som att parterna har ett gemensamt personuppgiftsansvar.

[25] SOU 2020:53.
[26] Tidigare den så kallad Artikel 29-arbetsgruppen (”WP29”).
[27] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021 (svensk officiell översättning saknas).

3.6.4.1 Vägledning kring personuppgiftsansvar vid forskning generellt

Example: Research project by institutes

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

Detta exempel tar sikte på flera institut som var för sig har samlat in data som därefter lagras i en gemensam databas. Varje institut har tillgång till lagrad data och är behörig att använda data inom ramen för det gemensamma forskningsändamålet.

Enligt exemplen är instituten gemensamt personuppgiftsansvariga för två behandlingar av personuppgifter: (1) *lagringen* och, (2) *tillhandahållandet* av personuppgifter genom databasen för det gemensamma forskningsändamålet.

För annan behandling av personuppgifter – till exempel den insamling av personuppgifter som föregått lagringen av personuppgifter i databasen – föreligger det enligt exemplet inget gemensamt personuppgiftsansvar. Exemplet utgår från antagandet om att personuppgifterna som lagras i databasen för ett gemensamt forskningsändamål har samlats in i ett tidigare skeende. Vid insamlingsstadiet torde det med andra ord inte finnas ett gemensamt forskningsändamål och personuppgiftsansvaret ligger på den insamlande parten ensamt.

3.6.4.2 Riktlinje kring personuppgiftsansvar vid klinisk läkemedelsprövning specifikt

Example: Clinical Trials[28]

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.

In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial.

Detta exempel tar implicit sikte på klinisk läkemedelsprövning (eftersom det finns en sponsor). Exemplets slutsats är att det är den eller de aktörer som utformar prövningsprotokollet och därmed har avgörande inflytande över hur studien genomförs som normalt är den personuppgiftsansvarige för studien. Som

[28] Av intresse kan nämnas att motsvarande exempel var med även i art 29-gruppens dokument från 2010. Där fastslogs att ”Therefore, it appears that responsibilities are vested in the individual actors. […] Against this background, in this case both trial centres and sponsors make important determinations with regard to the way personal data relating to clinical trials are processed. Accordingly, they may be regarded as joint data controllers.”. Ett något större fokus på gemensamt ansvar således, något som är ganska spännande mot bakgrund av att gemensamt personuppgiftsansvar hade ett betydligt mindre tillämpningsområde innan GDPR.

framgår av EDPB:s yttrande 3/2019 (se avsnitt 3.6.4.3, nedan) ryms flera olika behandlingar av personuppgifterna för olika ändamål inom ramen för klinisk läkemedelsprövning enligt CTR. Det finns därför ett behov av att precisera (1) vilka behandlingar som avses med personuppgiftsansvar för en klinisk studie, och (2) hur riktlinje 07/2020 samspelar med yttrande 3/2019.

Det är värt att poängtera skillnaden mellan detta exempel och exemplet avseende forskning (avsnitt 3.6.4.1, ovan). I exemplet avseende forskning verkar behandlingen av personuppgifter utanför den gemensamma databasen inte anses omfattas av något gemensamt personuppgiftansvar. Gemenskapen ansvarsmässigt verkar alltså fokusera mycket på den gemensamma plattformen. Det finns ett behov av att noggrannare precisera skillnaden mellan de båda exemplen.

För det första: i exemplet avseende klinisk läkemedelsprövning bestämmer *och enas* (engelska: ”determine and agree on”) aktörerna tillsammans om det gemensamma ändamålet. För det andra: aktörerna bestämmer gemensamt de väsentliga medlen för behandlingen i båda exempel (kan ifrågasättas huruvida parterna anses göra det i forskning där parterna endast accepterat ett av parternas IT-system som lämpligt). Dessa två exempel, läst gemensamt, talar därför för att det inte är tillräckligt med endast ett gemensamt ändamål för att det ska råda gemensamt personuppgiftsansvar utan även att alla ingående parter utövar ett inflytande i *fastställandet* av ändamålet, samt i någon grad vid fastställande av medlen.

Vad som närmare avses med att aktörerna ska *enas* (ha ett inflytande i fastställandet) om det gemensamma ändamålet framgår inte. Motsvarande krav finns inte i legaldefinitionen av personuppgiftsansvarig enligt artikel 4.7 GDPR.

Det är också intressant att i exemplet på klinisk läkemedelsprövning anges uttryckligen att det kan tänkas utgöra en personuppgiftsbiträdesrelation om den ena parten endast utför behandlingen, något som inte ens nämns i exemplet forskning.

3.6.4.3 Yttrande 3/2019 om samspelet med den kliniska försöksförordningen och GDPR

Yttrande 3/2019 publicerades av EDPB efter att EU-kommissionen begärt samråd enligt artikel 70.1 b GDPR avseende samspelet mellan CTR och GDPR. Detta yttrande har därför en delvis annan karaktär än riktlinje 07/2020 som är beslutad på grundval av artikel 70.1 e GDPR. Syftet med yttrandet är att ge vägledning till kommissionen i dess arbete snarare än till marknaden/omvärlden medan syftet med riktlinje 07/2020 är att utfärda riktlinjer och rekommendationer för att främja en enhetlig tillämpning av GDPR.

Detta yttrande tar primärt sikte på vad som är den rättsliga grunden för behandling av personuppgifter inom ramen för klinisk läkemedelsprövning. För att kategorisera CTR konstaterar EDPB att personuppgifter behandlas för tre *övergripande* ändamål inom ramen för klinisk läkemedelsprövning:

- **Primär användning**, det vill säga för ändamål som *endast* avser forskning enligt den kliniska läkemedelsprövningens prövningsprotokoll som är det ursprungliga ändamål varför personuppgifterna behandlas.
- **Sekundär användning**, det vill säga för *andra* forskningsändamål än enligt prövningsprotokollet efter att försökspersonen lämnat sitt informerade samtycke.
- **Tillförlitlighets- och säkerhetsändamål**, det vill säga tillförlitlighet för det läkemedel som prövas samt patientsäkerheten för försökspersonen.

Denna struktur utgår från specifika bestämmelser i CTR om kliniska läkemedelsprövningar som ännu inte har trätt i kraft. Motsvarande bestämmelser finns i direktiv 2001/20/EG. Med andra ord: om det finns tre kategorier av ändamål enligt CTR bör dessa tre kategorier av ändamål även kunna härledas ifrån läkemedelslagen och Läkemedelsverkets föreskrift LVFS 2011:19.

3.6.5 Integritetsskyddsmyndighetens förteckning om konsekvensbedömningar

Konsekvensbedömning är en sorts riskanalys som under vissa förutsättningar ska ske enligt artikel 35 GDPR innan en behandling av personuppgifter påbörjas. Inom ramen för en konsekvensbedömning ska en bedömning ske över vilka risker som finns med en behandling utifrån ett dataskyddsperspektiv och hur dessa risker kan minskas. Integritetsskyddsmyndigheten har på grundval av artikel 35.4 GDPR upprättat och offentliggjort en förteckning över behandlingar som *kräver* en konsekvensbedömning avseende dataskydd enligt artikel 35 GDPR.[29] Förteckningen baseras på ett antal kriterier: om två eller fler kriterium är tillämpliga ska en konsekvensbedömning som huvudregel genomföras.

Det är den personuppgiftsansvarige för behandling av personuppgifter som ska genomföra konsekvensbedömningen. Ett personuppgiftsbiträde ska enligt artikel 28.3 f GDPR bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artikel 35 GDPR fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

Enligt denna förteckning ska en konsekvensbedömning genomföras vid följande behandling:

Behandling, innefattande lagring i arkiveringssyfte, av pseudonymiserade känsliga personuppgifter som rör registrerade från forskningsprojekt eller kliniska prövningar. (kriterium 4 och 7).
Verksamheter som samlar in och lagrar känsliga personuppgifter som kan utgöra underlag för urval för framtida forskningsändamål. (kriterium 4 och 7).

Integritetsskyddsmyndigheten ger inget uttalande, explicit eller implicit, om vilken aktör eller vilka aktörer som är personuppgiftsansvarige för behandlingarna, ovan. Exemplen ger dock uttryck för att myndighetens uppfattning är att det sker två typer av behandlingar inom ramen för forskning, en behandling som avser bevarandet av pseudonymiserad information från tidigare forskningsprojekt, en annan som berör insamlandet av känsliga personuppgifter för att utgöra underlag för framtida forskningsändamål. Det senare låter nära beskrivningen av det så kallad Life-gene-projektet för vilken en särskild, tillfällig lagstiftning finns inrättad.[30] Det som är av intresse här är att Integritetsskyddsmyndigheten skiljer på dessa två typer av verksamheter, vilket också tyder på att de är att betrakta som två olika typer av behandlingar.

[29] Integritetsskyddsmyndigheten: Förteckning enligt artikel 35.4 Dataskyddsförordningen (2019-01-16), dnr DI-2018-13200.
[30] Se Lag (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa.

4 Metod för fastställande och fördelning av personuppgiftsansvaret

Personuppgiftsansvaret utgår från den aktör som har ett bestämmande inflytande över ändamålen och medlen för behandlingen av personuppgifter. Det **första steget** är därför att kartlägga *den aktuella behandlingen* eller behandlingarna. Det **andra steget** är att därefter bedöma och fastställa personuppgiftsansvaret. Det **tredje steget** är att dokumentera och reglera personuppgiftsansvaret.

Det har återkommande av tillsynsmyndigheter upprepats att det är de faktiska omständigheterna i det enskilda fallet som är avgörande för bedömningen av vem som är personuppgiftsansvarig.[31] Det är alltså inte av avgörande betydelse vad som avtalats eller vad som typiskt sätt gäller för en viss relation utan det krävs att en analys görs av de faktiska omständigheterna i det enskilda fallet.

En viktig aspekt är att göra en analys av vem som faktiskt är den part som bestämmer över själva ändamålet med behandlingen. Det är *bestämmanderätt* över ändamålen som är den mest avgörande faktorn för fördelningen. I komplicerade behandlingssituationer är det nödvändigt att gå systematiskt tillväga utifrån en arbetsmetod för att genomföra en korrekt bedömning. Varje bedömning om personuppgiftsansvar bör dokumenteras, samtliga fall där flera aktörer är inblandade i en behandling bör avtalas, även om det endast är personuppgiftsansvarig-personuppgiftsbiträde-förhållandet där det direkt i GDPR framgår ett krav på avtal.

4.1 Steg ett: Vad är den aktuella behandlingen/behandlingarna

I steg ett identifieras och kartläggs en viss ”faktisk behandling”, det vill säga en åtgärd eller en kombination av åtgärder som sker för samma ändamål.[32] För att kunna utföra identifieringen krävs information om i vart fall: a) ändamålet (varför behandlingen ska utföras), b) vilka personuppgifter som behandlas, och c) vilka aktörer som är involverade i åtgärderna.

4.1.1 Vilka behandlingar sker inom klinisk läkemedelsprövning?

Såsom konstaterats ovan (se avsnitt 3.6.4.2, ovan) har klinisk läkemedelsprövning ansetts bestå av i vart fall tre olika behandlingar.

- Ändamålet som avser endast forskningen enligt prövningsprotokollet.
- Ändamålet och den behandling som kan komma att följa avseende andra forskningsändamål än det enligt prövningsprotokollet.
- Den behandling som krävs för tillförlitlighet och säkerhet och som innebär att resultaten bevaras för att senare kunna verifieras.

Utifrån ett hälso- och sjukvårdsperspektiv tillkommer en fjärde behandling:

- Behandling som vårdgivaren utför genom att de ger en intervention till en patient och de journalanteckningar som måste ske i anledning av detta inom ramen för uppdraget som vårdgivare.

Således torde vanligtvis en klinisk läkemedelsprövning bestå av i vart fall dessa fyra behandlingar. Det kan konstateras att dessa behandlingar inte omfattar någon uttrycklig process för insamling av forskningsunderlaget. Vår bedömning är att denna del bör anses omfattas av den första punkten.[33]

[31] Se bl.a. Integritetsskyddsmyndigheten beslut 2010-07-02, dnr 686-2010, beslut 2012-04-18, dnr 811-2011).
[32] Enligt artikel 4 GDPR.
[33] Det är EDPB som gjort bedömningen av förekommande behandlingar genom sitt yttrande i 3.6.4.3 ovan. Vi har valt att behålla uppdelningen och ser den även enligt detta resonemang som en logisk följd av de kliniska läkemedelsprövningarnas process.

4.1.2 Vilka behandlingar sker inom klinisk forskning?

Vad avser klinisk forskning finns inte samma tydliga lagstiftning som för klinisk läkemedelsprövning utifrån vilken det är möjligt att bedöma vilken personuppgiftsbehandling som genomförs. Det kan dock antas att i de flesta fall består processen av följande behandlingar:

- Ändamålet och den behandling som sker genom insamlandet av forskningsunderlag, till exempel i form av dokumentation vid provtagning, klinisk undersökning, enkäter eller i annan form av insamling av dataunderlag (så kallad registerforskning).
- Ändamålet i form av analysen av underlaget för att bekräfta eller falsifiera det forskningsprojektet beskrivna hypoteserna.
- Ändamålet och den behandling som krävs för tillförlitlighet och säkerhet vilken innebär att resultat bevaras för att senare kunna verifieras.
- Ändamålet och den behandling som kan komma att följa avseende andra forskningsändamål än det aktuella forskningsprojektet.

Utifrån ett hälso- och sjukvårdsperspektiv kan det anmärkas att ytterligare en behandling tillkommer:

- Behandling som vårdgivaren utför för det fall inhämtande av underlaget innebär att vårdgivaren samtidigt behandlar en patient genom en vårdinsats och de journalanteckningar som i så fall ska föras i anledning av detta.

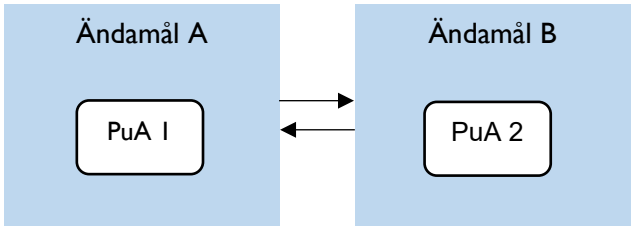
4.2 Steg två: Bedöma och fastställa personuppgiftsansvar för behandlingen

När ett antal behandlingar har definierats (se avsnitt 4.1 ovan), ska för varje behandling fastställas vilken organisation som är personuppgiftsansvarig.

Så fort fler än en aktör är inblandad i en samordnad behandling av personuppgifter och utbyter person-uppgifter med varandra blir det aktuellt att utreda om något av följande scenarion föreligger: (**Situation A**) ett utlämnande sker mellan två ”självständigt” personuppgiftsansvariga (var och en är alltså ensidigt ansvarig för sin respektive behandling), (**Situation B**) en behandling som är samordnad på så sätt att det finns ett gemensamt syfte och därigenom gemensamt personuppgiftsansvar, eller (**Situation C**) att en part bestämmer ändamålet med behandling på så sätt att en annan aktör inte har någon bestämmanderätt utan endast utför en behandling av personuppgifter på uppdrag av den andre parten.

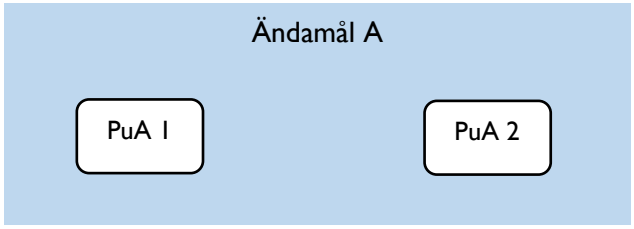
Situation A - Separata PuA

Personuppgiftsansvariga (”**PuA**”) med olika ändamål och samordnad behandling som innebär ett utlämnande genom överföring.



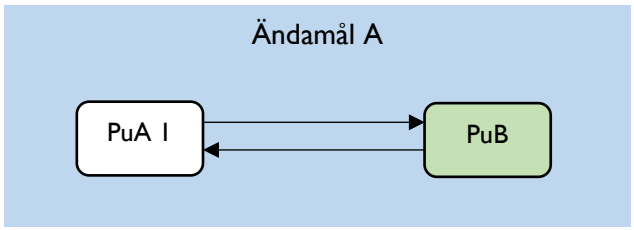
Situation B – Gemensam PuA

Gemensamt personuppgiftsansvar.



Situation C – PuA - PuB

En ensamt personuppgiftsansvarig med personuppgiftsbiträde (”**PuB**”).



Även om den ovan beskrivna modellen ser konkret och enkel ut att tillämpa är det inte alltid det framstår som självklart vilken av de tre situationerna det är som föreligger. Erfarenhetsmässigt har det också visat sig att bedömningar av personuppgiftsansvar ofta är komplexa att göra, särskilt när flera aktörer är inblandade i samarbeten där det inte är helt tydlig att en av parterna uppdragit åt den andre att utföra något.

Denna rapport har i avsnitt 3 och 4, ovan, redovisat de kriterier och bedömningsgrunder som ska ligga till grund för en bedömning av personuppgiftsansvaret. Ett schematiskt flödesschema återfinns i bilaga 1 som kan användas som modell för hur en bedömning av personuppgiftsansvar kan ske.

När bedömningen är mer komplicerad eller omfattande bör istället frågorna som följer nedan användas för att dokumentera den bedömning som genomförs avseende respektive behandling. Frågorna, med hjälptext i kursivt, är utformade för att systematiskt dokumentera vilken av parterna inblandade i en personuppgiftsbehandling som har störst inflytande i olika delar före, under och efter behandlingen. Frågorna har utformats mot bakgrund av den lagstiftning som gäller, de rekommendationer som givits av olika organ och praxis i övrigt.

Aktiviteter före behandlingen

i. Vilken/vilka aktör är det som kommer på idén med hanteringen?

Här ska återknytas vill vad EDPB skrivit om att vid gemensamt personuppgiftsansvar ska aktörerna enas om det gemensamma ändamålet med behandlingen. Båda parter bör alltså ha ett inflytande annars torde tendensen vara att personuppgiftsvaret inte ska betraktas som gemensamt.

ii. Vilken/vilka av aktörerna är det som har förberett och planerat för projektet?

Den som bedriver själva arbetet kan vara den som förfogar över personuppgiftsansvaret, men det torde inte vara ovanligt att sådant arbete läggs ut på en annan part som har särskilda kvalifikationer vad gäller planering och/eller genomförande.

iii. Vem/vilka är aktiv och beslutsför när det gäller förberedelserna för behandlingen?

Mycket talar för att den organisation som faktiskt initierar och tillför idématerialet till ett projekt också är den som förfogar över ansvaret.

iv. Vilken/vilka aktör är det som har beslutat om att projektet/hanteringen faktiskt igångsätts?

Den som faktiskt beslutar att ett projekt ska lämna planeringsstadier och faktiskt sättas igång torde i många fall vara den som förfogar över ansvaret.

Aktiviteter under behandlingen

i. Vem/vilka initierar avtal/uppdrag med andra parter som ska bidra till projektet?

När andra aktörer ska vidta åtgärder eller understödja vid hanteringen så är det normalt den aktör som har ett huvudansvar som har att initiera sådana uppdrag. Det är också bara en personuppgiftsansvarig som kan ge ett personuppgiftsbiträde i uppdrag att behandla personuppgifter. Den aktör som initierar och ingår uppdrag/avtal med andra aktörer är därmed ofta den som förfogar över ansvaret.

ii. Vem/vilka bestämmer över och inför säkerhetsåtgärder i hanteringen?

Här ska påpekas att säkerhetsåtgärder närmare utformning i och för sig anses vara sådana beslut som även ett biträde kan ta. Det är således inte av avgörande betydelse vem som har beslutar kring detta. Det kan dock vara av intresse att titta närmare på vem som faktiskt bestämmer att en säkerhetsåtgärd inte måste vidtas, alltså den som beslutar över vilket risktagande som är acceptabelt i anslutning till behandlingen.

iii. Vem/vilka är den som har att hantera ett eventuellt problem som uppstår?

Den aktör som faktiskt agerar när ett problem eller incident uppstår har ofta ansvaret för hanteringen i stort. Med detta menas inte i första hand agerar i den mening att incidenten uppmärksammas utan den som tar ställning till incidenten, verifierar den och bedömer på vilket sätt den ska hanteras (och ev. rapporteras)

iv. Vem/vilka beslutar att införa någon förändring i processen?

När det av någon anledning finns orsak till att förändra någon del av processen tar en part ett initiativ till detta och beslutar även om att förändring ska ske. Den som faktiskt beslutar om sådana förändringar är ofta den som förfogar över ansvaret.

v. Vem/vilka informerar den registrerade om behandlingen och dennes rättigheter?

Vem är det som lokaliserar den registrerade och samlar in dennes personuppgifter? Vem uppsöker den registrerade för att inhämta ett samtycke? Vem tar ställning till att samtycket är korrekt? Den som utför det aktiva uppsökandet av registrerade kan vara den som förfogar över ansvaret, men kan också göra det på uppdrag av denne.

vi. Till vem/vilka vänder sig den registrerade med frågor?

Vem är kontaktpunkt för registrerade som ingår i projektet? Till vem är det registrerade vänder sig för att ställa frågor kring behandlingen av personuppgifter? Den som uppträder som representant på detta sätt förfogar ofta över ansvaret.

vii. Vem/vilka är det som faktiskt har att besluta om den registrerades rättigheter (till exempel begäran om radering)?

Den som faktiskt bedömer huruvida en registrerad har rätt till att utverka en viss rättighet och vilken åtgärd som ska utföras är ofta den som förfogar över ansvaret.

Aktiviteter efter behandlingen

i. Vem/vilka tar del av resultaten från projektet och omsätter detta i vinst/vidareutveckling/ publicering/annan aktivitet?

Den som faktiskt skördar resultatet och har möjlighet att omsätta detta i sin egen verksamhet är ofta den som förfogar över ansvaret. Det här ska inte misstas för den aktör som erhåller ekonomisk ersättning för det arbete denne lagt ner i ett projekt. En sådan förtjänst säger ofta inte mycket om vem som förfogar över ansvaret.

ii. Vem/vilka kommer att hantera personuppgifterna som kvarstår efter att projektet har avslutats?

Den som har fortsatt ansvar för hanteringen av informationen efter att själva projektet har slutförts är den som har det långsiktiga ansvaret och kan ofta vara den som även förfogar över ansvaret under pågående projekt. Notera dock att detta också kan vara något som sker på uttryckligt uppdrag från den som faktiskt innehar ansvaret.

iii. Vem/vilka ansvarar för att radera/avidentifiera de personuppgifter som ska gallras?

Den aktör som faktiskt ser till att lagringsprincipen tillämpas och att personuppgifter inte behandlas längre tid än nödvändigt är ofta den som också förfogar över ansvaret under pågående projekt.

Bestämmande av personuppgiftsansvar

När frågorna har gåtts igenom och svaren dokumenterats bör det vara betydligt enklare att erhålla en överblick över vilken eller vilka av parterna som har ett betydande inflytande över behandlingen av personuppgifterna. Detta underlag kommer då också kunna utgöra ett beslutsunderlag för om en av parterna ensamt är personuppgiftsansvarig, om det finns ett gemensamt ansvar, eller om var och en av parterna har ett eget personuppgiftsansvar som inte är gemensamt (se situationer A, B, C i avsnitt 4.2 ovan). Vid bedömningen av om personuppgiftsansvaret är gemensamt eller om det är var och en som har ett eget ansvar bör särskilt beaktas om ändamålen och medlen framkommer i samförstånd mellan parterna. Det torde alltså krävas att samtliga parter har ett utrymme att påverka besluten. Däremot krävs inte att samtliga parterna är lika aktiva i den praktiska behandlingen, om ens aktiva alls.

Nedan i avsnitt 5 följer en analys av personuppgiftsansvarets placering för vart och ett av de scenarier som varit utgångspunkten för rapporten.[34]

[34] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.

5 Genomgång av scenarion

Här bedöms personuppgiftsansvarig strukturerat utifrån ett givet forskningsscenario.

5.1 Klinisk läkemedelsprövning, singelcenter – prövarinitierad

5.1.1 Scenariobeskrivning

Forskningstyp:	• Klinisk läkemedelsprövning, kräver tillstånd av Läkemedelsverket och Etikprövningsmyndigheten.
Aktörer:	• Det är samma aktör (en vårdgivare) som är sponsor och huvudansvarig forskningshuvudman.
Prövare: **(en prövare är en fysisk person)**	• Ansvarig prövare är anställd av vårdgivaren. Prövaren kan ha en kombinationstjänst och samla in och/eller utföra delar av analysen vid en akademisk institution vilket kan påverka personuppgiftsansvaret då flera organisationer blir inblandade i behandlingen.
Singel- eller multicenter:	• Singelcenter.
Kommentar:	• Sponsorn ansöker om tillstånd från Läkemedelsverket, medan prövaren (fysisk person) ansöker till Etikprövningsmyndigheten i egenskap av representant för huvudansvarig forskningshuvudman. I detta scenario är sponsor och den organisation prövaren representerar samma juridiska person.

5.1.1.1 Illustration av scenario 5.1

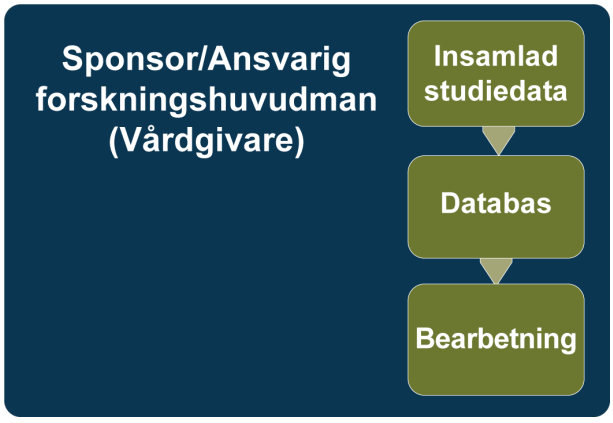


Bild 5.1a. Datainsamling, databasens placering, samt databearbetning (som till exempel analys) sker inom samma huvudman.

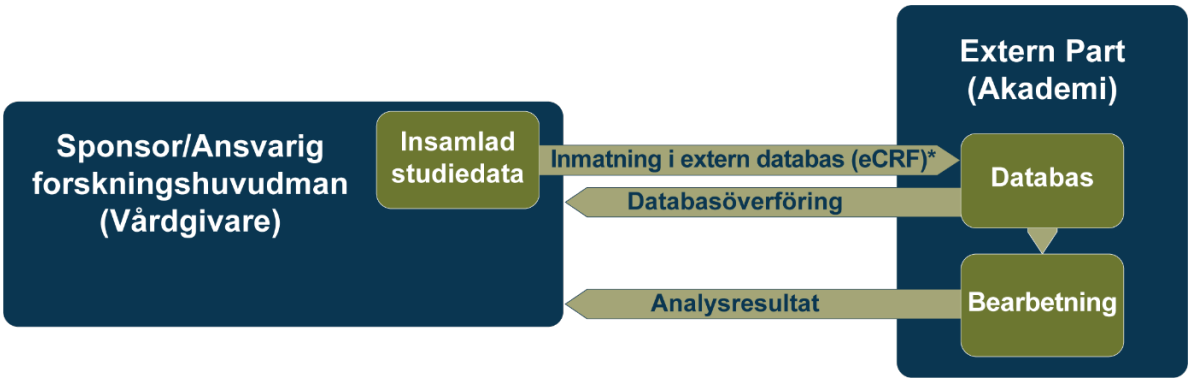


Bild 5.1b: Datainsamling och databasens placering, samt databearbetning (som till exempel analys) sker inom olika huvudmän. Slutgiltig databas bör alltid återföras till Sponsor/Ansvarig forskningshuvudman. *överföring bör ske kodat/ pseudonymiserat.

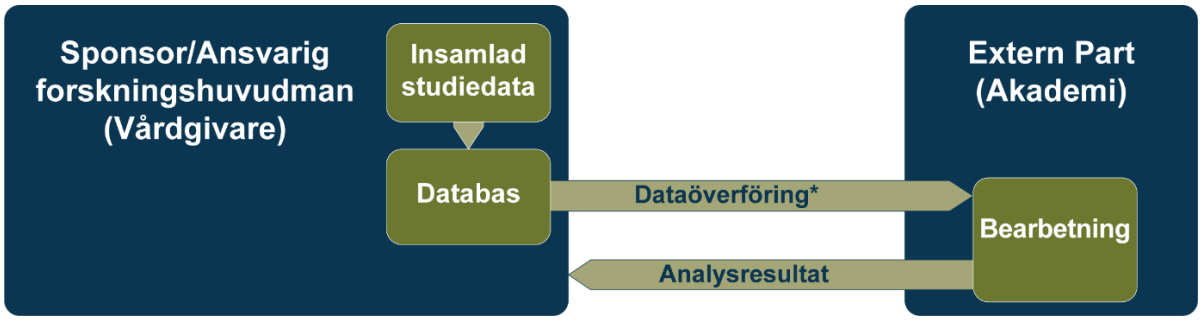


Bild 5.1c: Datainsamling samt databasens placering och databearbetning (som till exempel analys) sker inom olika huvudmän. *överföring bör ske kodat/ pseudonymiserat.

5.1.2 Personuppgiftsansvarets fördelning

Hälso- och sjukvård samt forskning utgör två separata verksamhetsgrenar hos vårdgivare. Klinisk läkemedelsprövning förutsätter deltagande av hälso- och sjukvård i de fall prövningen utförs avseende patienter.

Behandling av personuppgifter som sker inom ramen för hälso- och sjukvård omfattas av PDL. En vårdgivare är alltid personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför enligt PDL. En myndighet som bedriver hälso- och sjukvård är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgifter inom hälso- och sjukvården får behandlas för de ändamål som listas i den uttömmande ändamålskatalogen i 2 kap. 4 § PDL. Att en patientjournal bland annat är en informationskälla för forskning framgår av 3 kap. 2 § andra stycket PDL. Syftet med en patientjournal är dock i första hand att bidra till en god och säker vård av patienten.

I detta forskningsscenario förekommer endast en organisation (se dock avsnittet Akademisk institution, nedan). Det är således denna organisation som är personuppgiftsansvarig. Notera dock att det rör sig om olika behandlingar med olika ändamål vilket innebär att det inom organisationen kan finnas olika aktörer som har det organisatoriska ansvaret (till exempel en forskningsenhet som är skild från verksamhetsområdet vård). Det innebär också att det normalt förekommer sekretess mellan dessa skilda verksamhetsområden. En eventuell överföring av information från den ett verksamhetsområde till ett annat kan därför behöva föregås av en sekretessprövning och ett formellt beslut om utlämnande.

Personuppgiftsansvarig: Vårdgivaren, tillika forskningshuvudmannen, är personuppgiftsansvarig för samtliga behandlingar.

Akademisk institution

I vissa fall kan prövaren (som alltid är en fysisk person) ha en kombinationstjänst och samla in och/eller utföra delar av analysen vid en akademisk institution. Anledningen till detta kan vara flera olika, till exempel att forskningshuvudmannen saknar särskilda IT-verktyg eller att den akademiska institutionen helt enkelt förfogar över bättre tekniska förutsättningar att hantera eller analysera stora datamängder. I dessa situationer blir det viktig att avgöra vilken roll prövaren har och vilken organisation denne representerar när den utför sin uppgift som prövare.

Om den akademiska institutionen endast tillhandahåller tekniska verktyg som prövaren kan nyttja i forskningen ter det sig naturligt att se institutionen som ett *personuppgiftsbiträde*. Det är i sådant fall också viktigt att etablera huruvida den akademiska institutionen tar på sig denna roll och det ansvar det innebär eller om det helt enkelt bara är så att prövaren valt att använda sig av de verktyg som finns tillgängliga för denne genom sin anställning vid akademin utan att institutionen godkänt det. Det torde vara av stor betydelse att personuppgifter hanteras på ett strukturerat och medvetet sätt och att rutiner och riktlinjer klargörs mellan parterna så att ansvariga representanter för båda organisationerna tydliggör vilken hantering som faktiskt är avsedd och att relevanta avtal kan ingås mellan behöriga representanter för respektive organisation.

Det kan naturligtvis förekomma situationer där den akademiska institutionen har en mer avgörande roll än enbart att tillhandhålla en teknisk infrastruktur för att hantera forskningsdata, det får då sker en bedömning från fall till fall vilken part som är personuppgiftsansvarig. Även i dessa situationer är det dock av yttersta vikt att institutionens vilja tydliggörs och att bedömningen inte enbart utgår ifrån vad prövaren med kombinationstjänst har för uppfattning.

5.1.3 Behov av avtal

I de fall det inte förekommer något personuppgiftsbiträde i scenariot finns det inget i lag angivet krav på något avtal i detta scenario, däremot bör det finnas en dokumenterad process för hanteringen av informationsflödet särskilt då informationen ska passera sekretessgränser mellan verksamhetsgrenar (såsom vård → forskning).

I det fall prövaren samlar in/analyserar data vid en akademisk institution såsom beskrivits ovan i exempel b) och c) och ett personuppgiftsbiträdesförhållande därmed uppstår finns det ett absolut krav om att ett personuppgiftsbiträdesavtal (PUB-avtal) upprättas i enlighet med GDPR, som närmare reglerar personuppgiftsbiträdets behandling av personuppgifter. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna. Det kan vara på sin plats att påpeka att det inte är nödvändigt med ett personuppgiftsbiträdesavtal i samband med varje enskild kliniskt forskningsprojekt. Ett mer allmänt avtal mellan en akademisk institution och en vårdgivare kan mycket väl ingås där även hantering av personuppgifter i framtida forskningsprojekt regleras.

5.2 Klinisk läkemedelsprövning, singelcenter – industriinitierad

5.2.1 Scenariobeskrivning

Forskningstyp:	• Klinisk läkemedelsprövning, kräver tillstånd av Läkemedelsverket och Etikprövningsmyndigheten.
Aktörer:	• Industriinitierad läkemedelsprövning med endast en forskningshuvudman. Sponsor är industrin och en annan aktör (en vårdgivare) är huvudansvarig forskningshuvudman.
Prövare: **(en prövare är en fysisk person)**	• Ansvarige prövare är anställd av vårdgivaren.
Singel- eller multicenter:	• Singelcenter.
Kommentar:	• Sponsorn ansöker om tillstånd från Läkemedelsverket, medan prövaren (fysisk person) ansöker till Etikprövningsmyndigheten i egenskap av representant för huvudansvarig forskningshuvudman. När Förordningen för klinisk läkemedels-prövning (CTR) kommer att börja gälla kommer det vara en gemensam ansökan till de två myndigheterna som sponsorn ansvarar för att skicka in (för forskningshuvudmannens räkning). • I uppdragsforskning (industriinitierad) genomför prövaren studier för att leverera data till sponsorn för analys. Hypotesen med forskningen har genererats av sponsorn (till exempel om läkemedel A är bättre än läkemedel B). Studien genomförs sedan för att stödja eller förkasta denna hypotes. Det kan förekomma att prövaren är med och tar fram protokollet för studien. Det kan i detta fall också förekomma att prövaren då är med på publikationen av resultatet i medicinsk tidskrift. • Ansvarig prövare ska spara en kopia av den data som prövningsstället har genererat åt sponsor för ändamålet att kunna inspektera och rekonstruera prövningen. Samtliga insamlade data finns i pseudonymiserad (kodad) form hos sponsorn.

5.2.1.1 Illustration av scenario 5.2

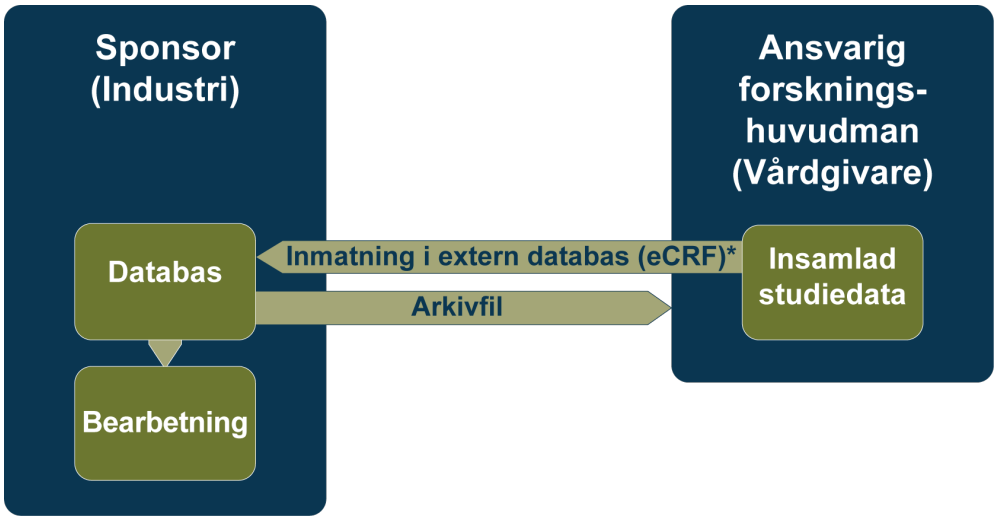


Bild 5.2: Datainsamling och databasens placering, samt databearbetning (som till exempel analys) sker inom olika huvudmän. En kopia av forskningshuvudmannens data, ”arkivfil”, ska återföras för arkivering. *överföring bör ske kodat/ pseudonymiserat.

5.2.2 Personuppgiftsansvarets fördelning

Uttrycklig behörighet

Det saknas författningsreglering som ger någon av parterna en uttrycklig behörighet avseende personuppgiftsansvar. I Läkemedelsverkets föreskrifter och CTR[35] definieras sponsorn som den som är huvudsakligen ansvarig för den kliniska läkemedelsprövningen, men regleringen saknar ett uttryckligt utpekade vad gäller just personuppgiftsansvaret. Vad gäller behandlingen av personuppgifter som sker för att journalföra den behandling som ges till patienter framgår dock av PDL att det är den vårdgivare som vårdar patienten som är personuppgiftsansvarig för de uppgifter som dokumenteras avseende vården av patienten.[36]

Underförstådd behörighet

Vad avser underförstådd behörighet kan konstateras att det finns en etablerad branschpraxis på området att sponsorn vid industriinitierade studier i de allra flesta fall är den som ensamt arbetat med och tagit fram ett protokoll för studien. Protokollet som studien utförs efter dikterar i princip uttömmande vilka typer av personuppgifter som ska samlas in och på vilket sätt de ska dokumenteras. Även om prövaren har ett utrymme att själv hantera rekryteringen av de fysiska personer som ska ingå i studien måste dessa vara representanter för den studiepopulation som protokollet ställer upp. I praktiken torde således prövarens utrymme för egna beslut vara begränsat.

Det kan också konstateras att det i EDPB:s riktlinjer har rekommenderats att såväl sponsor som prövare kan ha ett gemensamt personuppgiftsansvar, men att det kan förekomma fall där sponsor har ett så pass stort inflytande att det är sponsor som är att betrakta som personuppgiftsansvarig medan prövaren endast agerar på uppdrag av denne, då i egenskap av personuppgiftsbiträde. [37]

---

[35] *LVFS 2011:19 1 kap. 3 § m.*, kommande *artikel 2.14 CTR*.
[36] PDL 2 kap 6 §.
[37] Se avsnitt 3.6.4 ovan (EDPB:s riktlinje 07/2020 v 2.0 om begreppen personuppgiftsansvarig och personuppgiftsbiträde).

Den underförstådda behörigheten som återfunnits på området pekar därmed mot att sponsor är personuppgiftsansvarig för personuppgifterna som behandlas i läkemedelsprövningen och att det i vissa fall kan förekomma ett gemensamt personuppgiftsansvar tillsammans med prövare.

Faktiskt inflytande

Vid bedömning av faktiskt inflytande ska ställning tas till de faktiska omständigheterna. Så har skett genom ett antal workshops inom ramen för framtagande av denna rapport.[38]

Sammanfattningsvis har följande konstaterats:
Prövaren har ett väldigt begränsat inflytande över de egentliga ramarna för varför och hur personuppgifterna ska behandlas. Även om prövaren är den som så att säga arbetar närmast de registrerade, tillika forskningspersonerna, och är den som har kontakten med dessa så sker allt sådant arbete utifrån de strikta rutiner som protokollet anvisar.

Vad gäller intresse och nytta av slutprodukten av personuppgiftsbehandlingen så är det vanligtvis endast sponsorn som tar del av detta dels i den rent affärsmässiga vidare hanteringen av en marknadsetablering av ett eventuellt läkemedel, och dels i den eventuella publicering som sker av studien i medicinsk facklitteratur. Det förekommer förvisso att även prövaren medverkar i en sådan publikation, det sker främst när prövaren även deltagit aktivt i framtagandet av protokollet. Dessa fall sker som regel endast undantagsmässigt och är främst då prövaren är en person med särskild sakkunskap eller är en ledande forskare inom området och kring den specifika medicinska frågeställningen.

Det har vidare konstaterats att prövaren i ett flertal situationer har en direkt eller indirekt förpliktelse att rapportera förändringar eller händelser kring behandlingen av personuppgifter till sponsor. Det är i de allra flesta förekommande fall sponsorn som har det avgörande beslutet i hur prövaren eventuellt ska agera utifrån händelsen.

Prövaren är den som praktiskt utför de studiespecifika momenten och dokumenterar all data. Inom ramen för denna roll är det också prövaren som därmed har att fatta en mängd beslut om säkerheten kring utförandet. Det är förvisso så att både sponsorn och prövaren har ett mandat och ansvar att agera, men vad avser prövaren är det i mångt och mycket endast inom ramen för sin egen sfär som prövaren beslutar något. Exempel på beslut som prövaren fattar är hur kontakt och rekrytering av försökspersonen ska genomföras samt detaljerna kring hur prövningen ska genomföras lokalt. Detta ter sig dock sammantaget vara detaljer som utfyller den övergripande planen som sponsorn tagit fram och som prövaren inte heller har mandat att avvika ifrån, annat än om det avser försökspersonens omedelbara säkerhet. Det ter sig därför sammantaget inte som att prövaren är involverad i framtagandet av den övergripande planen och därmed inte heller över ändamålen för behandlingen och i väldigt liten del över medlen med desamma.

Särskilt om bevarande av data

Ett särskilt fokus är de personuppgifter som bevaras för framtiden för att resultaten senare ska kunna verifieras. Det bör här tydliggöras att detta bevarande sker för just ändamålet tillförlighet och säkerhet kring läkemedelsprövningen. Det finns således inget annat ändamål med bevarandet som prövaren bestämmer över. Denna behandling sker i likhet med övriga medel utifrån vad som är föreskrivet i sponsorns protokoll. Det är sponsorn som (utifrån de ramar lagstiftning ger) avgör under hur lång tid data ska bevaras. Under denna bevarandetid har prövaren inte någon given rätt att behandla uppgifterna för andra ändamål. Det ter sig sammantaget som att bevarade personuppgifter bevaras på uppdrag av sponsorn och att det således är denne som är personuppgiftsansvarig för dessa. Att sponsorn inte har direktåtkomst till personuppgifterna förändrar inte denna bedömning. Det har i domstolspraxis fastslagits att personuppgiftsansvarig inte behöver ha åtkomst till de personuppgifter som behandlas, se avsnitt 3.3, ovan. När bevarandet för ändamålet uppföljning är slutfört innebär det att det inte längre finns någon grund för att fortsatt bevara personuppgifter. Personuppgifterna ska då gallras eller arkiveras i enlighet med personuppgiftsbiträdets bevarande- och gallringsinstruktioner. Notera då även att personuppgiftsansvarig enligt

[38] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.

artikel 28.3 g GDPR ska lämna instruktioner i PUB-avtalet om vad som ska ske med personuppgifterna vid uppdragets slutförande.

Monitorering (kvalitetskontroll) fungerar på så sätt att sponsorn gör uppföljningar för att kontrollera att källdata överensstämmer med de uppgifterna som överförts till sponsorn. Sponsorn har inte tillgång till källan och måste därför anlita en monitor som utför denna kontroll. Monitorering torde inte innebära några andra ställningstaganden kring personuppgiftsansvar. För det fall som monitorering sker av ett externt bolag kan det förvisso finnas ett personuppgiftsbiträdesförhållande med detta externa bolag, men det faller utanför ramen för den aktuella bedömningen.

Prövare i förhållande till forskningshuvudmannen

Något som bör beröras i samband med detta är det faktum att regelverket definierar prövaren som en fysisk person medan personuppgiftsansvaret normalt faller på en juridisk person. Forskningshuvudmannen i ansökan till Etikprövningsmyndigheten är också alltid en organisation i motsats till en fysisk person. Denna diskrepans mellan regelverket för läkemedelsprövningar och personuppgiftsbehandling bedöms dock i praktiken inte ha någon avgörande betydelse. Det torde i alla situationer där den fysiske personen (prövaren) agerar å sin arbetsgivares vägnar och i egenskap av anställd innebära att det är arbetsgivaren, det vill säga den juridiska personen, vårdgivaren, som prövaren är verksam inom som också tar på sig ansvaret enligt GDPR, antingen som personuppgiftsbiträde eller personuppgiftsansvarig.

Personuppgiftsansvarig: Sponsor bedöms vara personuppgiftsansvarig för merparten av de behandlingar som sker inom ramen för en industriinitierad prövning. I de allra flesta fallen torde sponsor även vara ensam personuppgiftsansvarig för dessa behandlingar och prövare (den juridiske person som prövaren är anställd hos) anses agera på uppdrag av sponsorn i kapacitet av ett personuppgiftsbiträde.

Det bör beaktas att det finns situationer som kan tyda på att både sponsor och prövare agerar tillsammans och i samförstånd och därigenom har ett gemensamt personuppgiftsansvar. Detta torde främst förekomma i de fall där prövare är involverad i ett tidigt skede i processen, aktivt deltagit i framtagande av protokoll och sedermera även i publikationer. Här bör en bedömning dock ske utifrån vilken egenskap prövaren gör detta; är prövaren (den fysiske personen) i denna situation en representant för forskningshuvudmannen (vårdgivaren) eller deltar prövaren i framtagning av protokoll i rollen som konsult på uppdrag av sponsorn? Det senare (prövaren i en konsultkapacitet) skulle tyda på att personuppgiftsansvaret även i denna situation tillkommer sponsorn ensamt.

Personuppgiftsansvar inom ramen för vårdgivares journalföring

Notera att den personuppgiftsbehandling som sker för ändamålet att journalföra den vård i form av medicinsk behandling som skett på patienter och som utförs av prövaren i egenskap av vårdgivare regleras särskilt i 2 kap. 6 § PDL. Denna hantering (journalföring) är således vårdgivaren (dvs. prövarens arbetsgivare) ensamt personuppgiftsansvarig för.

5.2.3 Behov av avtal

Utgör behandlingen en konstellation där sponsorn anses vara personuppgiftsansvarig och prövaren endast personuppgiftsbiträde krävs enligt GDPR ett personuppgiftsbiträdesavtal (”PUB-avtal”) som närmare reglerar personuppgiftsbiträdets behandling av personuppgifter. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna.

Görs bedömningen att det istället handlar om ett gemensamt personuppgiftsansvar kräver GDPR att det finns ett ”inbördes arrangemang”. Det torde vara mycket lämpligt, men inte strikt tvingande, att detta arrangemang regleras genom ett skriftligt avtal om gemensamt personuppgiftsansvar mellan parterna där det närmare framgår vem som har att hantera vilken del av personuppgiftsansvaret. För mer information om arrangemanget se avsnitt 3.3, ovan.

5.3 Klinisk läkemedelsprövning, multicenter – prövarinitierad

5.3.1 Scenariobeskrivning

Forskningstyp:	• Klinisk läkemedelsprövning, kräver tillstånd av Läkemedelsverket och Etikprövningsmyndigheten.
Aktörer:	• Det är samma aktör (en vårdgivare) som är sponsor och huvudansvarig forskningshuvudman. Prövningen innefattar även en eller flera andra deltagande kliniker från andra forskningshuvudmän (vårdgivare) eftersom det är en multicenterstudie.
Prövare: **(en prövare är en fysisk person)**	• En koordinerande prövare arbetar under den huvudansvariga forskningshuvudmannen. Vid de andra medverkande forskningshuvudmännen finns ansvariga prövare.
Singel- eller multicenter:	• Multicenter.
Kommentar:	• I detta scenario är sponsor och huvudansvarig forskningshuvudman samma juridiska person. Den av forskningshuvudmännen som har ansvaret att ansöka om etikprövning, är även den som vanligtvis ansvarar för att koordinera alla medverkande forskningshuvudmän, samt ansvaret för att ansöka om tillstånd från Läkemedelsverket. • I prövarinitierad forskning är det vanligt att alla/eller en del av de ansvariga prövarna är delaktiga i framtagandet av det protokoll som styr prövningen. Särskilt den koordinerande prövaren men även övriga ansvariga prövare är således delaktiga på ett helt annat sätt jämfört med en industriinitierad prövning. Vanligtvis är prövare då också delaktiga i publikationen av forskningsresultaten. • I multicenterstudier är det flera prövare/kliniker involverade, dvs flera forskningshuvudmän. Det är en juridisk person som är forskningshuvudman även om en prövare enligt definition i lagstiftning är en fysisk person. • Ansvariga prövare ska spara en kopia av den data som prövningsstället har genererat för ändamålet att kunna inspektera och rekonstruera prövningen. Slutresultatet av samtliga insamlade data finns i pseudonymiserad (kodad) form hos sponsorn.

5.3.1.1 *Illustration av scenario 5.3*

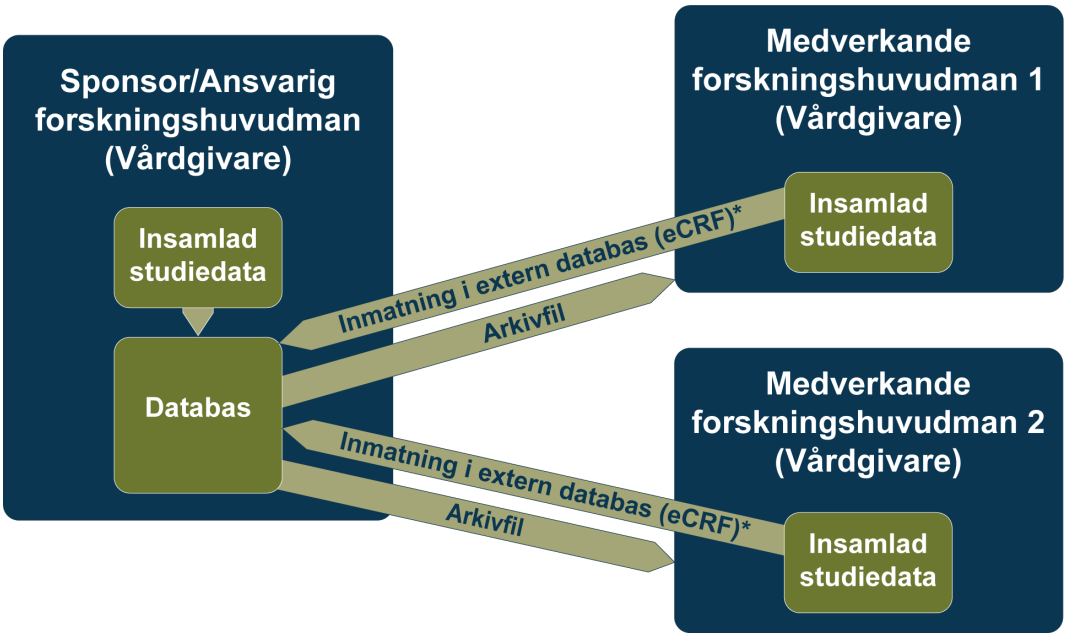


Bild 5.3: Datainsamling sker hos flera olika huvudmän. Databasens placering, samt databearbetning (som till exempel analys) kan förekomma hos olika huvudmän, men vanligen hos sponsorn, och slutgiltig databas bör alltid återföras till sponsor. En kopia av forskningshuvudmannens data, ”arkivfil”, ska återföras för arkivering. *överföring bör ske kodat/ pseudonymiserat.

5.3.2 Personuppgiftsansvarets fördelning

Uttrycklig behörighet

Det saknas författningsreglering som ger någon av parterna en uttrycklig behörighet avseende personuppgiftsansvar. I Läkemedelsverkets föreskrifter och CTR[39] definieras sponsorn som den som är huvudsakligen ansvarig för den kliniska läkemedelsprövningen, men regleringen saknar ett uttryckligt utpekade vad gäller just personuppgiftsansvaret. Vad gäller behandlingen av personuppgifter som sker för att journalföra den behandling som ges till patienter framgår dock av PDL att det är den vårdgivare som vårdar patienten som är personuppgiftsansvarig för de uppgifter som dokumenteras avseende vården av patienten.[40]

Underförstådd behörighet

Vad avser underförstådd behörighet kan konstateras att det finns en etablerad praxis på området att sponsorn, som tillika vanligen är huvudansvarig forskningshuvudman, vid prövarinitierade studier i de allra flesta fall samarbetar med övriga prövare för att ta fram protokollet för studien. Protokollet som studien utförs efter innehåller de egentliga hypoteserna och dikterar i princip uttömmande vilka slags personuppgifter som ska samlas in och på vilket sätt de ska dokumenteras. Samtliga prövare som ingår i prövningen och som varit delaktiga i att ta fram protokollet kan i någon mån sägas påverka ändamålen och medlen med behandlingen.

Det kan också konstateras att det i EDPB:s riktlinjer har rekommenderats att såväl sponsor som prövare kan ha ett gemensamt personuppgiftsansvar, men att det kan förekomma fall där sponsor har ett så pass

[39] *LVFS 2011:19 1 kap. 3 § m.*, kommande *artikel 2.14 CTR*.
[40] PDL 2 kap 6 §.

stort inflytande att det är sponsor som är att betrakta som personuppgiftsansvarig medan prövaren endast agerar på uppdrag av denne, då i egenskap av personuppgiftsbiträde.[41]

Den underförstådda behörighet som återfunnits på området pekar därmed mot att i vart fall sponsor är personuppgiftsansvarig för personuppgifterna som behandlas i läkemedelsprövningen. Om flera prövare från olika organisationer är delaktiga i framtagandet av protokollet kan det även förekomma situationer där gemensamt personuppgiftsansvar föreligger.

Faktiskt inflytande

Vid bedömning av faktiskt inflytande ska ställning tas till faktiska omständigheter. Så har skett genom ett antal workshops inom ramen för framtagande av denna rapport.[42]

Sammanfattningsvis kan följande konstaterats:
Prövaren kan i detta scenario ha ett betydligt större inflytande över ramarna för behandlingen av personuppgifterna jämfört med motsvarande scenario i en industriinitierad läkemedelsprövning (scenario 5.3, ovan). Prövaren har i regel ett stort inflytande över utformningen av protokollet och således inom vilka ramar personuppgifter ska behandlas.

Vad gäller intresse och nytta av slutprodukten med personuppgiftsbehandlingen är det normalt främst sponsorn som tar del av denna slutprodukt. Det beror dels på ett kliniskt intresse där läkemedel till exempel kan användas så kallad off-label i de fall som läkemedlet visat sig tillräckligt effektivt och säkert, och dels på publiceringen av studien i medicinsk facklitteratur. I de fall som prövarna är involverade i framtagande av protokollet föreligger det däremot en betydligt större grad av involvering. Det står därför klart att inte endast sponsorn förfogar över ändamål och medel. Tvärtom styrs i dessa fall ramarna för behandlingen i största del även av deltagande prövare gemensamt med sponsorn. Det är också i dessa fall normalt att även prövare namnges vid en publicering av forskningen vilket tydliggör att även prövare har intresse av att nyttja inte endast processen utan även slutprodukten.

Oaktat nyttan och intresset i slutprodukten har det redogjorts för att prövaren i ett flertal situationer har ett direkt eller indirekt krav att rapportera förändringar eller händelser kring behandlingen av personuppgifter till sponsorn. Det är i de allra flesta förekommande fall sponsorn som har det avgörande beslutet i hur prövaren eventuellt ska agera utifrån händelsen. Sponsorn är i egenskap av huvudansvarig för prövningen i stort den som har att besluta hur tillvägagångssättet ska vara i ett antal situationer. Som exempel kan nämnas att om kodlistan försvinner eller röjs har prövaren en skyldighet enligt god klinisk sed (GCP)[43] att rapportera detta till sponsorn som har att agera på incidenten. Vidare framgår av GCP att sponsorn har ansvaret att övervaka hela prövningen (så kallad ”sponsor-oversight”).

Prövaren är den som praktiskt genomför läkemedelsprövningen och dokumenterar all data. I denna roll utför prövaren naturligtvis en stor del av det praktiska arbetet och det är också prövaren som därmed har att fatta en mängd beslut både kring utförande och säkerheten kring utförandet. Det är förvisso så att både sponsorn och prövaren har ett mandat och ansvar att agera. Eftersom prövaren också varit med att utforma den övergripande planen för läkemedelsprövningen ter det sig som om prövaren också har praktisk möjlighet att påverka hur behandlingen och hanteringen av personuppgifter kommer att ske.

[41] Se avsnitt 3.6.4 ovan (EDPB:s riktlinje 07/2020 v 2.0 om begreppen personuppgiftsansvarig och personuppgiftsbiträde).
[42] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.
[43] ICH E6 (R2) Good Clinical Practice (GCP).

Särskilt om bevarande av data

Ett särskilt fokus är de personuppgifter som bevaras för framtiden för att resultaten senare ska kunna verifieras. Det bör här tydliggöras att detta bevarande sker för just ändamålet tillförlighet och säkerhet av läkemedelsprövningen. Det finns således inget annat ändamål med bevarandet. Denna behandling sker som föreskrivet i protokollet utifrån de ramar lagstiftning ger. Under denna bevarandetid har varken prövare eller sponsor någon given rätt att behandla uppgifterna för andra ändamål. Det ter sig sammantaget som att bevarade personuppgifter, i likhet med behandling i övrigt, sker utifrån det protokoll som upprättats och att det således är de som aktivt deltagit i framtagandet av protokollet som är personuppgiftsansvariga för dessa. Att sponsorn eller övriga prövare inte har direkt åtkomst till personuppgifterna hos en enskild prövare förändrar inte denna bedömning. Det har i domstolspraxis fastslagits att personuppgiftsansvarig inte nödvändigtvis behöver ha åtkomst till de personuppgifter som behandlas, se avsnitt 3.3, ovan. När bevarandet för ändamålet uppföljning är slutfört innebär det att det inte längre finns någon grund för att fortsatt bevara personuppgifter. Personuppgifterna ska då gallras eller arkiveras i enlighet med envar vårdgivares bevarande- och gallringsinstruktioner.

Monitorering (kvalitetskontroll) fungerar på så sätt att sponsorn gör uppföljningar för att kontrollera att källdata överensstämmer med de uppgifterna som överförts till sponsorn. Sponsorn har inte tillgång till källan och måste därför anlita en monitor som utför denna kontroll. Monitorering torde inte innebära några andra ställningstaganden kring personuppgiftsansvar. För det fall som monitorering sker av ett externt bolag kan det förvisso finnas ett personuppgiftsbiträdesförhållande med detta externa bolag, men det faller utanför ramen för den aktuella bedömningen.

Prövare i förhållande till forskningshuvudman

Något som bör beröras i samband med detta är det faktum att regelverket definierar prövaren som en fysisk person medan personuppgiftsansvaret normalt faller på en juridisk person. Forskningshuvudmannen i ansökan till Etikprövningsmyndigheten är också alltid en organisation i motsats till en fysisk person. Denna diskrepans mellan regelverket för läkemedelsprövningar och personuppgiftsbehandling bedöms dock i praktiken inte ha någon avgörande betydelse. Det torde i alla situationer där den fysiske personen (prövaren) agerar å sin arbetsgivares vägnar och i egenskap av anställd innebära att det är arbetsgivaren, det vill säga den juridiska personen, vårdgivaren, som prövaren är verksam inom som också tar på sig ansvaret enligt GDPR, antingen som personuppgiftsbiträde eller personuppgiftsansvarig.

Personuppgiftsansvarig: Utifrån vad som framkommit i workshops[44] och lagstiftning på området är det klart att sponsorn har ett övergripande ansvar för läkemedelsprövningen. Det har också framkommit att planering av prövarinitierade prövningar samt framtagandet av det protokoll som styr densamma i mångt och mycket är ett samarbete mellan sponsor och prövare. Det innebär att samtliga dessa parter har ett väsentligt inflytande över hur personuppgiftsbehandlingen ska komma att ske och, genom framtagande av hypotes för prövningen, också varför behandlingen sker. Sammantaget bör både sponsor och prövare i många fall bedömas som att de agerar tillsammans och i samförstånd och därför har ett gemensamt personuppgiftsansvar.

Notera att denna slutsats till stor del bygger på att en eller flera av prövarna faktiskt är delaktig i processen med framtagande av protokollet. Här behöver därför en bedömning i varje enskilt fall göras i vilken utsträckning en prövare är delaktig. Om liten eller ingen medverkan från övriga medverkande prövare förekommer kan det tyda på att personuppgiftsansvaret i denna situation tillkommer sponsorn ensamt.

[44] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.

Personuppgiftsansvar inom ramen för vårdgivares journalföring

Notera att den personuppgiftsbehandling som sker för ändamålet att journalföra den vård i form av medicinsk behandling som skett på patienter och som utförs av prövaren i egenskap av vårdgivare regleras särskilt i 2 kap. 6 § PDL. Denna hantering (journalföring) är således vårdgivaren (dvs. prövarens arbetsgivare) ensamt personuppgiftsansvarig för.

5.3.3 Behov av avtal

Utgör behandlingen en konstellation där sponsorn och prövarna anses vara gemensamt personuppgiftsansvariga så kräver GDPR att det finns ett inbördes arrangemang. Det torde vara mycket lämpligt, men inte strikt tvingande, att detta arrangemang regleras genom ett skriftligt avtal om gemensamt personuppgiftsansvar mellan parterna där det närmare framgår vem som har att hantera vilken del av personuppgiftsansvaret. För mer information om arrangemanget se avsnitt 3.3, ovan.

Gör bedömningen att sponsorn är personuppgiftsansvarig och prövarna endast personuppgiftsbiträden så krävs enligt GDPR ett personuppgiftsbiträdesavtal (PUB-avtal) som närmare reglerar biträdets behandling av personuppgifter. Ett sådant avtal ska finnas mellan sponsorn och var och en av prövarnas organisationer. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna.

5.4 Klinisk läkemedelsprövning, multicenter – industriinitierad

5.4.1 Scenariobeskrivning

Forskningstyp:	• Klinisk läkemedelsprövning, kräver tillstånd av Läkemedelsverket och Etikprövningsmyndigheten.
Aktörer:	• Det är en aktör (industri) som är sponsor och en annan aktör (vårdgivare) som är huvudansvarig forskningshuvudman. Prövningen innefattar även en eller flera andra deltagande kliniker från andra forskningshuvudmän (vårdgivare) eftersom det är en multicenterstudie.
Prövare: **(en prövare är en fysisk person)**	• En koordinerande prövare arbetar under den huvudansvariga forskningshuvudmannen. Vid de andra medverkande forskningshuvudmännen finns en ansvarig prövare.
Singel- eller multicenter:	• Multicenter.
Kommentar:	• Sponsorn ansöker om tillstånd från Läkemedelsverket, medan huvudansvarig prövare (fysisk person) ansöker till Etikprövningsmyndigheten i egenskap av representant för huvudansvarig forskningshuvudman. När Förordningen för klinisk läkemedelsprövning (CTR) kommer att börja gälla kommer det vara en gemensam ansökan till de två myndigheterna som sponsorn ansvarar för att skicka in (för forskningshuvudmannens räkning). • I industriinitierad uppdragsforskning genomför prövaren studier för att leverera data till sponsorn för analys. Prövaren dokumenterar i första hand de resultat som framkommer under studien. Forskningens hypotes har genererats av bolaget (till exempel om läkemedel A är bättre än läkemedel B). Studien genomförs sedan för att stödja eller förkasta denna hypotes. Det kan förekomma att prövare är med och tar fram protokollet för studien. Normalt är

	prövare även då med på publikationen av resultatet i medicinsk tidskrift. Det kan också hända att prövaren är med på publikationen av andra anledningar. • I multicenter är det flera prövare/kliniker involverade, det vill säga flera forskningshuvudmän. Det är en juridisk person som är forskningshuvudman även om en prövare enligt definition i lagstiftning är en fysisk person. • En av forskningshuvudmännen har ansvaret att ansöka om etikprövning (vilket innebär att denne står som huvudansvarig forskningshuvudman, de andra prövarna benämns för medverkande forskningshuvudmän). Den huvudansökande ansvarar för att koordinera deltagande forskningshuvudmän. Huvudansvarig har dock i praktiken inget ytterligare ansvar än andra forskningshuvudmän i själva studien. • Samtliga prövare ska spara en kopia av data som prövningsstället har genererat åt sponsor för ändamålet att kunna inspektera och rekonstruera prövningen. Samtliga insamlade data finns i pseudonymiserad (kodad) form hos sponsorn.

5.4.1.1 Illustration av scenario 5.4

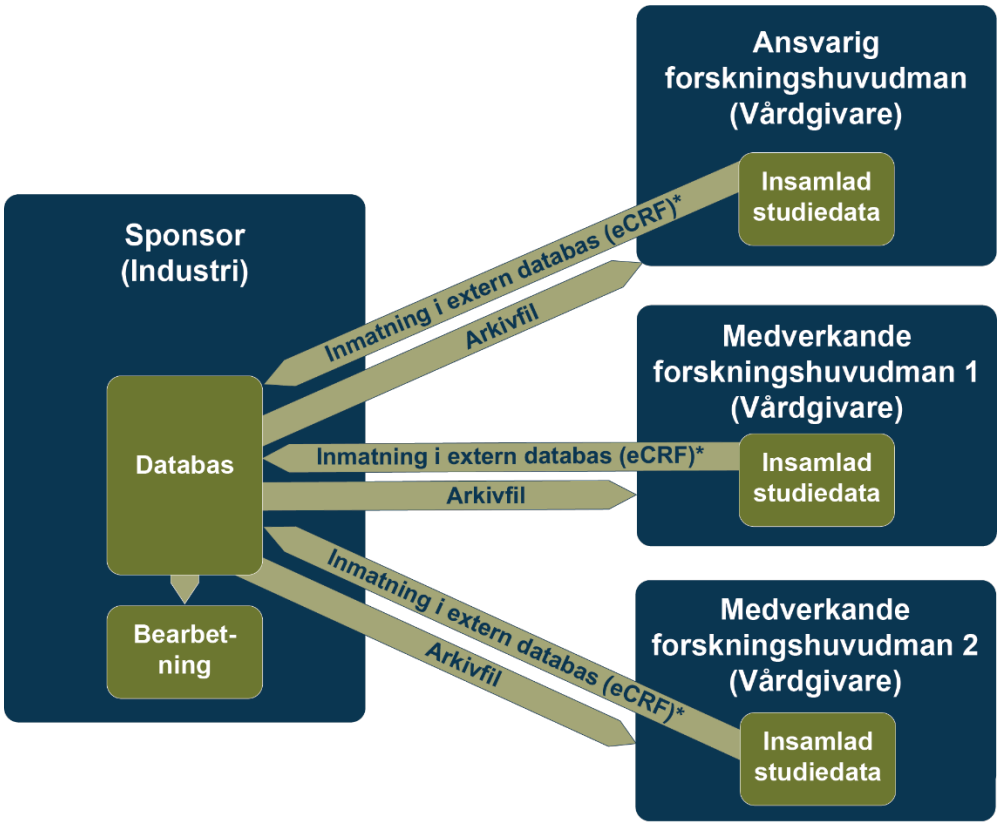


Bild 5.4: Datainsamling sker hos flera olika huvudmän. Databasens placering, samt databearbetning (som till exempel analys) sker hos en annan huvudman (sponsorn). En kopia av forskningshuvudmannens data, ”arkivfil”, ska återföras för arkivering. *överföring bör ske kodat/ pseudonymiserat.

5.4.2 Personuppgiftsansvarets fördelning

Uttrycklig behörighet

Det saknas författningsreglering som ger någon av parterna en uttrycklig behörighet avseende personuppgiftsansvar. I Läkemedelsverkets föreskrifter och CTR[45] definieras sponsorn som den som är huvudsakligen ansvarig för den kliniska läkemedelsprövningen, men regleringen saknar ett uttryckligt utpekade vad gäller just personuppgiftsansvaret. Vad gäller behandlingen av personuppgifter som sker för att journalföra den behandling som ges till patienter framgår dock av PDL att det är den vårdgivare som vårdar patienten som är personuppgiftsansvarig för de uppgifter som dokumenteras avseende vården av patienten.[46]

Underförstådd behörighet

Vad avser underförstådd behörighet kan konstateras att det finns en etablerad branschpraxis på området att sponsorn, vid industriinitierade studier, i de allra flesta fall är den som ensamt arbetat med och tagit fram ett protokoll för studien. Protokollet som studien utförs efter dikterar i princip uttömmande vilka slags personuppgifter som ska samlas in och på vilket sätt de ska dokumenteras. Även om de olika prövarna har ett utrymme att själva hantera rekryteringen av de fysiska personer som ska ingå i studien måste dessa vara representanter för den studiepopulation som protokollet dikterar. I praktiken torde således utrymmet för egna beslut vara begränsat.

Det kan också konstateras att det i EDPB:s riktlinjer har rekommenderats att såväl sponsor som prövare har ett gemensamt personuppgiftsansvar, men att det kan förekomma fall där sponsor har ett så pass stort inflytande att det är sponsor som är att betrakta som personuppgiftsansvarig medan prövaren endast agerar på uppdrag av denne, då i egenskap av personuppgiftsbiträde.[47]

Den underförstådda behörighet som återfunnits på området pekar därmed mot att sponsor är personuppgiftsansvarig för personuppgifterna som behandlas i läkemedelsprövningen och att det även i vissa fall kan förekomma ett gemensamt personuppgiftsansvar tillsammans med prövare.

Faktiskt inflytande

Vid bedömning av faktiskt inflytande ska ställning tas till hur det faktiskt förhåller sig i praktiken. Så har skett genom ett antal workshops inom ramen för framtagande av denna rapport.[48]

Sammanfattningsvis har följande konstaterats:
Prövarna, inklusive den koordinerande prövaren har ett väldigt litet inflytande över de egentliga ramarna för varför och hur personuppgifterna ska behandlas. Även om prövaren är den som så att säga arbetar närmast de registrerade och är den som har kontakten med dessa så sker allt sådant arbete utifrån de strikta rutiner som protokollet reglerar.

Vad gäller intresse och nytta av slutprodukten av personuppgiftsbehandlingen är det vanligtvis endast sponsorn som tar del av denna. Dels i den rent affärsmässiga vidarehanteringen av en marknadsetablering av ett eventuellt läkemedel. Dels i den eventuella publicering som sker av studien i medicinsk facklitteratur. Det förekommer förvisso att även prövaren medverkar i en sådan publikation vilket förekommer främst när prövaren även deltagit aktivt i framtagandet av protokollet. Dessa fall sker som regel endast undantagsmässigt och främst när prövaren är en person med särskilda sakkunskaper eller är en ledande forskare inom området.

Det har vidare konstaterats att prövarna i ett flertal situationer har ett direkt eller indirekt krav på sig att rapportera förändringar eller händelser kring behandlingen av personuppgifter till sponsor. Det är i de allra

[45] *LVFS 2011:19 1 kap. 3 § m.*, kommande *artikel 2.14 CTR*.
[46] PDL 2 kap 6 §.
[47] Se avsnitt 3.6.4 ovan (EDPB:s riktlinje 07/2020 v 2.0 om begreppen personuppgiftsansvarig och personuppgiftsbiträde).
[48] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.

flesta förekommande fall sponsorn som har det avgörande beslutet i hur prövaren eventuellt ska agera utifrån händelsen.

Prövaren är den som praktiskt utför de studiespecifika momenten och dokumenterar all data. I denna roll är det också prövaren som därmed har att fatta en mängd beslut om säkerheten kring utförandet. Det är förvisso så att både sponsorn och prövaren har ett mandat och ansvar att agera, men vad avser prövaren är det i mångt och mycket endast inom ramen för sin egen sfär som prövaren kan fatta beslut. Till exempel hur kontakt och rekrytering av försökspersoner ska ske, och detaljer kring hur prövningen ska genomföras lokalt. Detta ter sig dock vara detaljer som utfyller den övergripande planen som sponsorn tagit fram och som prövaren inte heller har mandat att avvika ifrån, annat än om det rör försökspersonens omedelbara säkerhet. Det ter sig därför sammantaget som att prövaren inte är involverad i framtagandet av den övergripande planen och därmed inte heller involverad i bestämmandet över ändamålen för behandlingen och i väldigt liten del över medlen med desamma.

Särskilt om bevarande av data

Ett särskilt fokus är de personuppgifter som bevaras för framtiden för att resultaten senare ska kunna verifieras. Det bör här tydliggöras att detta bevarande sker för ändamålet tillförlighet och säkerhet kring läkemedelsprövningen, det finns således inget annat ändamål med bevarandet som prövaren styr över. Denna behandling sker i likhet med övriga såsom föreskrivet i sponsorns protokoll. Det är sponsorn som (utifrån de ramar lagstiftning ger) avgör under hur lång tid data ska bevaras. Under dessa bevarandetid har prövaren inte någon given rätt att behandla uppgifterna för andra ändamål. Det ter sig sammantaget som att bevarade personuppgifter bevaras på uppdrag av sponsorn och att det således är denne som är personuppgiftsansvarig för dessa. Att sponsorn inte har direkt åtkomst till personuppgifterna förändrar inte denna bedömning, det har av praxis slagits fast att personuppgiftsansvarig inte nödvändigtvis behöver har åtkomst till de personuppgifter som behandlas, se avsnitt 3.3, ovan. När bevarandet för ändamålet uppföljning är slutfört innebär det att det inte längre finns någon grund för att fortsatt bevara personuppgifter. Personuppgifterna ska då gallras eller arkiveras i enlighet med envar vårdgivares bevarande- och gallringsinstruktioner. Notera då även att personuppgiftsansvarig enligt artikel 28.3 g GDPR ska lämna instruktioner i PUB-avtalet om vad som ska ske med personuppgifterna vid uppdragets slutförande.

Monitorering (kvalitetskontroll) fungerar på så sätt att sponsorn gör uppföljningar för att kontrollera att källdata överensstämmer med de uppgifterna som överförts till sponsorn (sponsorn har inte tillgång till källan och måste därför anlita en monitor som utför denna kontroll). Monitorering torde inte innebära några andra ställningstaganden kring personuppgiftsansvar. För det fall som monitorering genomförs av ett externt bolag kan det förvisso finnas ett personuppgiftsbiträdesförhållande med detta externa bolag, men det faller utanför ramen för den aktuella bedömningen.

Prövare i förhållande till forskningshuvudman

Något som bör beröras i samband med detta är det faktum att regelverket definierar prövaren som en fysisk person medan personuppgiftsansvaret normalt faller på en juridisk person. Forskningshuvudmannen i ansökan till Etikprövningsmyndigheten är också alltid en organisation i motsats till en fysisk person. Denna diskrepans mellan regelverket för läkemedelsprövningar och personuppgiftsbehandling bedöms dock i praktiken inte ha någon avgörande betydelse. Det torde i alla situationer där den fysiske personen (prövaren) agerar å sin arbetsgivares vägnar och i egenskap av anställd innebära att det är arbetsgivaren, det vill säga den juridiska personen, vårdgivaren, som prövaren är verksam inom som också tar på sig ansvaret enligt GDPR, antingen som personuppgiftsbiträde eller personuppgiftsansvarig.

Personuppgiftsansvarig: Sponsor bedöms vara personuppgiftsansvarig för merparten av de behandlingar som sker i en industriinitierad prövning. I de allra flesta fallen torde sponsor även vara ensam personuppgiftsansvarig och de olika prövarna (den juridiske person som prövaren är anställd hos) endast i egenskap av personuppgiftsbiträde agera på uppdrag av sponsorn.

Det bör beaktas att det finns situationer som kan tyda på att både sponsor och prövare agerar tillsammans och i samförstånd och därför har ett gemensamt personuppgiftsansvar. Detta torde främst förekomma i

de fall där prövare är involverad i ett tidigt skede i processen och aktivt deltagit i framtagande av protokoll och sedermera även i publikationer. Här bör en bedömning dock ske i vilken egenskap prövaren gör detta; är prövaren (den fysiske personen) en representant för forskningshuvudmannen (vårdgivaren) eller sker deltagandet i en konsultroll på uppdrag av sponsorn? Det senare (att prövaren agerar på konsultbasis) skulle tyda på att personuppgiftsansvaret även i denna situation tillkommer sponsorn ensamt.

Den huvudansvariga prövaren har inte bedömts ha någon egentlig inverkan eller beslutsmandat än andra prövare när det gäller den praktiska behandlingen av personuppgifter. Att det är denne som ansöker om etikprövning är främst en formell hantering. Det bedöms således inte som att den koordinerande prövaren har en annan grad av personuppgiftsansvar än andra prövare. Det ska tilläggas att om någon prövare, tillsammans med sponsor, varit delaktig i framtagande av protokollet så är det normalt den koordinerande prövare. Av den anledningen kan det ligga närmare till hands att den koordinerade prövaren kan ha ett gemensamt personuppgiftsansvar gemensamt med sponsorn.

Personuppgiftsansvar inom ramen för vårdgivares journalföring

Notera att den personuppgiftsbehandling som sker för ändamålet att journalföra den vård i form av medicinsk behandling som skett på patienter och som utförs av prövaren i egenskap av vårdgivare regleras särskilt i 2 kap. 6 § PDL. Denna hantering (journalföring) är således vårdgivaren (dvs. prövarens arbetsgivare) ensamt personuppgiftsansvarig för.

5.4.3 Behov av avtal

Om behandlingen genomförs av en konstellation där sponsorn anses vara personuppgiftsansvarig och prövaren endast personuppgiftsbiträde krävs enligt GDPR ett personuppgiftsbiträdesavtal (PUB-avtal) som närmare reglerar personuppgiftsbiträdets behandling av personuppgifter. Ett sådant avtal ska finnas mellan sponsorn och var och en av prövarna. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna. Den koordinerande prövaren anses inte ha något större ansvar än övriga prövare. Personuppgiftsansvaret utgår från sponsorn och det är också denne som har att avtala om delegering av behandlingen av personuppgifter.

Om behandlingen genomförs av en konstellation där flera av de ingående parterna anses vara gemensamt personuppgiftsansvariga kräver GDPR att det finns ett inbördes arrangemang. Det torde vara mycket lämpligt, men inte strikt tvingande, att detta arrangemang regleras genom ett skriftligt avtal om gemensamt personuppgiftsansvar mellan parterna där det närmare framgår vem som har att hantera vilken del av personuppgiftsansvaret. Det bör även innehålla gemensamt framtagna instruktioner kring vem som ska utföra vad i samband med personuppgiftsbehandlingen.

Särskilt när antalet aktörer är stort torde det vara i princip nödvändigt att tydliggöra vilken part som har att ta olika delar av personuppgiftsansvaret, till exempel vad gäller rapportering av personuppgiftsincidenter eller säkerställande av att tillräckliga säkerhetsåtgärder har vidtagits. Det ska understrykas att gemensamt personuppgiftsansvar innebär ett solidariskt ansvar. Vid en eventuell tillsyn har alltså alla parter som har ett personuppgiftsansvar skyldighet att se till att de registrerades rättigheter tillvaratas på ett säkert sätt. Om en tillsyn skulle leda till en administrativ sanktionsavgift eller om en registrerad har skadestånds-anspråk kan sådana avgifter eller skadestånd riktas mot vilken som helst av de ingående parterna. För mer information om arrangemanget se avsnitt 3.3, ovan.

5.5 Klinisk Forskning, singelcenter

5.5.1 Scenariobeskrivning

Forskningstyp:	• Forskning som kräver godkännande från Etikprövningsmyndigheten.
Aktörer:	• Det är en aktör (vårdgivare) som är ansvarig forskningshuvudman. Prövaren kan ha en kombinationstjänst och samla in och/eller utföra delar av analysen vid en akademisk institution.
Singel- eller multicenter:	• Singelcenter.
Kommentar:	• Klinisk forskning innebär att en framtagen hypotes ska prövas utifrån en forskningsplan som beskrivs i ett forskningsprotokoll. • Klinisk forskning sker genom dokumentation av intervention, eller genom att tidigare dokumentation (journaler eller andra medicinska databaser), så kallad registerstudier, gås igenom. • Klinisk forskning omfattas inte av någon specifik reglering på samma sätt som läkemedelsprövning; processer och styrning är därför inte i detalj författnings-reglerad.

5.5.1.1 Illustration av scenario 5.5

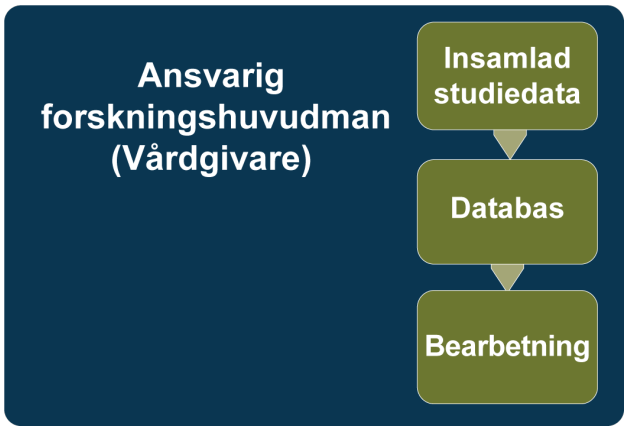


Bild 5.5a: Datainsamling och databasens placering, samt databearbetning (som till exempel analys) sker inom samma huvudman.

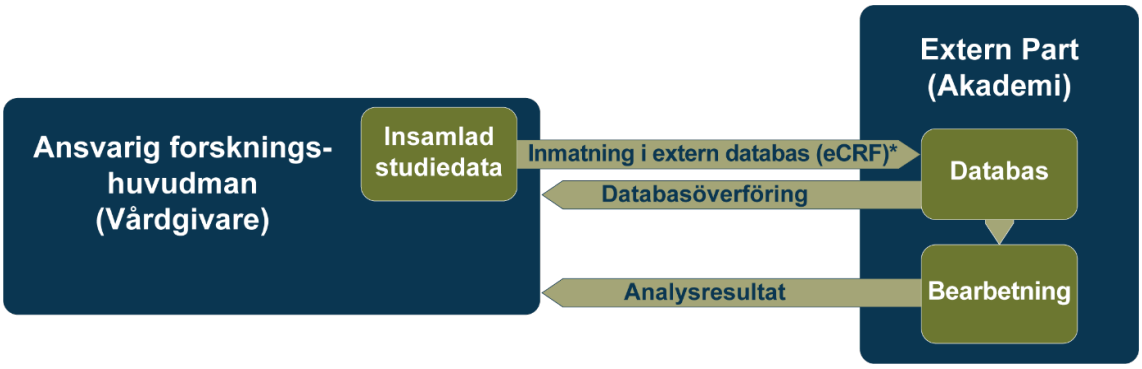


Bild 5.5b: Datainsamling och databasens placering, samt databearbetning som till exempel analys) sker inom olika huvudmän. Slutgiltig databas bör alltid återföras till Sponsor/Ansvarig forskningshuvudman. *överföring bör ske kodat/pseudonymiserat.

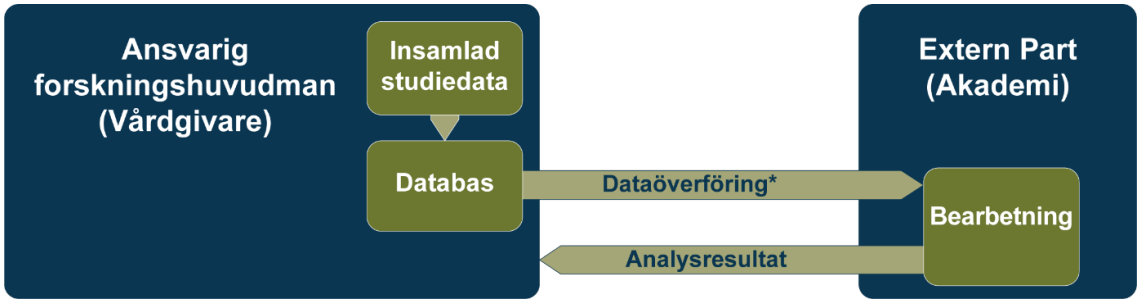


Bild 5.5c: Datainsamling samt databasens placering och databearbetning (som till exempel analys) sker inom olika huvudmän. *överföring bör ske kodat/pseudonymiserat.

5.5.2 Personuppgiftsansvarets fördelning

Hälso- och sjukvård samt forskning utgör två separata verksamhetsgrenar hos en vårdgivare. Forskningen förutsätter vårdens strukturer och resurser samt utgår från de behov som finns i hälso- och sjukvården vilka förväntas leda till patient- och samhällsnytta. Klinisk forskning innebär således normalt deltagande från en hälso- och sjukvårdsorganisation i de fall prövningen utförs med patienter. Det finns dock undantag och forskning kan ske helt inom akademin utan inblandning från klinisk hälso- och sjukvård. Detta gäller särskilt så kallad registerstudier där endast historiska data gås igenom och inga fysiska kontakter eller ingrepp sker gentemot försökspersoner.

Behandling av personuppgifter som sker inom ramen för hälso- och sjukvård omfattas av patientdatalagen (PDL). En vårdgivare är alltid personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför enligt PDL. En myndighet som bedriver hälso- och sjukvård är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Personuppgifter inom hälso- och sjukvården får behandlas för de ändamål som listas i den uttömmande ändamålskatalogen i 2 kap. 4 § PDL. Att en patientjournal bland annat är en informationskälla för forskning framgår av 3 kap. 2 § andra stycket PDL. Syftet med en patientjournal är dock i första hand att bidra till en god och säker vård av patienten. När det kommer till ändamålet forskning torde PDL därför inte vara avgörande för bedömningen av vem som är personuppgiftsansvaret för behandlingen utan denna bedömning ska ske utifrån GDPR.

I detta scenario förekommer endast en organisation (se dock avsnittet Akademisk institution, nedan). Det är således denna organisation som utför forskningen samt prövningen och därför är personuppgiftsansvarig.

Notera dock att det rör sig om olika behandlingar med olika ändamål vilket innebär att det inom organisationen kan finnas olika aktörer som har det organisatoriska ansvaret (till exempel en forskningsenhet som är skild från verksamhetsområdet vård). Det innebär också att det normalt förekommer sekretess mellan dessa skilda verksamhetsområden. En eventuell överföring av information från den ena verksamheten till den andra kan därför behöva föregås av en sekretessprövning och ett formellt beslut om utlämnande. Detta torde dock inte påverka bedömningen av personuppgiftsansvaret.

Personuppgiftsansvarig: Vårdgivaren, tillika forskningshuvudmannen är personuppgiftsansvarig för samtliga behandlingar.

Akademisk institution

I vissa fall kan prövaren (som alltid är en fysisk person) ha en kombinationstjänst och samla in och/eller utföra delar av analysen vid en akademisk institution. Anledningen till detta kan vara flera olika, till exempel att forskningshuvudmannen saknar särskilda IT-verktyg eller att den akademiska institutionen helt enkelt förfogar över bättre tekniska förutsättningar att hantera eller analysera stora datamängder. I dessa situationer blir det viktig att avgöra vilken roll prövaren har och vilken organisation denne representerar när den utför sin uppgift som prövare.

Om den akademiska institutionen endast tillhandahåller tekniska verktyg som prövaren kan nyttja i forskningen ter det sig naturligt att se institutionen som ett personuppgiftsbiträde. Det är i sådant fall också viktigt att etablera huruvida den akademiska institutionen tar på sig denna roll och det ansvar det innebär eller om det helt enkelt bara är så att prövaren valt att använda sig av de verktyg som finns tillgängliga för denne genom sin anställning vid akademin utan att institutionen godkänt det. Det torde vara av stor betydelse att personuppgifter hanteras på ett strukturerat och medvetet sätt och att rutiner och riktlinjer klargörs mellan parterna så att ansvariga representanter för båda organisationerna tydliggör vilken hantering som faktiskt är avsedd och att relevanta avtal kan ingås mellan behöriga representanter för respektive organisation.

Det kan naturligtvis förekomma situationer där den akademiska institutionen har en mer avgörande roll än enbart att tillhandhålla en teknisk infrastruktur för att hantera forskningsdata, det får då sker en bedömning från fall till fall vilken part som är personuppgiftsansvarig. Även i dessa situationer är det dock av yttersta vikt att institutionens vilja tydliggörs och att bedömningen inte enbart utgår ifrån vad prövaren med kombinationstjänst har för uppfattning.

5.5.3 Behov av avtal

I de fall det inte förekommer något personuppgiftsbiträde i scenariot finns det inget i lag angivet krav på något avtal i detta scenario, däremot bör det finnas en process för hanteringen av informationsflödet särskilt då informationen ska passera sekretessgränser mellan verksamhetsgrenar (såsom vård → forskning).

I det fall prövaren samlar in/analyserar data vid en akademisk institution såsom beskrivits ovan i exempel b) och c) och ett personuppgiftsbiträdesförhållande därmed uppstår (till exempel för att institutionens tekniska infrastruktur nyttjas) finns det ett absolut krav om att ett personuppgiftsbiträdesavtal upprättas i enlighet med GDPR, som närmare reglerar personuppgiftsbiträdets behandling av personuppgifter. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna. Det kan vara på sin plats att påpeka att det inte är nödvändigt med ett personuppgiftsbiträdesavtal i samband med varje enskild kliniskt forskningsprojekt. Ett mer allmänt avtal mellan en akademisk institution och en vårdgivare kan mycket väl ingås där även hantering av personuppgifter i framtida forskningsprojekt regleras.

5.6 Klinisk Forskning, multicenter

5.6.1 Scenariobeskrivning

Forskningstyp:	• Forskning som kräver godkännande från Etikprövningsmyndigheten.
Aktörer:	• Det är en aktör (vårdgivare) som är huvudansvarig forskningshuvudman. Forskningsstudien innefattar även en eller flera andra deltagande kliniker från andra medverkande forskningshuvudmän (vårdgivare eller akademiska institutioner) eftersom det är en multicenterstudie.
Singel- eller multicenter:	• Multicenter
Kommentar:	• I multicenterforskning är det flera forskare från olika forskningscentra/ kliniker involverade. Det är en juridisk person som är forskningshuvudman, vanligen den region som forskaren representerar. • En av forskningshuvudmännen har ansvaret att ansöka till Etikprövningsmyndigheten (vilket innebär att denne står som huvudansvarig forskningshuvudman, de andra prövarna kallas för medverkande forskningshuvudmän). Den huvudansökande ansvarar för att koordinera de andra deltagande forskningshuvudmännen. • Samtliga forskningshuvudmän bör följa sina interna instruktioner för bevarande och gallring vad gäller bevarande av kopia av data som respektive forskare insamlat. • Slutresultatet, studiedatabasen, samlas i pseudonymiserad (kodad) form, vanligen hos den ansvarige forskningshuvudmannen.

5.6.1.1 Illustration av scenario 5.6

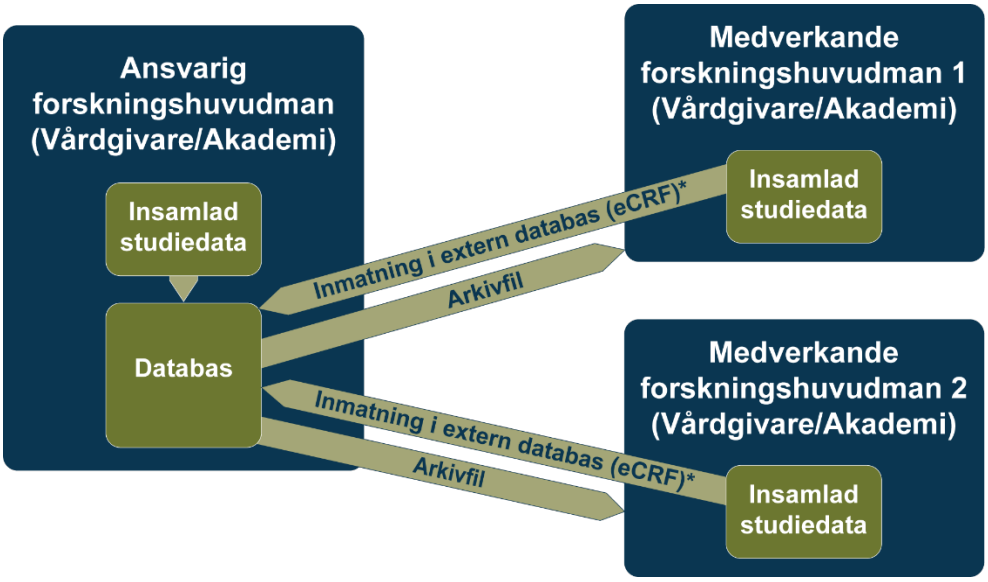


Bild 5.6: Datainsamling sker hos flera olika huvudmän. Databasens placering, samt databearbetning (som till exempel analys) kan förekomma hos olika huvudmän, men vanligen hos ansvarig forskningshuvudman, och slutgiltig databas bör alltid återföras till densamma. En kopia av forskningshuvudmannens data, ”arkivfil”, ska återföras för arkivering. *överföring bör ske kodat/ pseudonymiserat.

5.6.2 Personuppgiftsansvarets fördelning

Hälso- och sjukvård samt forskning utgör två separata verksamhetsgrenar hos en vårdgivare. Forskningen förutsätter vårdens strukturer och resurser samt utgår från de behov som finns i hälso- och sjukvården vilka förväntas leda till patient- och samhällsnytta. Klinisk forskning innebär således normalt deltagande från en vårdgivare i de fall prövningen utförs med patienter. Det finns dock undantag och forskning kan ske helt inom akademin utan inblandning från klinisk hälso- och sjukvård. Det gäller särskilt så kallad registerstudier där endast historiska data gås igenom och inga fysiska kontakter eller ingrepp sker gentemot försöksdeltagare.

Behandling av personuppgifter som sker inom ramen för hälso- och sjukvård omfattas av patientdatalagen (PDL). En vårdgivare är alltid personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför enligt PDL. En myndighet som bedriver hälso- och sjukvård är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Personuppgifter inom hälso- och sjukvården får behandlas för de ändamål som listas i den uttömmande ändamålskatalogen i 2 kap. 4 § PDL. Att en patientjournal bland annat är en informationskälla för forskning framgår av 3 kap. 2 § andra stycket PDL. Syftet med en patientjournal är dock i första hand att bidra till en god och säker vård av patienten. När det kommer till ändamålet forskning torde PDL därför inte vara avgörande för bedömningen av vem som är personuppgiftsansvaret för behandlingen utan denna bedömning ska ske utifrån GDPR.

I detta scenario förekommer flera organisationer där en av organisationerna tar ett övergripande ansvar och också är den organisation som söker tillstånd hos Etikprövningsmyndigheten.[49] Denna aktör benämns ansvarig forskningshuvudman och övriga deltagande benämns medverkande forskningshuvudmän.

Uttrycklig behörighet

Det saknas reglering som ger någon av parterna en uttryckligen behörighet avseende personuppgiftsansvar. I etikprövningslagen anges att godkänd forskning får innebära behandling av personuppgifter, men inte någon konkret bestämmelse om vem som har personuppgiftsansvaret för behandlingen. Av 6 § etikprövningslagen framgår att forskningshuvudmannen ska vidta åtgärder för att förebygga att forskning i den egna verksamheten utförs i strid med de villkor som meddelas. I övrigt pekas egentligen inget ansvar ut. Bestämmelsen torde inte heller peka ut den ansvarige forskningshuvudmannen specifikt eftersom bestämmelsen anger att huvudmannen endast ansvarar för den egna verksamheten.

Vad gäller behandlingen av personuppgifter som eventuellt sker för att journalföra den behandling som givits patienter som utförs inom ramen för den kliniska forskningen framgår dock av PDL att det är den vårdgivare som vårdar patienten som är personuppgiftsansvarig för de uppgifter som dokumenteras avseende vården av patienten.[50]

Underförstådd behörighet

Vad avser underförstådd behörighet kan konstateras att det inte finns en motsvarande branschpraxis som vid industriinitierade prövningar, det vill säga att det är en part som ensamt utför en stor del av förarbetet. Klinisk forskning av multicenterkaraktär sker tvärtom ofta i samarbete redan under framtagandet av en forskningshypotes och forskningsprotokollet.

Det kan också konstateras att det i EDPB:s riktlinjer har rekommenderats att när forskning utförs gemensamt av flera organisationer så har de ett gemensamt personuppgiftsansvar för den sambehandling som sker av personuppgifterna, men att respektive organisation har ett eget ansvar för de eventuella andra behandlingar som sker av personuppgifterna utanför denna sambehandling. [51] I exemplet beskrivs sambehandling som att samtliga organisationer exporterar sina personuppgifter till en gemensam databas där ett specifikt forskningsprojekt genomförs.

[49] Av 23 § etikprövningslagen framgår att när flera forskningshuvudmän medverkar i ett och samma forskningsprojekt ska de gemensamt uppdra åt en av dem att ansöka om etikprövning av projektet för allas räkning.
[50] PDL 2 kap 6 §.
[51] EDPB:s riktlinje 07/2020 v 2.0 om begreppen personuppgiftsansvarig och personuppgiftsbiträde.

De underförstådda behörigheter som återfunnits på området pekar därmed mot att i vart fall den ansvarige forskningshuvudmannen är personuppgiftsansvarig för personuppgifterna som behandlas i forskningsprojektet och mycket talar också för att de personuppgifter som tillförs till databasen av andra organisationer ska hanteras som ett gemensamt personuppgiftsansvar.

Faktiskt inflytande

Vid bedömning av faktiskt inflytande ska ställning tas till hur det faktiskt förhåller sig i praktiken. Så har skett genom ett antal workshops inom ramen för framtagande av denna rapport.[52]

Sammanfattningsvis har följande konstaterats:

De övriga deltagande forskningshuvudmännen har ett väsentligt inflytande över ramarna för varför och hur personuppgifterna ska behandlas. Det är i de allra flesta fall ett samarbete som sker både avseende framtagande av forskningshypotes, vilka underlag som kommer att krävas samt hur forskningsprotokollet ska utformas.

Vidare delas det ett intresse för slutprodukten av forskningen som är tänkt att kunna användas i vården och inte tillkomma någon särskild part. Den som utses till ansvarig forskningshuvudman är ansvarig att söka till Etikprövningsmyndigheten, men det behöver inte betyda att denne har varit mer delaktig än andra i framtagandet av forskningsprojektet.

Det förekommer förvisso att vissa av forskningshuvudmännen är mer engagerade än andra. Det kan vara så att en eller ett fåtal av forskningshuvudmännen påbörjar framtagandet av forskningshypotes och protokoll och ytterligare forskningshuvudmän tillkommer i ett senare skede. Här bör en bedömning dock ske i vilken grad de ytterligare forskningshuvudmännen är engagerade och i vilket skede. I det fall den huvudansvarig forskningshuvudmannen kommer fram till att ett större forskningsunderlag krävs för utförande och först då vänder sig till ytterligare deltagare för att göra utsökningar eller liknande, för därigenom säkerställa att forskningsunderlaget blir tillräckligt brett, kan exempelvis tyda på att den huvudansvariga ensamt har bestämt över ramarna för personuppgiftsbehandlingen.

När slutresultatet av ett forskningsprojekt publiceras som en vetenskaplig artikel namnges normalt samtliga forskare som deltagit i forskningsprojektet från samtliga forskningshuvudmän. All forskningscentra/vårdinrättningar har lika rätt att ta del av det slutliga resultatet av forskningen.

Det ter sig därför sammantaget som att det vanligtvis är en gemensamt planerad och utförd aktivitet där ingen av parterna egentligen har ett betydligt större beslutsmandat än någon annan. Data som levereras till studiedatabasen är normalt också tillgänglig för samtliga (i vart fall i pseudonymiserad form som en integritetsfrämjande säkerhetsåtgärd) ingående organisationer. Som angivits i stycket ovan kan det dock vara så att den huvudansvarig forskningshuvudmannen ensam eller tillsammans med en begränsad grupp av forskningshuvudmännen är de som faktiskt haft det avgörande inflytandet. En sådan bedömning måste ske i det enskilda fallet för att avgöra vilken part eller vilken grupp av parter som kan anses vara personuppgiftsansvariga.

Särskilt om bevarande av data

Ett särskilt fokus är de personuppgifter som bevaras för framtiden för att resultaten av forskningen senare ska kunna verifieras. Det bör här tydliggöras att detta bevarande sker för just ändamålet tillförlighet och säkerhet kring forskningen, det finns således inget annat ändamål med bevarandet. Personuppgifterna som sambearbetas pseduonymiseras vanligen för att skydda informationen som skapas och sambearbetas. Kodlistor som hör till pseudonymiseringen (som kopplar respektive patient/individ till respektive informationsmängd) bevaras då hos kliniken som upprättat den och överlämnas inte till den ansvarige forskningshuvudmannen. Vidare bevaras samtycken från deltagande forskningspersoner hos respektive klinik. När bevarandet för ändamålet uppföljning är slutfört innebär det att det inte längre finns någon

[52] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.

grund för att fortsatt bevara personuppgifter. Personuppgifterna ska då gallras eller arkiveras i enlighet med envar vårdgivares bevarande- och gallringsinstruktioner.

Inom respektive organisation bör dock noteras att det kan röra sig om olika behandlingar med olika ändamål, vilket innebär att olika aktörer kan ha det organisatoriska ansvaret (till exempel en forskningsenhet som är skild från verksamhetsområdet vård). Det innebär också att det normalt förekommer sekretess mellan dessa skilda verksamhetsområden. En eventuell överföring av information från den ena verksamheten till den andra kan därför behöva föregås av en sekretessprövning och ett formellt beslut om utlämnande. Detta torde dock inte påverka bedömningen av personuppgiftsansvaret.

Personuppgiftsansvarig är: Utifrån vad som framkommit i workshops[53] och lagstiftning på området är det tydligt att ett gemensamt forskningsprojekt också utgår från ett gemensamt deltagande och ansvarstagande. Sammantaget bör huvudansvarig forskningshuvudman och medverkande forskningshuvudmän ha ett gemensamt personuppgiftsansvar för de personuppgifter som *sambearbetas*. Mot bakgrund av det gemensamma arbete som sker inför ett forskningsåtagande, framtagande av forskningsprotokollet samt det mål om att allt ska ske i samförstånd från samtliga deltagande huvudmän ter sig som ett mycket tydligt tecken på att forskarna, och därmed de forskningshuvudmän de representerar, agerar tillsammans i samförstånd och således har ett gemensamt personuppgiftsansvar. Som angivits i avsnittet ovan kan det dock vara så att huvudansvarig ensam eller tillsammans med en begränsad grupp av forskningshuvudmännen är de som faktiskt haft det avgörande inflytandet. En sådan bedömning måste ske i det enskilda fallet för att avgöra vilken part eller vilken grupp av parter som i så fall kan anses vara personuppgiftsansvariga.

Notera att slutsatsen avser sambearbetningen av personuppgifter, således den sammantagna informationsmängden som tagits in i studiedatabasen. De delmängder av studiedatabasen som varje klinik förfogar själv över torde vara dennes eget ansvar, vad gäller de personuppgifter som behandlats genom att föra in i patientjournaler ansvarar respektive vårdgivare för enligt PDL.

5.6.3 Behov av avtal

Om behandlingen genomförs av en konstellation där samtliga forskningshuvudmän anses vara gemensamt personuppgiftsansvariga kräver GDPR att det finns ett ”inbördes arrangemang”. Det torde vara mycket lämpligt, men inte strikt tvingande, att detta arrangemang regleras genom ett skriftligt avtal om gemensamt personuppgiftsansvar mellan parterna (se avsnitt 3.3, ovan) där det närmare framgår vem som har att hantera vilken del av personuppgiftsansvaret och gemensamt framtagna instruktioner kring vem som ska utföra vad i samband med personuppgiftsbehandlingen. Särskilt när antalet aktörer är högt torde det vara i princip nödvändigt att tydliggöra vilken part som har att ta olika delar av personuppgiftsansvaret, till exempel vad gäller rapportering av personuppgiftsincidenter eller säkerställande av att tillräckliga säkerhetsåtgärder har vidtagits. Det ska understrykas att gemensamt personuppgiftsansvar innebär ett solidariskt ansvar, vid en eventuell tillsyn har alltså alla ingående aktörer skyldighet att se till att de registrerades rättigheter tillvaratas på ett säkert sätt. Om en tillsyn skulle leda till en administrativ sanktionsavgift eller om en registrerad har skadeståndsanspråk så kan sådana avgifter eller skadestånd riktas mot vilken som helst av de ingående parterna.

[53] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.

5.7 Klinisk läkemedelsprövning, multicenter, konsortium som uppdragsgivare

5.7.1 Scenariobeskrivning

Forskningstyp:	• Klinisk läkemedelsprövning, kräver tillstånd av Läkemedelsverket och Etikprövningsmyndigheten.
Aktörer:	• Ett konsortium etablerat i EU/EES[54] ger i uppdrag till en svensk aktör (vårdgivare) att vara sponsor/co-sponsor och huvudansvarig forsknings-huvudman för prövningen i Sverige. Prövningen innefattar även en eller flera andra deltagande kliniker från andra medverkande forskningshuvudmän (vårdgivare) eftersom det är en multicenterstudie.
Prövare: **(en prövare är en fysisk person)**	• En koordinerande prövare arbetar under den huvudansvariga forsknings-huvudmannen. Vid de andra medverkande forskningshuvudmännen finns ansvariga prövare.
Singel- eller multicenter:	• Multicenter
Kommentar:	• Det finns ingen enhetlig internationell definition vad ett konsortium är samt om ett konsortium är en juridisk person som kan ingå avtal samt rättsligt åtnjuta förpliktelser och rättigheter. Enligt svensk rätt finns det ingen definition ett konsortium. • Efter att prövningen genomförts samlas pseudonymiserad (kodad) data hos konsortiet eller en aktör på uppdrag av konsortiet.

5.7.1.1 Illustration av scenario 5.7

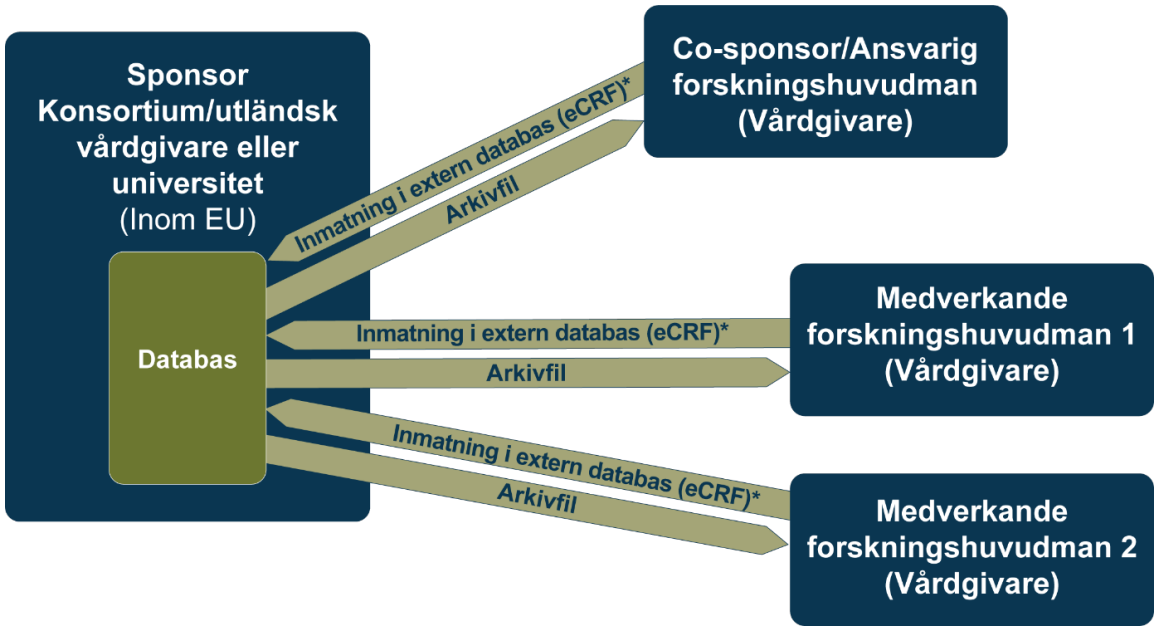


Bild 5.7: Datainsamling sker hos flera olika huvudmän. Databasens placering, samt databearbetning (som till exempel analys) sker hos en annan huvudman på uppdrag av ett konsortium/utländsk vårdgivare eller universitet inom EU. En kopia av forskningshuvudmannens data, ”arkivfil”, ska återföras för arkivering. *överföring bör ske kodat/pseudonymiserat.

[54] EES står för Europeiska ekonomiska samarbetsområdet och innefattar, förutom EU:s medlemsstater, Norge, Island och Liechtenstein.

5.7.2 Personuppgiftsansvarets fördelning

Den stora utmaningen här är knappast att utreda vilken part som är ansvarig, i detta fall är det konsortiet som är att betrakta som sponsor och bedömningen av personuppgiftsansvar borde följa resonemanget kring industriinitierade läkemedelsprövning. Den nationelle sponsorn (det som kallas co-sponsorer) behöver inte nödvändigtvis ha varit medverkande i framtagandet av hypotes eller protokoll. De ansvarar för att organisatoriskt hantera studien i respektive land och ingår därmed avtal med medverkande forskningshuvudmän för deras deltagande.

Utmaningen från ett juridiskt perspektiv är dock vad konsortiet ska anses utgöra för rättsfigur. Det finns i svensk rätt ingen definition av konsortium och det saknas därför också utrymme att se en sådan konstellation som något annat än flera olika parter som agerar tillsammans och i samförstånd. Ett konsortium bildas genom att två eller flera bolag beslutar om att samverka för att genomföra ett större projekt. Samverkan kan antingen vara ett gemensamt ägt bolag, eller bygga på avtal där de ingående parterna ansvarar för valda dela av det större projektet. I juridisk mening så räknas dock ett konsortium endast som ett enkelt bolag, och alltså ingen egen juridisk person. Detta innebär att varje ingående företag eller organisation ansvarar för sina skulder och äger sina tillgångar. För ingångna avtal ansvarar vanligtvis endast de bolagsmän som ingått avtalet.

Slutsatsen kring personuppgiftsansvaret bör bli densamma som i industriinitierade läkemedelsprövningar (jmf scenario 5.2 och 5.4 ovan). Det vill säga att den part (ev. parter) som tagit fram hypotes och protokoll är den som förfogar över ändamål och medel och således är personuppgiftsansvarig. Övriga aktörer som deltar och endast utför sitt uppdrag genom att följa sagda protokoll är att betrakta som personuppgiftsbiträden.

Konsortiet bör bedömas utgöras av de personer/organisationer som ingår i varje enskilt avtal. Personuppgiftsansvar som ankommer på konsortiet måste rimligen anses falla på samtliga dessa personer/organisationer gemensamt (gemensamt personuppgiftsansvar). Det här innebär att det är mycket viktigt att säkerställa vilka personer/organisationer som faktiskt står bakom en viss studie. Det är *inte* tillräckligt att endast konstatera att det är ett konsortium som gör det.

5.7.3 Behov av avtal

Om behandlingen genomförs av en konstellation där flera av de ingående parterna anses vara gemensamt personuppgiftsansvariga så kräver GDPR att det finns ett inbördes arrangemang. Det torde vara mycket lämpligt, men inte strikt tvingande, att detta arrangemang regleras genom ett skriftligt avtal om gemensamt personuppgiftsansvar mellan parterna där det närmare framgår vem som har att hantera vilken del av personuppgiftsansvaret (se avsnitt 3.3, ovan). Det bör även innehålla gemensamt framtagna instruktioner kring vem som ska utföra vad i samband med personuppgiftsbehandlingen. Särskilt när antalet aktörer är högt torde det vara i princip nödvändigt att tydliggöra vilken part som har att ta olika delar av personuppgiftsansvaret, till exempel vad gäller rapportering av personuppgiftsincidenter eller säkerställande av att tillräckliga säkerhetsåtgärder har vidtagits. Det ska understrykas att gemensamt personuppgiftsansvar innebär ett solidariskt ansvar, vid en eventuell tillsyn har alltså alla ingående aktörer skyldighet att se till att de registrerades rättigheter tillvaratas på ett säkert sätt. Om en tillsyn skulle leda till en administrativ sanktionsavgift eller om en registrerad har skadeståndsanspråk så kan sådana avgifter eller skadestånd riktas mot vilken som helst av de ingående parterna.

Eftersom ett konsortium inte är en juridisk person utan består av ett antal personer/organisationer som samarbetar (ofta i form av ett så kallad enkelt bolag) är det också högst rekommenderat att det ingås ett gemensamt studiespecifikt avtal enligt ovan där det tydligt framgår vilka åtaganden som respektive person/organisation har inom ramen för personuppgiftansvaret. Ett sådant avtal måste då undertecknas av samtliga ingående personer/organisationer i konsortiet som ska delta i den aktuella studien.

Vidare ska det finns ett personuppgiftsbiträdesavtal (PUB-avtal) med de prövare som inte varit delaktiga i att ta fram protokollet och därmed inte anses förfoga över medlen eller ändamålen med behandlingen och

såldes ingå i det gemensamma personuppgiftsansvaret. Enligt GDPR krävs ett personuppgiftsbiträdesavtal som närmare reglerar biträdets behandling av personuppgifter. Ett sådant avtal ska finnas mellan sponsorn och var och en av prövarna. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna. Den koordinerande prövaren anses inte ha något större ansvar än övriga, personuppgiftsansvaret utgår från sponsorn och det är också den som har att avtala om delegering av behandlingen av personuppgifter. Eftersom sponsorn är ett konsortium så måste avtalet ingås med samtliga organisationer som ingår i konsortiet.

5.8 Klinisk läkemedelsprövning, multicenter, på uppdrag av sponsor utanför EU/EES

5.8.1 Scenariobeskrivning

Forskningstyp:	• Klinisk läkemedelsprövning, kräver tillstånd av Läkemedelsverket och Etikprövningsmyndigheten.
Aktörer:	• En sponsor – etablerad utanför EU/EES – ger en aktör inom EU/ESS i uppdrag att tillhandahålla ett datainsamlingsformulär (CRF) för flera prövningsställen etablerade i EU/EES. En vårdgivare i Sverige är forskningshuvudman. Prövningen innefattar även en eller flera andra deltagande kliniker från andra forskningshuvudmän (vårdgivare) eftersom det är en multicenterstudie.
Prövare: **(en prövare är en fysisk person)**	• En koordinerande prövare arbetar under den huvudansvariga forsknings-huvudmannen. Vid de andra medverkande forskningshuvudmännen finns ansvariga prövare.
Singel- eller multicenter:	• Multicenter.
Kommentar:	• En sponsor etablerad i ett tredjeland kan omfattas av GDPR och kan därmed vara personuppgiftsansvarig, ensamt eller gemensamt, för behandling av person-uppgifter. Syftet med denna rapport är inte att utreda det geografiska tillämp-ningsområdet för gränsöverskridande forskning. Detta scenario behöver därför utredas utifrån antagandet om att sponsorn omfattas av GDPR eller inte.

5.8.1.1 Illustration av scenario 5.8

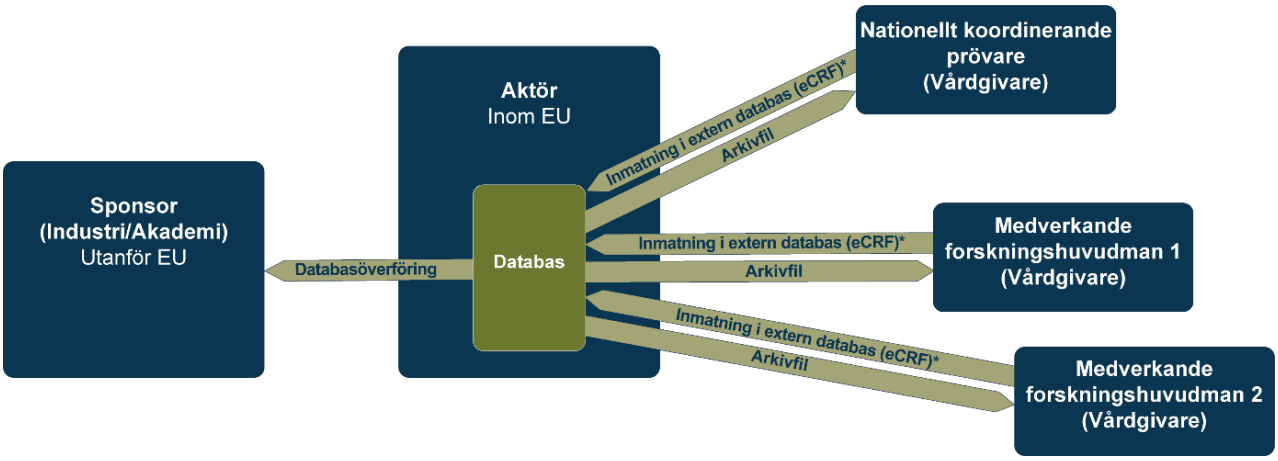


Bild 5.8: Datainsamling sker hos flera olika huvudmän. Databasens placering, samt databearbetning (som till exempel analys) sker hos en huvudman utanför EU. En kopia av forskningshuvudmannens data, ”arkivfil”, ska återföras för arkivering. *överföring bör ske kodat/ pseudonymiserat.

5.8.2 Personuppgiftsansvarets fördelning

Till att börja med kan konstateras att det enligt artikel 3.1 GDPR framgår att GDPR är tillämplig på sådan behandling av personuppgifter som sker inom ramen för ett verksamhetsställe inom EU. Den behandlingen som sker genom att prövare utför läkemedelsprövningen är även en behandling av personuppgifter som omfattas av GDPR. Om det bedöms att en sponsor är den som förfogar över ändamålen och medlen för behandlingen torde denne därför vara att betrakta som personuppgiftsansvarig för behandlingen, oavsett om sponsorn har verksamhetsställe inom EU eller inte.[55]

Bedömningen av personuppgiftansvaret bör här följa samma modell som industriinitierad läkemedels-prövning som beskrivs närmare i scenario 5.4, ovan. Det finns inte några tydliga särskiljande drag mellan detta scenario och scenario 5.4 som ger vid handen att några andra slutsatser skulle dras. I de allra flesta fall har sponsorn, etablerad utanför EU/EES, bestämt alla förutsättningar och är därför att betrakta som personuppgiftsansvarig.

En överföring av personuppgifter till sponsorn innebär dock att dessa uppgifter överförs till tredjeland. Sådan överföring är förbjudet enligt artikel 44 GDPR om inte vissa förutsättningar är uppfyllda som ska säkerställa att de registrerades rättigheter inte undergrävs, vilket kan ske då deras uppgifter överförs till ett land som saknar lagstiftning av motsvarande skyddsnivå som GDPR.

Området är komplext och har gjorts mer komplext på senare år genom EU-domstolens dom i det så kallad Schrems II-målet[56] som inneburit en skärpning av praxis vad gäller ansvaret för de personuppgiftsansvariga att faktiskt se till att det finns effektiva skyddsåtgärder för de registrerade och inte enbart förlita sig på att ett ingånget avtal med kommissionens standardavtalsklausuler (de så kallade SCC standard contractual clauses[57]). En sådan skyddsåtgärd som även föreslås av den Europeiska dataskyddstyrelsen (EDPB) är att

[55] En annan fråga kan vara vilka möjligheter som finns att med verkan faktiskt rikta rättsliga anspråk mot en organisation som inte är etablerad inom en medlemsstat, men denna fråga berörs inte närmare inom ramen för denna rapport.
[56] Mål Court of Justice of the European Union, C-311/18 https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_sv.
[57] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

alla uppgifter som överförs till tredjeland är pseudonymiserade och att mottagaren därmed i praktiken har svårare att avgöra vilken fysisk person uppgifterna är hänförliga till.

Det saknas utrymme att beröra frågan mer än så inom ramen för denna rapport. Det bör understrykas att en noggrann bedömning måste ske i varje enskilt fall, både vad avser vilket land personuppgifter avses överföras till och huruvida det finns en laglig grund att göra detta. Situationen kan föranleda krav på att vidta ytterligare skyddsåtgärder, utöver användningen av kommissionens standardavtalsklausuler. Användningen av pseudonymisering kan betraktas som en skyddsåtgärd som, kombinerat med andra åtgärder (som att kommissionens standardavtalsklausuler för överföring till tredjeland ingås mellan parterna), kan göra det möjligt att faktiskt överföra uppgifter till sponsorn i ett tredjeland.

5.8.3 Behov av avtal

Om behandlingen genomförs av en konstellation där sponsorn anses vara personuppgiftsansvarig och prövarna endast personuppgiftsbiträde så krävs enligt GDPR ett personuppgiftsbiträdesavtal (PUB-avtal) som närmare reglerar personuppgiftsbiträdets behandling av personuppgifter. Ett sådant avtal ska finnas mellan sponsorn och var och en av prövarna. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna. Den koordinerande prövaren anses inte ha något större ansvar än övriga prövare. Personuppgiftsansvaret utgår från sponsorn och det är därför sponsorn som har att avtala om delegering av behandlingen av personuppgifter. Notera att det är fullt möjligt att ha ett avtal direkt mellan en svensk organisation och en utländsk sådan.

Om behandlingen genomförs av en konstellation där flera av de ingående parterna anses vara gemensamt personuppgiftsansvariga så kräver GDPR att det finns ett inbördes arrangemang. Det torde vara mycket lämpligt, men inte strikt tvingande, att detta arrangemang regleras genom ett skriftligt avtal om gemensamt personuppgiftsansvar mellan parterna där det närmare framgår vem som har att hantera vilken del av personuppgiftsansvaret. Det bör även innehålla gemensamt framtagna instruktioner kring vem som ska utföra vad i samband med personuppgiftsbehandlingen. Särskilt när antalet aktörer är högt torde det vara i princip nödvändigt att tydliggöra vilken part som har att ta olika delar av personuppgiftsansvaret, till exempel vad gäller rapportering av personuppgiftsincidenter eller säkerställande av att tillräckliga säkerhetsåtgärder har vidtagits. Det ska understrykas att gemensamt personuppgiftsansvar innebär ett solidariskt ansvar, vid en eventuell tillsyn har alltså alla ingående aktörer skyldighet att se till att de registrerades rättigheter tillvaratas på ett säkert sätt. Om en tillsyn skulle leda till en administrativ sanktionsavgift eller om en registrerad har skadeståndsanspråk så kan sådana avgifter eller skadestånd riktas mot vilken som helst av de ingående parterna. För mer information om arrangemanget se avsnitt 3.3, ovan.

Oaktat vilken slags avtal som ska upprättas mellan parterna är det av vikt att det inom ramen för det avtalet framgår särskilt vilka krav som ställs på överföringen av information som kommer att ske till tredjeland.

5.9 Extern hantering av data

5.9.1 Scenariobeskrivning

Forskningstyp:	• Detta är ett generellt scenario, det vill säga scenariot är inte specifikt för viss typ av forskning.
Aktörer:	• En forskare skickar data till en extern part för bearbetning, analys eller annan hantering. Efter utfört uppdrag skickas all data tillsammans med ev. analyser tillbaka till forskaren. Ingen data finns kvar hos den externa parten.
Kommentar:	• Den aktör som ska utföra analysen ska genomföra analysen utifrån ett protokoll eller en prövningsplan. • Den externa parten kan finnas både inom och utanför EU/ESS.

5.9.1.1 Illustration av scenario 5.9

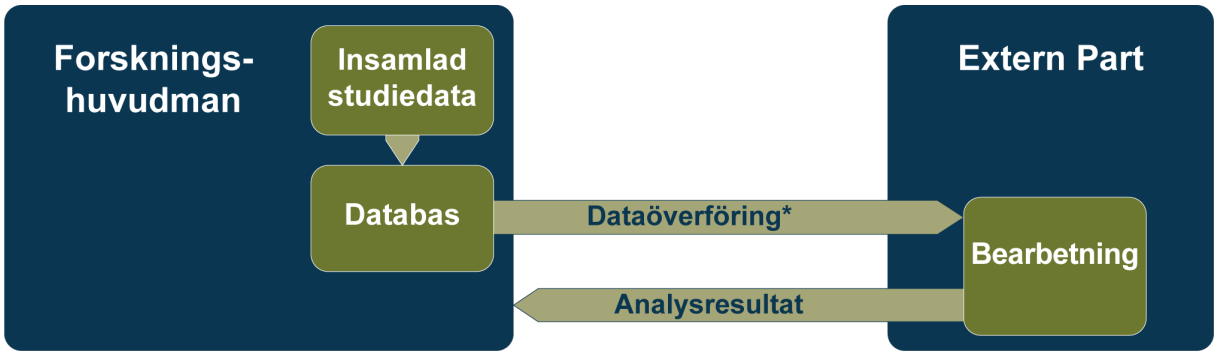


Bild 5.9: Datainsamling samt databasens placering och databearbetning (som till exempel analys) sker inom olika huvudmän. *överföring bör ske kodat/ pseudonymiserat.

5.9.2 Personuppgiftsansvarets fördelning

Scenariot beskriver en analys.

Uttrycklig behörighet

Det saknas reglering som ger någon av parterna en uttryckligen behörighet avseende personuppgiftsansvar. Det finns alltså inte någon specifik lag som pekar ut ett personuppgiftsansvar i detta fall.

Underförstådd behörighet

Vad avser underförstådd behörighet kan konstateras att det inte framkommit någon branschpraxis vad gäller hantering av personuppgiftsansvaret vid dataanalyser.

Det kan dock konstateras att det i EU:s dataskyddsmyndigheters rekommendationer (EDPB) har rekommenderat att när en aktör utför en hantering av personuppgifter enbart utifrån den andre aktörens begäran och inte själv har någon egentlig möjlighet att påverka vilka personuppgifter det handlar om eller vad det är för någon behandling som ska utföras så tyder detta på ett personuppgiftsbiträdesförhållande.

Faktiskt inflytande

Situationen som beskrivs utgår från att analysen utförs av analysföretaget helt i enlighet med det uppdrag som givits dem. När analysen är genomförd kommer resultatet av analysen samt den information som analysen är genomförd på att återbördas till beställaren.

Personuppgiftsansvar: Den externa parten har inte bedömts ha någon egentlig inverkan eller beslutsmandat när det gäller den praktiska behandlingen av personuppgifter mer än att utföra den analys som beställaren har uppdragit. Enbart det faktum att en leverantör erbjuder en på förhand bestämd typ av tjänst, till exempel en viss analys av en viss slags information, innebär inte att det är leverantören som bestämmer och förfogar över behandlingen av de aktuella personuppgifterna som utförs. Tvärtom behandlar leverantören dessa enbart utifrån den erbjudna tjänsten. Leverantören har inte någon möjlighet att till exempel använda sig av personuppgifterna för att slutföra en annan kunds analys.

Sammantaget ter sig scenariot vara att bedöma som en typisk situation där den personuppgiftsansvarige ger en annan part i uppdrag att utföra en viss behandling. När uppdraget är slutfört ska personuppgifterna återbördas till den personuppgiftsansvarige. Analysföretaget är därför att betrakta som personuppgiftsbiträde och uppdragsgivaren som personuppgiftsansvarig.

5.9.3 Behov av avtal

Eftersom behandlingen utgör en personuppgiftsbiträdessituation så krävs enligt GDPR ett personuppgiftsbiträdesavtal (PUB-avtal) som närmare reglerar personuppgiftsbiträdets behandling av personuppgifter. Ett sådant avtal måste finnas mellan uppdragsgivaren och det externa analysparten. Till avtalet bör även finnas instruktioner som mer i detalj beskriver vilka åtgärder som får vidtas och till exempel vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna.

Om den externa parten är etablerad utanför EU/EES kan en överföring av personuppgifter till den externa parten innebära att dessa uppgifter överförs till tredjeland. Sådan överföring är förbjuden enligt artikel 44 GDPR om inte vissa förutsättningar är uppfyllda som ska säkerställa att de registrerades rättigheter inte undergrävs, vilket kan ske då deras uppgifter överförs till ett land som saknar lagstiftning av motsvarande skyddsnivå som GDPR.

Området är något komplext och har gjorts mer komplext på senare år genom EU-domstolens dom i det så kallad Schrems II-målet[58] som inneburit en skärpning av praxis vad gäller ansvaret för de personuppgiftsansvariga att faktiskt se till att det finns effektiva skyddsåtgärder för de registrerade och inte enbart förlita sig på att ett ingånget avtal med kommissionens standardavtalsklausuler (de så kallad SCC standard contractual clauses[59]). En sådan skyddsåtgärd som även föreslås av den Europeiska dataskyddstyrelsen (EDPB) är att alla uppgifter som överförs till tredjeland är pseudonymiserade och att mottagaren därmed i praktiken har svårare att avgöra vilken fysisk person uppgifterna är hänförliga till.

Det saknas utrymme att beröra frågan mer än så inom ramen för denna rapport. Det bör understrykas att en noggrann bedömning måste ske i varje enskilt fall, både vad avser vilket land personuppgifter avses överföras till och huruvida det finns en laglig grund att göra detta. Situationen kan föranleda krav på att vidta ytterligare skyddsåtgärder, utöver användningen av kommissionens standardavtalsklausuler. Användningen av pseudonymisering kan betraktas som en skyddsåtgärd som, kombinerat med andra åtgärder (som att kommissionens standardavtalsklausuler för överföring till tredjeland ingås mellan parterna), kan göra det möjligt att faktiskt överföra uppgifter till sponsorn i ett tredjeland.

[58] Mål Court of Justice of the European Union, C-311/18 https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_sv.
[59] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

5.10 Klinisk forskning – Utlämnade av data från vårdgivare till forskningshuvudman

5.10.1 Scenariobeskrivning

Forskningstyp:	• Forskning som kräver godkännande från Etikprövningsmyndigheten.
Aktörer:	• En forskningshuvudman begär att data från en vårdgivare ska utlämnas för en specifik forskningsstudie.
Kommentar:	• Vårdgivaren har i detta scenario ingen del i forskningen. Vårdgivarens roll är endast att journalinformation finns bevarad hos vårdgivaren och begärs utlämnad från densamme.

5.10.1.1 Illustration av scenario 5.10

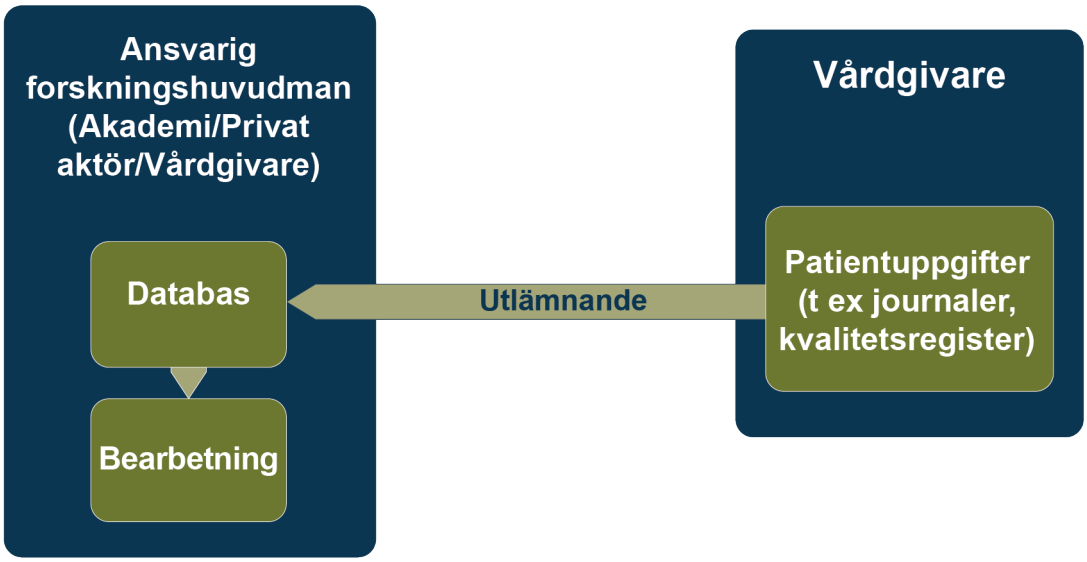


Bild 5.10: Patientuppgifter är insamlade inom en vårdgivare. Utlämnade data placeras i en databas hos en annan huvudman där databearbetning (som till exempel analys) även sker.

5.10.2 Personuppgiftsansvarets fördelning

I detta scenario finns det endast en forskningshuvudman. Denne forskningshuvudman behöver underlag i form av patientuppgifter från journaler, kvalitetsregister etcetera och begär denna data utlämnad från en eller flera vårdgivare. Vårdgivare lämnar ut begärda uppgifter efter en sekretessprövning och är sedan inte involverade i forskningsprojektets vidare analys eller hantering av patientuppgifterna.

Uttrycklig behörighet

Det saknas författningsreglering som ger någon av parterna en uttryckligen behörighet avseende personuppgiftsansvar. I etikprövningslagen anges att godkänd forskning får innebära behandling av personuppgifter, men inte någon konkret bestämmelse om vem som har ansvaret för behandlingen. Av 6 § framgår att forskningshuvudmannen ska vidta åtgärder för att förebygga att forskning i den egna verksamheten utförs i strid med de villkor som meddelas, i övrigt pekas egentligen inget ansvar ut.

Patientuppgifterna utlämnas från vårdgivaren, en offentlig myndighet, och som på begäran har en skyldighet att utlämna allmänna handlingar utifrån offentlighetsprincipen. Utlämnandet sker alltså inte som ett led i ett gemensamt forskningsprojekt utan utgör en del av myndighetens uppgift. PDL pekar ut

vårdgivaren som personuppgiftsansvarig för behandlingen av personuppgifter inom ramen för hälso- och sjukvård. Personuppgiftsansvaret innefattar även utlämnande av personuppgifter inom ramen för offentlighetsprincipen[60]

Underförstådd behörighet

Hanteringen är att betrakta som en samordnad behandling i den bemärkelse att den består av flera på varandra följande moment. En aktör samlar in personuppgifterna för ändamålet att överlämna dem. En annan aktör tar emot uppgifterna för ändamålet att hantera dem i ett forskningsprojekt. Även om båda dessa aktörer är inblandade i den samordnade behandlingen är de inte delaktiga i respektive motparts behandling. Det står således klart att den aktör som samlar in och lämnar ut personuppgifterna är ansvarig för dessa behandlingar. Vidare är den aktör som mottar uppgifterna ansvarig för alla behandlingar som denne utför efter att överföringen har skett. Vad gäller ansvaret för själva överföringen är situationen mer komplicerad. I vissa fall kan det vara lämpligt att betrakta utlämnande och mottagande aktör som gemensamt personuppgiftsansvariga för själva överföringen, förutsatt att de tillsammans bestämmer ändamålen och medlen för överföringen. I detta fall är det dock en myndighet som lämnar ut personuppgifter som en led i sitt åtagande enligt offentlighetsprincipen. Det torde dessutom vara myndigheten som är den aktör som har att ställa eventuella säkerhetskrav avseende på vilket sätt utlämnandet tekniskt ska ske. Det är därför troligt att det är vårdgivaren som är personuppgiftsansvarig fram till dess att personuppgifterna är inom forskningshuvudmannens kontroll.

Faktiskt inflytande

Utifrån vad som framkommit i workshops [61] är det tydligt att detta scenario utgår från en situation när forskningsprojektet inte är ett gemensamt projekt och där aktörerna inte gemensamt vare sig planerar eller bestämmer innehållet i projekt eller protokoll. Det kan förvisso vara så att det funnits en dialog mellan organisationerna tidigare och att till exempel förfrågan om ”feasability” (studieförfrågning) gjorts från forskningshuvudmannen till vårdgivaren, men det innebär inte att det finns något gemensamt åtagande eller bestämmande kring själva forskningshypotesen eller forskningsprotokollet.

Personuppgiftsansvarig är: I detta scenario är det tydligt att forskningshuvudmannen och vårdgivaren har separata personuppgiftsansvar för den respektive behandling de utför.

Forskningshuvudmannen är personuppgiftsansvarig för den behandling som sker av personuppgifterna inom ramen för forskningsprojektet som Etikprövningsmyndigheten godkänt. Vårdgivaren är personuppgiftsansvarig för den behandling som sker av personuppgifterna inom ramen för insamlande och utlämnade av allmänna handlingar i enlighet med den av forskningshuvudmannen ställda begäran.

Särskild kommentar kring anställning hos flera huvudmän

Även om scenariot ter sig tydligt kan det ofta förekomma att enskilda medarbetare som är engagerade i forskningsprojektet är anställda av såväl vårdgivaren som ett universitet. Detta kan leda till en otydlighet avseende vilken organisation som faktiskt hanterar personuppgifterna vid olika tillfällen i processen. I sådana fall är det av synnerlig vikt att det är mycket tydligt vilken organisation medarbetaren agerar som representant för när personen befattar sig med personuppgifterna eller fattar beslut inom kring hanteringen av dessa. Det torde också vara att rekommendera att personer som har ett direkt intresse i det aktuella forskningsprojektet inte är samma personer som har att besluta om utlämnandet av sagda uppgifter från vårdgivaren.

[60] PDL 5 kap 1 §.
[61] Se avsnittet 1.3 Utförande för beskrivning hur scenarier tagits fram och arbetet i övrigt bedrivits.

5.10.3 Behov av avtal

Mot bakgrund av att parterna agerar utifrån varsitt separat personuppgiftsansvar torde det inte finnas något lagstadgat krav på avtal vad gäller hantering av personuppgifterna.

Däremot bör det finnas en dokumenterad process för hanteringen av informationsflödet särskilt då informationen ska passera sekretessgränser genom utlämnande från vårdverksamheten till en extern part så att kraven om sekretessprövning och utlämnande tillgodoses. Även om det inte finns något krav i lag är det även generellt rekommenderat att ingå ett så kallad datautlämningsavtal med mottagande part när personuppgifter överförs från en part till en annan.[62]

Det ska här särskilt kommenteras att överföringar i dessa fall ofta har sin grund i att uppgifter begärs ut från en offentlig organisation, som till exempel en region, och därmed utlämnas inom ramen för offentlighetsprincipen enligt Tryckfrihetsförordning (1949:105) 2 kap 1 §. I dessa situationer kan den utlämnande parten bara under särskilda omständigheter villkora ett utlämnande. Oavsett detta finns det all anledning att i samband med ett sådant utlämnande påpeka och påminna om det ansvar som mottagaren har när det kommer till att hantera känsliga uppgifter och vilka informationssäkerhetsmässiga krav som den utlämnande myndigheten själv anser bör tillämpas. I de fall utlämnandet sker till en enskild (alltså privat) aktör kan ett utlämnande även villkoras, ett så kallat utlämnande med förbehåll. Dessa villkor kan utgöras av tystnadsplikt att informationen endast får användas på visst sätt eller annat.

[62] Med datautlämningsavtal menas här ett så kallad data transfer agreement. Ett avtal som ingås mellan två parter som skickar information till varandra, där det i avtalet kan finnas villkor för hur informationen får hanteras, vilka säkerhetsåtgärder som ska vidtas etc. Det är inte ett avtal som syftar till att reglera personuppgiftsansvaret i sig (dvs. inte ett så kallad personuppgiftsbiträdesavtal (artikel 28.3 GDPR) eller avtal om gemensamt personuppgiftsansvar (artikel 26.1 GDPR)).

6 Avslutande ord

6.1 Målsättning

Sedan GDPR började gälla istället för personuppgiftslagen har lagstiftningen kring personuppgiftsbehandling och dataskydd fått ett allt större utrymme inom den allmänna diskursen. Inte minst införandet av administrativa sanktionsavgifter som avskräckande effekt har inneburit att effekten av att inte följa gällande lag en direkt mätbar kostnad vilket tidigare saknades. Det innebär i praktiken att det blir allt viktigare för alla parter att ha kännedom om och vara medvetna om vilken roll ens organisation har i samband med överföring och behandling av personuppgifter, detta är inte minst viktigt inom ramen för klinisk forskning.

Det förtjänar också att uppmärksamma att just personuppgiftsansvar och hur olika aktörer inom ramen för klinisk forskning är ett område där tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY) tidigare haft invändningar främst vad gäller den information som ges till deltagare i forskningsprojekt och då till stor del just vilka organisationer som ingår i ett forskningsprojekt och vem som är personuppgiftsansvarig för dessa.[63] Det finns och har också funnits en osäkerhet kring dessa frågor i branschen och det vore därför också en stor fördel om en samsyn kunde uppnås.

Ambitionen med föreliggande rapport är att bidra till en mer enhetlig bedömning av personuppgiftsansvarets placering i samband med olika typer av klinisk forskning. Placeringen av personuppgiftsansvar har en central betydelse för all hantering av personuppgifter då många av skyldigheterna i GDPR utgår från just den personuppgiftsansvarige.

I samband med remissrundor av rapporten har det inkommit synpunkter kring att ett införande av gemensamt personuppgiftsansvar mellan deltagande forskningsaktörer i stor omfattning skulle förändra det sätt organisationerna för närvarande arbetar och det avtalsstrukturer som används idag. Det är självklart på det sättet att en förändrad syn på personuppgiftsansvarets placering måste få effekter på hur organisationerna hanterar avtalsskrivning, men också själva behandlingen av personuppgifter. Det säger sig självt att en samling personuppgifter som behandlas i egenskap av personuppgiftsbiträde eller tillsammans med andra parter inom ramen för ett gemensamt personuppgiftsansvar måste hanteras på ett annat sätt än sådana personuppgifter som organisationen har ett ensamt ansvar för, inte minst påverkas organisationens handlingsutrymme att ensamt bestämma om olika frågor kring uppgifternas hantering. Den bedömning som görs i rapporten är att GDPR och den rättspraxis som utvecklats under senare år tyder på ett större utrymme för att tillämpa ett gemensamt personuppgiftsansvar inom områden där flera aktörer är inblandade för att gemensamt behandla informationsmängder för ett mål där samtliga dessa aktörer har ett intresse.

6.2 Framtida arbete

Förslag på avtal för gemensamt personuppgiftsansvar

En detalj av stor betydelse i situationer där det finns ett gemensamt personuppgiftsansvar är det ”inbördes arrangemang mellan gemensamt personuppgiftsansvariga” som ska utformas enligt artikel 26.1 GDPR.

Som ett fortsatt kompletterande arbete till denna rapport kommer därför ett förslag på utformning av avtal för gemensamt personuppgiftsansvar tas fram som kan användas i de fall flera parter bedöms ha ett gemensamt personuppgiftsansvar och därmed behöva formalisera deras inbördes arrangemang. Erfarenhetsmässigt förekommer det många exempel på utformningar av personuppgiftsbiträdesavtal, men betydligt färre exempel på avtal för gemensamt personuppgiftsansvar. Bedömningen är därför att det

[63] Se bland annat IMY:s beslut diarienummer 581-2014 och 559-2014, https://www.imy.se/globalassets/dokument/beslut/press-150703-roche-ab.pdf, https://www.imy.se/globalassets/dokument/beslut/press-150703-pfizer-ab.pdf.

skulle vara av stort mervärde att i vart fall stommen för ett sådant togs fram i mallformat för olika huvudmän att använda som utgångspunkt.

Beskrivning av legala förutsättningar för åtkomst till hälsodata inom ramen för klinisk forskning

Bedömningen av vilken organisation som är personuppgiftsansvarig är en viktig del av de juridiska frågorna kring klinisk forskning. En annan fråga, av minst lika stor betydelse, är vilka förutsättningar det finns att få åtkomst till eller på annat sätt ta del av personuppgifter inom hälso- och sjukvården för användning inom ramen för klinisk forskning och vilka lagar och regler som påverkar detta. Under remissrundan för den aktuella rapporten har många av frågeställningarna kretsat kring just utlämning eller överföringen av personuppgifter från till exempel patientjournaler till forskningsprojekt, vad det egentligen innebär personuppgiftsbehandlings-mässigt och vem det är inom en organisation som har att besluta om sådana överföringar. För att tydliggöra detta, men samtidigt säkerställa att frågeställningarna kring dessa frågor inte sammanblandas med bedömningen av personuppgiftsansvaret vid klinisk forskning kommer en separat utredning att tas fram som närmare redogör för dessa frågor.

Beskrivning av överföring till tredjeland och säkerhetsåtgärder som kan vidtas

GDPR innebär att det finns starka etablerade skydd för behandlingen av personuppgifter i de länder där GDPR gäller. För att säkerställa att detta skydd upprätthålls finns det särskild reglering i GDPR om överföring av personuppgifter till länder som saknar ett lika starkt skydd för personuppgifter som GDPR. Sådana länder kallas i lagstiftningen för *tredjeland.*

En överföring av personuppgifter till ett annat land är särskilt reglerat i GDPR. Något förenklat kan det sägas att GDPR förbjuder överföringar till länder som inte har motsvarande garantier för skyddet av personuppgifter som GDPR ger inom EU. Personuppgifter får därför föras över endast om det finns en adekvat skyddsnivå i mottagarlandet eller om det finns särskilda garantier för att uppgifterna och de registrerades rättigheter skyddas (trots att det tredjelandets lagstiftning saknar samma skydd).

I princip finns alltså ett förbud mot överföring [64]av uppgifter till ett land utanför EU om inte ”adekvat nivå av skydd” finns för uppgifterna. Vad som menas då är inte säkerhetsåtgärder i första hand utan att det i landet finns ett juridiskt skydd för uppgifterna, alltså adekvat lagstiftning. Om så inte är fallet kan detta ”överbryggas” genom att den personuppgiftsansvarige avtalsmässigt ser till att det skydd som landets lagar saknar upprätthålls genom ett avtal mellan den ansvarige och den som ska behandla uppgifterna (vanligen ett personuppgiftsbiträde). Ett sådant standardavtal kallas för *kommissionens standardvillkor* och innebär att skyldigheterna som GDPR genom lag ställer på en aktör nu civilrättsligt ställs mellan de båda parterna.

Genom den så kallade SchremsII-domen[65] som EU-domstolen avkunnade 2020 fastställdes att den så kallade privacy shield[66] mellan EU och USA om säker personuppgiftsbehandling ogiltigförklarades. Det gjordes också klart att den personuppgiftsansvarige inom EU verkligen måste göra en bedömning av vilken risk det innebar att överföra personuppgifter till ett tredjeland och vidta tillräckliga skyddsåtgärder som verkligen skyddade personuppgifterna. Det anses därmed inte längre tillräckligt att enbart ingå kommissionens standardvillkor och nöja sig med det (vilket i mångt och mycket i praktiken varit fallet innan SchremsII).

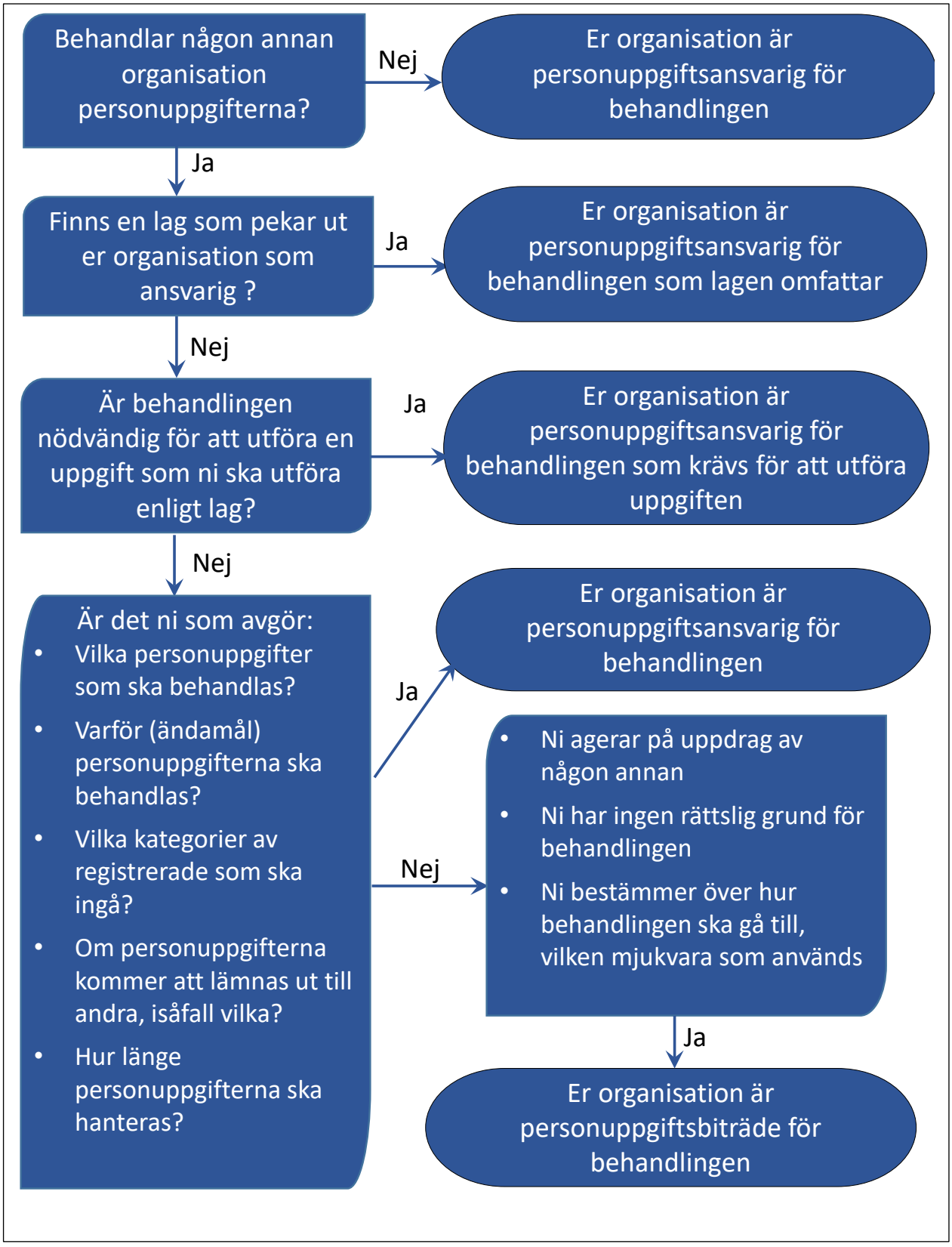
[64] Begreppet överföring omfattar all åtkomst till personuppgifter som kan ske från ett tredjeland. Om en person som befinner sig i ett tredjeland till exempel har elektronisk åtkomst genom ett inloggningsförfarande till personuppgifter inom EU genom anses alltså en överföring ha skett.
[65] Dom i mål C-311/18 Data Protection Commissioner/Maximillian Schrems och Facebook Ireland.
[66] Privacy Shield var en slags ackrediteringsförfarande som något förenklat innebar att amerikanska företag som anslutit sig till Privacy Shield ansågs ha vidtagit tillräckliga skyddsåtgärder och att förbudet mot överföring till tredjeland därmed inte längre var tillämpligt avseende dessa företag.

EDPB har tagit fram riktlinjer kring överföring av personuppgifter till tredjeland och hur man som personuppgiftsansvarig ska resonera och vilka bedömningar och åtgärder man är skyldig att vidta.[67] EDPB anger i riktlinjerna som exempel på tekniska skyddsåtgärder som kan vidtas är kryptering och pseudonymisering av personuppgifter.

Kliniska forskningsstudier innebär inte sällan att personuppgifter behöver delges till aktörer som befinner sig ett annat land, i många fall utanför EU och inte helt sällan länder som inte anses ha samma skydd för personuppgifter och således är att betrakta som tredje länder. Frågan är då i vilken utsträckning de verkligen är juridiskt möjligt att överföra personuppgifter i dessa situationer. Frågeställningen är komplex och utgångspunkten är att en bedömning ska ske i varje enskilt fall. Med det sagt kan det tänkas att många av frågeställningarna samt också lösningsalternativen i form av skyddsåtgärder är desamma i flera fall och det skulle därför finnas ett behov av en gemensam kartläggning av hur frågan bör bedömas inom ramen för olika scenarier inom klinisk forskning. Det föreslås därför att en framtida rapport tas fram som uteslutande fokuserar på just tredjelandsöverföring.

[67] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.
Notera att EDPB i Use Case 2 sid 31bedömer att pseudonymisering av personuppgifter kan utgöra effektiva skyddsåtgärder vid överföring till tredjeland inom ramen för en personuppgiftsbehandling för ändamålet forskning.

Bilaga 1: Flödesschema för bedömning av personuppgiftsansvar



Bilaga 2: Ordlista och begreppsförklaring

Begrepp (*Term*)	Beskrivning och anmärkning	Källa och lagrum
Avtal om gemensamt personuppgiftsansvar	Ett avtal som reglerar det inbördes arrangemang som ska gälla mellan parterna som delar ett gemensamt personuppgiftsansvar. Av detta inbördes arrangemang ska särskilt former och ansvar för utövande av den registrerade personens (försökspersonens) rättigheter samt förpliktelsen att lämna information till registrerade personer framgå.	Lagrum: Artikel 25 p. 1 GDPR. Notera att här regleras endast att det ska finnas ”ett inbördes arrangemang” mellan parterna. Uttrycket ”avtal om gemensamt personuppgiftsansvar” nämns inte.
Behandling av personuppgifter	all hantering av personuppgifter: “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”.	Dataskyddsförordningens definition Lagrum: *GDPR, Artikel 4 p. 2 GDPR.*
Case Report Form (”CRF”)	Ett tryckt, optiskt eller elektroniskt dokument avsett att dokumentera all information avseende varje försöksperson som ska rapporteras till sponsorn enligt prövningsprotokollet. ***Anmärkning***: kan även benämnas som ”datainsamlingsformulär”.	GCP: *§ 1.11.*
Contract Research Organisation (”CRO”)	En person eller organisation (kommersiell, akademisk eller annan) anlitad av sponsorn för att genomföra en eller flera av sponsorns uppgifter.	GCP: *§ 1.20.*
Datautlämningsavtal	Med datautlämningsavtal menas här vad som internationellt brukar kallas ett data transfer agreement. Ett avtal som ingås mellan två parter som skickar information till varandra, där det i avtalet kan finnas villkor för hur informationen får hanteras, vilka säkerhetsåtgärder som ska vidtas, hur informationen ska hanteras vid avtalets slut etcetera Det är inte ett avtal som syftar till att reglera personuppgiftsansvaret i sig (dvs. inte ett så kallad personuppgiftsbiträdesavtal (artikel 28.3 GDPR) eller avtal om gemensamt personuppgiftsansvar (artikel 26.1 GDPR))	Projektets egen benämning.
Eftergivande av sekretess	Den vars uppgifter skyddas av sekretess samtycker till att uppgifter kan röjas.	Lagrum: *OSL 12 kap. 2 §.*
Forskningshuvudman	En statlig myndighet eller en fysisk eller juridisk person i vars verksamhet forskningen utförs.	Lagrum: *Lag (2003:460) om etikprövning av forskning som avser människor, 2 §.*
Forskningsperson	En levande människa som forskningen avser.	Lagrum: *Lag (2003:460) om etikprövning av forskning som avser människor, 2 §.*
Försöksperson	En patient eller annan person som deltar i en klinisk läkemedelsprövning och som antingen får prövningsläkemedel eller som ingår i en	Läkemedelsverket: *LVFS 2011:19 1 kap. 3 § c.* Lagrum:

Begrepp (*Term*)	Beskrivning och anmärkning	Källa och lagrum
	kontrollgrupp. ***Anmärkning***: kan även benämnas som ”forskningsperson”, men i regelverken anges fortfarande ”försöksperson”.	*Artikel 2 i CTD.* *Artikel 2.17 CTR.* GCP: *§ 1.53.*
God klinisk sed (Good Clinical Practice)(”GCP”)	Internationellt erkända etiska och vetenskapliga kvalitetskrav som ska beaktas vid utformning, genomförandet, registreringen och rapporteringen av kliniska läkemedelsprövningar där försökspersoner medverkar.	ICH E6 (R2) Good Clinical Practice (GCP).
Huvudman	det landsting eller den kommun som enligt lagen ansvarar för att erbjuda hälso- och sjukvård inom ett geografiskt område.	Socialdepartementet: *Hälso- och sjukvårdslag | 2017, 2 kap. Definitioner* lagrum: *Hälso- och sjukvårdslag (2 kap 2 §).*
Informerat samtycke till att delta i ett forskningsprojekt	I etikprövningslagen framgår att samtycket ska vara frivilligt, uttryckligt och preciserat till viss forskning. Dessutom ska samtycket dokumenteras.	Lagrum: *Lag (2003:460) om etikprövning av forskning som avser människor, 17 §.*
Informerat samtycke till läkemedelsprövning	beslut, som skall vara skriftligt, daterat och undertecknat, om att delta i en klinisk prövning vilket fattas frivilligt, av en person som har blivit vederbörligen informerad om prövningens art, omfattning, konsekvenser och risker och erhållit lämplig dokumentation om denne är förmögen att lämna sitt samtycke eller, i annat fall, av personens lagliga ställföreträdare. Om den berörda personen är oförmögen att skriva kan i undantagsfall ett muntligt samtycke lämnas i närvaro av minst ett vittne, i enlighet med den nationella lagstiftningen.	Lagrum: *Artikel 2 j CTD.* *Jfr reviderad legaldefinition i Artikel 2.14 CTR.* *Jfr GCP § 1.28.* *Nuvarande lagrum avseende beslutsoförmögna är Läkemedelslag (2015:315) 7 kap 3 §. CTR kommer erhålla nationell kompletterande lagstiftning som berör detta.*
Koordinerande prövare	Den prövare som har ansvar för att den prövningsrelaterade verksamheten vid de olika prövningsställe som deltar i en multicenterprövning utförs på ett enhetligt sätt.	Lagrum: Läkemedelsverkets föreskrifter: *LVFS 2011:19 1 kap. 3 § j.*
Multicenterprövning	En klinisk läkemedelsprövning som genomförs enligt samma prövningsprotokoll men på flera prövningsställen och därigenom av mer än en prövare.	Läkemedelsverket: *LVFS 2011:19 1 kap. 3 § k.* Lagrum: *Artikel 2 b CTD.* *Artikel 2.15 CTR.* GCP: *§ 1.40.*
Offentlig vårdgivare	statlig myndighet, landsting och kommun i fråga om sådan hälso- och sjukvårdsverksamhet som myndigheten, landstinget eller kommunen har ansvar för.	*Termbanken Socialstyrelsen* Lagrum: *PDL (1 kap 3 § PDL).*
Patient	person som erhåller eller är registrerad för att erhålla hälso- och sjukvård	Socialstyrelsen: *Socialstyrelsens termbank (2016).*
Patientuppgift	All information som direkt eller indirekt kan kopplas till en person som erhåller eller är registrerad för att erhålla hälso- och sjukvård ***Anmärkning:*** Patientuppgift är inte ett juridiskt definierat begrepp. Det används vanligtvis för att förtydliga att de personuppgifter som är aktuella är de som omfattas av patientdatalagen.	
Personuppgift	all information som direkt eller indirekt kan kopplas till en fysisk person som är i livet	Socialstyrelsens termbank (2016) Lagrum: *Artikel 4 p. 1 GDPR art 4 p 1.*

Begrepp (*Term*)	Beskrivning och anmärkning	Källa och lagrum
	Anmärkning: Inom ramen för PDL omfattas även avlidna personers personuppgifter.	
Personuppgiftsansvarig	den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål personuppgifter ska behandlas för och hur behandlingen ska gå till. ***Anmärkning***: Det är normalt organisationen som är personuppgiftsansvarig, inte chefen på en arbetsplats eller en anställd som i sitt arbete hanterar personuppgifterna. Även en fysisk person kan vara personuppgifts-ansvarig vilket till exempel är fallet för enskilda firmor.	Integritetsskyddsmyndigheten: *Ordlista* Lagrum: Begreppet finns även definierat i artikel 4 p7 (GDPR).
Privat vårdgivare	annan juridisk person (än statlig myndighet, landsting eller kommun) eller enskild närings-idkare som bedriver hälso- och sjukvårds-verksamhet.	*Termbanken Socialstyrelsen* lagrum: *Patientedatalagen (1 kap 3 §).*
Prövare	Legitimerad läkare eller legitimerad tandläkare som genomför en klinisk läkemedelsprövning på ett prövningsställe. Om en prövning genomförs av en grupp av Individer på ett prövningsställe, är prövaren den som är ansvarig ledare för gruppen.	Läkemedelsverket: *LVFS 2011:19 1 kap. 3 § q.* Lagrum: *Artikel 2 f CTD.* *Artikel 2.15 CTR.* GCP: *§ 1.34.*
Prövningsställe	En vårdinrättning där prövningsrelaterade aktiviteter utförs på försökspersonerna.	Läkemedelsverket: *LVFS 2011:19 1 kap. 3 § p.* GCP: *§ 1.59.*
Samtycke	Varje slag av frivillig, särskilt och otvetydig viljeyttring genom vilken patienten, efter att ha fått information, godtar åtgärder, registrering eller informationsöverföring som rör honom/henne. Samtycket kan ske genom ett uttalande eller en entydig bekräftande handling.	Integritetsskyddsmyndighetens ordlista och GDPR Lagrum: *GDPR, Aartikel 4 p. 11 GDPR.*
Samtycke till behandling av personuppgifter enligt GDPR	Att individen samtycker till behandling av personuppgifter och detta samtycke utgör den rättsliga grunden för den personupp-giftsansvariges hela hantering av person-uppgifterna.	Följer av betydelsen av samtycke som rättslig grund i GDPR.
Sekretess	Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Sekretess är en beteckning för information som normalt inte ska lämnas ut och därför inte blir allmänt tillgänglig.	*Offentlighets och sekretesslag (OSL)* Lagrum: *OSL 3 kap 1§.*
Sponsor	Den person, det företag, den institution eller organisation som ansvarar för att initiera, organisera eller finansiera en klinisk läkemedelsprövning.	Läkemedelsverket: *LVFS 2011:19 1 kap. 3 § m.* Lagrum: *Artikel 2 h CTD.* *Artikel 2.14 CTR.* GCP: *§ 1.53.*
Utlämning av personuppgift	lämna ut information som direkt eller indirekt kan kopplas till en fysisk person som är i livet från en organisation till en extern part.	

Begrepp (*Term*)	Beskrivning och anmärkning	Källa och lagrum
Vårdgivare	statlig myndighet, landsting, kommun, annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet.	Socialdepartementet: *Hälso- och sjukvårdslag | 2017, 2 kap. Definitioner* Lagrum: *Hälso- och sjukvårdslag (2 kap 3 §).*
Vårdrelation/Patient-relation	Vårdrelation innebär att medarbetare aktivt deltar i vården av en patient. Vårdinsatsen kan vara direkt; det vill säga medarbetare som själv utför vården eller indirekt; medarbetare blir konsulterad angående vården av patienten. Det kan också gälla administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall. ***Anmärkning***: begreppet är inte juridiskt definierat men avses oftast omfatta vad som ingår i begreppet ”deltar i vården av en patient” vilket innebär behörighet att ta del av patientens journal inom den inre sekretessen enligt 4 kap 1 § patientdatalagen.	Lagrum: *PDL 4 kap 1 § PDL.*

Bilaga 3: Begreppsbildning vid forskning och klinisk prövning

1. Begreppsbildning vid forskning och klinisk prövning.

I denna rapport används begreppet klinisk prövning eftersom det är det begrepp som används i EU-lagstiftning samt svenska författningar.

En klinisk prövning är en undersökning för att studera effekten av ett läkemedel eller behandlingsmetod på friska eller sjuka människor. Exempelvis kan en prövning syfta till att utvärdera en substans lämplighet som läkemedel eller till studie på olika behandlingars effekt.

Klinisk prövning skiljer sig från hälso- och sjukvård. Hälso- och sjukvård ska bedrivas i enlighet med vetenskap och beprövad erfarenhet i enlighet med hälso- och sjukvårdslagen,[68] patientlagen,[69] och patientsäkerhetslagen[70] med flera. Vid klinisk prövning ska andra bestämmelser tillämpas och kravet på vetenskap och beprövad erfarenhet gäller inte för behandlingar som prövas inom ramen för en klinisk prövning.

Det kan också vara av betydelse att dra någon gräns mot vad som betecknas som klinisk prövning i den utsträckning detta utgör en klinisk prövning av ett framtaget läkemedel eller medicinteknisk produkt där denna produkt ska testas för att avgöra om den har avsedd effekt jämfört med annan forskning som kan bedrivas inom ramen för hälso- och sjukrådsområdet, som till exempel registerforskning eller annan forskning som utgår från levande människor. Merparten av de internationella regelverk som är framtagna och som redogörs för i denna PM utgår från just området klinisk prövning av läkemedel och medicintekniska produkter. Eftersom dessa regelverk utgör en viktig legal grund i att definiera olika parters ansvarsområde, vilket kommer har betydelse för bedömningen av personuppgiftsansvarsfrågan, redogörs de för här. Det är dock viktigt att komma ihåg att när det gäller andra former av klinisk forskning (som till exempel registerforskning) kan dessa regelverk rimligen främst användas som en allmänt accepterad syn på vad som är god klinisk sed.

2. Regelverk klinisk prövning

Det moderna regelverket om klinisk prövning kan i all väsentlighet spåras till den så kallad neurosedyn-skandalen på 1960-talet. Sedan dess har regelverket kontinuerligt skärpts och utvecklats. Det finns en långtgående internationell standardisering av hur klinisk prövning ska genomföras; framför allt genom standarden god klinisk sed (Good Clinical Practice)[71] som utvecklas av europeiska, amerikanska och japanska läkemedelsmyndigheter. En stor del av de begrepp som finns i EU-lagstiftning och i svenska författningar utgår därför från en internationell definition och syftet är att dessa begrepp ska användas enhetligt.

Det finns ett flertal regelverk som tar sikte på särskilda kategorier av klinisk prövning: särskilt klinisk läkemedelsprövning och prövning innefattande medicintekniska produkter.

[68] Hälso- och sjukvårdslag (1982:763).
[69] Patientlag (2014:821).
[70] Patientsäkerhetslag (2010:659).
[71] ICH E6 (R2) Good Clinical Practice.

3. Ansvarsfördelningen i klinisk prövning

God klinisk sed utgår från två nyckelfunktioner: **sponsorn** och **prövaren**. Syftet med dessa två funktioner är att etablera en tydlig och ändamålsenlig ansvarsfördelning inom ramen för kliniska prövningar. Sponsorn och prövaren har fått ett visst *ansvar* genom lag men har lämnats utrymme att delegera *arbetsuppgifter* genom skriftliga avtal, ansvaret kan dock inte delegeras.

Sponsorn och prövaren är inte de enda funktionerna inom klinisk prövning men särskiljer sig från flera övriga funktioner i och med det att de har en särskild rättslig ställning avseende klinisk prövning.

Enligt den Europeiska läkemedelsmyndigheten har den ökade användningen av olika aktörer genom olika avtalskonstruktioner medfört att ansvarsfördelningen vid klinisk prövning blir komplex och svår att överblicka. Det medför även att det bildas en viss diskrepans vid begreppsbildningen. Mot den bakgrunden är det nödvändigt för aktörerna att tydligt reglera det aktuella ansvarsförhållandet. Det sker bland annat genom det skriftliga avtal som ska finnas mellan aktörerna (och att detta avtal uppfyller kraven enligt god klinisk sed), prövningsprotokollet samt att den information som lämnas till Etikprövningsmyndigheten är fullständig och korrekt.[72]

3.1 Sponsor

En klinisk prövning initieras av en sponsor med ansvar för att inleda, leda och ordna med finansieringen av den aktuella prövningen. Sponsorn har med andra ord det *övergripande ansvaret* för att genomföra den kliniska prövningen. Genom god klinisk sed finns det en icke-uttömmande lista över sponsorns ansvar. Det är sponsorn som har ansvaret för att den datakvalitet och integritet i den data som samlas in inom ramen för prövningen. Detta ansvar inbegriper särskilt instruktioner för kvalitetskontroll (monitorering), instruktioner för kvalitetssäkring (auditering) samt att den kliniska prövningen följer prövningsprotokollet. Sponsorn har med andra ord ansvar att genom monitorering kontrollera att prövaren genomför prövningen korrekt.

En sponsor får, genom ett skriftligt avtal, delegera någon eller alla sina arbetsuppgifter till en enskild person, ett företag, en institution eller en organisation. Delegationen ska inte påverka sponsorns ansvar, särskilt avseende försökspersonernas säkerhet. Materiella krav på hur delegation av arbetsuppgifter ska ske uppställs i god klinisk sed.

Instruktioner om prövningens syfte (*varför*) och genomförande (*hur*) lämnas i ett prövningsprotokoll. Prövningsprotokollet är det dokument som beskriver vilka syften den kliniska prövningen har, hur den är utformad och vilken metod som ska användas samt vilka statistiska överväganden som gjorts och hur prövningen är upplagd. Det vetenskapliga ändamålet stadgas med andra ord i prövningsprotokollet.

En sponsor får anlita en så kallad Contract Research Organization (”**CRO**”). Vad som utgör en CRO är inte definierat i lag utan definieras genom god klinisk sed. CRO definieras som en organisation (kommersiell, akademisk eller annan) till vilken en sponsors ansvar överlåtits, helt eller delvis. Annorlunda uttryckt utgör en CRO med andra ord en *outsourcad* del av sponsorns funktion. En CRO behöver inte vara en kommersiell aktör vilket framgår av begreppsdefinitionen. Även en akademisk institution kan därför vara en CRO.

3.2 Prövare

Det är prövaren som har ansvaret för den kliniska prövningens genomförande utifrån prövningsprotokollet på en vårdinrättning (ett så kallad prövningsställe), det vill säga en **site**. Det är med andra ord sponsorn som har det övergripande ansvaret för hela prövningen; prövaren är forskaren som har ansvaret för prövningens genomförande på en vårdinrättning.

[72] https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-clinical-practice/qa-good-clinical-practice-gcp (hämtad 2020-05-20).

En klinisk prövning som genomförs på mer än en vårdinrättning, och därmed omfattar flera prövare, är en så kallad **multicenterprövning**. Vid en multicenterprövning ska det finnas en koordinerande prövare. Vid en multinationell multicenterprövning kan det finnas en nationell koordinerande prövare (”**NCI**”). Oaktat om prövningen genomförs av en eller flera prövare (och därmed om den sker på en vårdinrättning eller är en multicenterprövning) ska prövningen genomföras enligt *ett* prövningsprotokoll. Mot den bakgrunden har en koordinerande prövare ansvaret för att den prövningsrelaterade verksamheten utförs på enhetligt sätt.

En prövare är en legitimerad läkare eller tandläkare med sakkunskap inom den kliniska prövningens vetenskapliga ändamål. Med andra ord är prövaren alltid en fysisk person. Det finns inget hinder mot att sponsorn är prövare, notera dock att sponsorn kan vara en juridisk person (ett företag, en institution eller en organisation). Prövarens arbetsuppgifter är att genomföra prövningen på vårdinrättningen enligt prövningsprotokollet. Denna arbetsuppgift innebär särskilt:

- att säkerställa att försökspersonerna har ett fullgott skydd för sina rättigheter, sin integritet och sitt välbefinnande,
- att försökspersonerna får den vård och uppföljning efter deltagandet i prövningen har avslutats,
- att säkerställa att det är god kvalitet i allt arbete och data.

Sponsorn ska kontrollera prövarens efterlevnad genom extern kvalitetskontroll (monitorering/ övervakning).

Den vårdenhet vid vilken prövaren verkar eller är anställd har enligt god klinisk sed det ansvar som framgår av nationell författning. Det medför bland annat att det är forskningshuvudmannen – och inte prövaren – som ska ansöka om etikprövning (se avsnitt 4, nedan), att det är organisationen som prövar frågor om offentlighet och sekretess (innefattande utlämnande av data) samt att personuppgiftsansvaret enligt GDPR är placerat på organisationsnivå.

4. Ansökan om godkännande av klinisk prövning

En klinisk prövning (precis som annan forskning som sker på människor och biologiskt material från människor) ska genomgå etisk granskning av Etikprövningsmyndigheten (tidigare regionala etikprövningsnämnder) efter ansökan från forskningshuvudmannen. Etikprövningsmyndigheten genomför en prövning utifrån etikprövningslagen.[73] Vid en multinationell multicenterprövning ska etikprövning ske av den del av prövningen som sker i Sverige.

5. Insamling och behandling av data vid klinisk prövning

5.1 Samtycke

Det finns olika definitioner av samtycke: *informerat samtycke* till deltagande i den kliniska prövningen enligt god klinisk sed, samt *samtycke* enligt GDPR (se Bilaga 2: Ordlista och begreppsförklaring). Enligt etikprövningslagen ska forskningshuvudmannen samla in försökspersonernas samtycke till deltagande i prövningen. Vid så kallad registerforskning finns det inget krav på försökspersonens samtycke.

5.2 Insamling av data

Det är som regel prövaren som har uppgiften att samla in data inom ramen för klinisk prövning. Frågor om utlämnande av data omfattas, såvida att forskningshuvudmannen är en svensk myndighet, av

[73] Lagen (2003:460) om etikprövning av forskning avseende människor.

offentlighets- och sekretesslagen (”**OSL**”).[74] Ansvaret för behandling av personuppgifter inom ramen för klinisk prövning är placerat på organisationsnivå.

Data kan avse källdata (source data) och källdokument (source documents). Med källdokument avses dokument i original, data och observationer som till exempel patientjournal, minnesanteckningar, fotografier, röntgenkopior med mera. Källdata är innehållet i källdokument förutsatt att källdokumentet är en originalhandling eller en verifierad kopia.

5.2.1 Sekretess enligt OSL

Forskning är ett ämnesområde som faller utanför den ordinarie verksamhetsområdet inom hälso- och sjukvården. Mot den bakgrunden får data som behandlas för ändamålet att vårda en patient inte behandlas och utlämnas till verksamhetsområdet forskning. I den mån som upplysningar ska utlämnas från en verksamhetsgren till en annan krävs en menprövning och ett formellt beslut om utlämnande enligt OSL.

Inom hälso- och sjukvården är huvudregeln att sekretess gäller för uppgifter om en persons hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Det är alltså OSL:s bestämmelser som avgör om patientuppgifter får utlämnas från en offentlig vårdgivare. Varje vårdgivare ska självständigt ta ställning till om efterfrågade uppgifter får lämnas ut.

Som regel krävs två utlämnanden från verksamhetsområde hälso- och sjukvård till verksamhetsområde forskning: (1) utlämnande av upplysningar för upprättande av ett register avseende personer som förklarat sig intresserade av att delta i prövningen, samt (2) utlämnande av upplysningar för den specifika kliniska prövningen.

Som regel disponerar en patient själv över sina egna uppgifter. När en patient vill delta i en klinisk prövning kan han eller hon efterge den sekretess som finns för patientens uppgifter hos vårdgivaren. En sådan eftergift gör det möjligt för vårdgivaren att lämna ut uppgifter till den som ska bedriva en klinisk prövning. Eftergivande av sekretess görs oftast i samband med att patienten lämnar sitt informerade samtycke till att delta i prövningen.

Som framgår av definitionen till försökspersonen kan denne vara en patient eller en annan person (så kallad friska frivilliga). Det är med andra ord inte nödvändigt att upplysningar utlämnas från hälso- och sjukvården. Andra datakällor kan till exempel vara akademiska institutioner.

5.2.2 Behandling av personuppgifter

Inom hälso- och sjukvården regleras behandlingen av personuppgifter i patientdatalagen.[75] Forskning kan inte ske inom ramen för de ändamål som stadgas i patientdatalagens ändamålskatalog (som avgränsar vilka ändamål personuppgifter får behandlas för). Behandling av personuppgifter regleras därför avseende forskning, genom GDPR och, förutsatt att forskningen sker inom ramen för ett verksamhetsställe i Sverige, av den svenska dataskyddslagen.[76] Notera således att den svenska dataskyddslagen kan vara tillämplig på behandling av personuppgifter som inte samlats in i Sverige och som inte heller avser personer i Sverige.

För *särskilda kategorier* av personuppgifter (i svensk lagstiftning fortsatt kallade känsliga personuppgifter) finns ytterligare bestämmelser i GDPR. Särskilda kategorier av personuppgifter är uppgifter som avslöjar ras eller etniska ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i

[74] Offentlighets- och sekretesslag (2009:400).
[75] Patientdatalag (2008:355).
[76] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Huvudregeln är att behandling av känsliga personuppgifter är förbjuden. Det finns dock bestämmelser om undantag från förbudet, bland annat för behandling av känsliga personuppgifter i vetenskaplig forskning. Ett villkor för att forskning som innehåller känsliga personuppgifter ska vara laglig är att det finns ett godkännande från Etikprövningsmyndigheten. Detsamma gäller för forskning innefattande personuppgifter om lagöverträdelser.

5.3 Registrering av data i ett eCRF vid klinisk prövning

Syftet med klinisk prövning är att generera tillförlitliga och robusta källdata. I syfte att strukturera insamlingen av studiedata används vanligen ett elektroniskt Case Report Form (”**eCRF**”). Ett eCRF är ett strukturerat datainsamlingsverktyg som genererar en databas som skapas för analys. Det finns inget hinder mot att ett manuellt CRF används; det förutsätter dock att data därefter registreras elektroniskt i en databas.

Ett CRF ska kompletteras av en Data Management Plan (”**DMP**”) och en Data Validation Plan (”**DVP**”). Därigenom ska det bland annat finnas en plan för hur data samlas in, märks, och vem som har behörig åtkomst till data. Hur data ska samlas in användas och skyddas genom tekniska och organisatoriska åtgärder regleras genom ett omfattande antal bestämmelser enligt god klinisk sed.

5.4 Utlämning av data till sponsorn vid klinisk prövning

Källdata som samlats in inom ramen för den kliniska prövningen ska utlämnas till sponsorn utifrån prövningsprotokollet och god klinisk sed. Som redovisats ovan är beslutet om utlämnande av data placerat på organisationsnivå, och inte på prövaren, enligt nationell rätt. Utlämnade data ska kodas av prövaren på så sätt att sponsorn inte kan identifiera de försökspersoner som utlämnad data avser. Kopplingen mellan utlämnad data och försökspersonens identitet ska säkras genom en så kallad kodlista. Denna kodlista bevaras viss tid av prövaren beroende på ett antal faktorer (till exempel om läkemedlet övergår i produktion vid en klinisk läkemedelsprövning).

Kodning av data medför som regel att pseudonymisering, utifrån GDPR:s legaldefinition, sker.[77] Med *pseudonymisering* avses en behandling av personuppgifter som innebär att personuppgifterna inte längre kan tillskrivas en specifik fysisk person utan att kompletterande uppgifter används under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person. Med pseudonymiserad avses alltså exempelvis att identitet på patient eller försöksperson ersätts med ett löpnummer. En lista med löpnummer och identitet förvaras sedan separat. Förfarandet kallas även ibland kodat eller anonymiserat. Det är viktigt att understryka att förfarandet inte innebär att uppgifterna är avidentifierade (i denna mening används då begreppet avidentifierad som att uppgifterna är omöjliga att hänföra till en person).[78] Uppgifterna är fortfarande personuppgifter eftersom de kan härledas till en person genom kodlistan.

[78] Det är viktigt att känna till att många av begreppen anonymiserad, avidentifiera, pseudonymiserad, kodad m.m. används på olika sätt av olika aktörer. Det är därför mycket viktigt att vara tydlig med vad som avses. ”Pseudonymiserad” är numera ett begrepp som definieras i GDPR och bör endast användas i enlighet med denna definition. Övriga begrepp är inte juridiskt definierade och bör därför alltid förtydligas. Normalt inom dataskydd är att betrakta avidentifierad som en personuppgift som inte längre på något sätt kan härledas till en individ (vare sig direkt eller indirekt) och uppgiften är därför inte längre att betrakta som en personuppgift.

Utlämning av pseudonymiserade personuppgifter utgör sannolikt ett utlämnande av personuppgifter.[79] Det medför i sin tur att sponsorns behandling av utlämnande kodade personuppgifter utgör behandling av personuppgifter. Det förutsätter att det finns grund i författning för utlämnandet.

5.5 Prövarens bevarande av data vid klinisk prövning

All information som rör den kliniska prövningen ska registreras, behandlas, hanteras och lagras av sponsorn, eller prövaren om tillämpligt, så att den kan rapporteras, tolkas och kontrolleras på ett korrekt sätt. Utgångspunkten är därför att det är sponsorns ansvar att bevara insamlad och genererade data. Prövaren har dock också en skyldighet enligt god klinisk sed att lagra en oberoende kopia av den data som utlämnats till sponsorn för att i efterhand möjliggöra en kontroll.

Data som samlats in inom ramen för en vårdgivares verksamhet enligt hälso- och sjukvårdslagen omfattas av vårdgivarens skyldighet att föra patientjournal. Sådan data utgör en del av patientens journal och ska därför bevaras enligt patientdatalagen.

[79] Justitieombudsmannen (JO) nr 6794-2017 (kritik Region Halland för överföring av personuppgifter till ett tredjeland). Jfr Datainspektionens beslut dnr 811-2011 (föreläggande mot Göteborg universitet för Svensk nationell datatjänst (”SND”)).