



Personuppgifter i genforskning – uppföljning av förhandskontroller

DATAINSPEKTIONENS RAPPORT 2002:4

1. Inledning	2
2. Sammanfattning	3
3. Personuppgiftslagen	5
3.1 Allmänt	5
3.2 Några grundläggande begrepp	5
3.2.1 <i>Behandling</i>	5
3.2.2 <i>Personuppgift</i>	6
3.2.3 <i>Personuppgiftsansvar</i>	7
3.2.4 <i>Känsliga personuppgifter</i>	8
4. När får man använda känsliga personuppgifter i forskningen?	10
4.1 Utan samtycke endast i vissa fall	10
4.2 Med informerat samtycke	11
4.2.1 <i>Forskningsetisk prövning av informerat samtycke</i>	11
4.2.2 <i>Samtycke enligt personuppgiftslagen</i>	12
4.2.3 <i>Information</i>	13
4.2.4 <i>Särskilt om överföring till tredje land</i>	18
4.2.5 <i>Särskilt om biobanker</i>	19
4.2.6 <i>Uppgifter om släktingar</i>	20
5. Förhandskontroll	21
5.1 Varför förhandskontroll?	21
5.2 Vilka behandlingar skall anmälas för förhandskontroll?	21
5.3 Vad skall anmälan innehålla?	22
5.4 Handläggningen vid Datainspektionen	23
5.5 Vad innebär Datainspektionens beslut?	24
5.6 Säkerhetsföreskrifter	25
6. IT-säkerhet	26
6.1 Allmänt	26
6.2 Personuppgiftsbiträde	26
7. Övrigt	29
7.1 Skydd för företagshemlig information?	29

Bilagor

1. Inledning

Under våren och hösten 2002 har Datainspektionen genomfört ett tillsynsprojekt i syfte att följa upp ett antal personuppgiftsbehandlingar som anmälts för förhandskontroll, under främst år 2001. De behandlingar som valdes ut var sådana där Datainspektionen hade haft synpunkter på den information som skulle lämnas till de registrerade. Totalt granskades 36 forskningsprojekt hos 14 personuppgiftsansvariga genom fältinspektioner. Vilka dessa är framgår av bilaga 1. Inspektionerna inriktades på att granska om den patientinformation som slutligen använts i respektive projekt hade anpassats efter de synpunkter som Datainspektionen lämnat i sitt beslut, samt om säkerhetsföreskrifterna följdes. Samtliga granskade projekt avsåg genetiska forskningsstudier.

Inspektionerna är avslutade och varje personuppgiftsansvarig har fått ett beslut.

Under år 2001 anmäldes 73 behandlingar av personuppgifter för forskningsändamål till Datainspektionen för förhandskontroll. I stort sett samtliga anmälningar avsåg genetiska forskningsstudier. Datainspektionen lämnade i många av sina beslut synpunkter på hur informationen till de registrerade skulle vara utformad för att uppfylla personuppgiftslagens krav. I samtliga ärenden meddelade Datainspektionen säkerhetsföreskrifter.

Stockholm i december 2002

2. Sammanfattning

Syftet med projektet har varit att följa upp Datainspektionens beslut efter förhandskontroll av personuppgiftsbehandling för forskningsändamål och kontrollera om de personuppgiftsansvariga följer inspektionens synpunkter i besluten. Det är anmärkningsvärt många som väljer att inte följa besluten. Följden blir att känsliga personuppgifter behandlas utan att ett giltigt samtycke inhämtats och utan att deltagarna fått tillräcklig information.

För den enskilde som har för avsikt att medverka i en forskningsstudie är det viktigt att få information inte bara om de medicinska riskerna utan också om vad som händer med hans eller hennes oftast mycket känsliga personuppgifter. Den enskilde skall ha klart för sig vem eller vilka som skall ha tillgång till uppgifterna och till vad de skall användas. Vidare måste den enskilde få veta vem som ytterst ansvarar för att personuppgifterna behandlas i enlighet med lagen och för att de har ett tillräckligt skydd. När det gäller uppgifter om genetiska anlag är det dessutom svårt att bedöma vilken betydelse de kan få på sikt. Informationen till de registrerade är därför särskilt viktig.

I de granskade forskningsprojekten är det i flera fall oklart vem som är personuppgiftsansvarig. Känsliga personuppgifter behandlas utan att det är utrett vem som bär det yttersta ansvaret för att behandlingen sker i enlighet med personuppgiftslagen och för att uppgifterna har ett tillräckligt skydd.

Den personuppgiftsansvarige har ett ansvar för att information om personuppgiftslagen sprids och förankras i organisationen. Den personuppgiftsansvarige är skyldig att se till att instruktionerna är tydliga och att ingen otillåten behandling sker. Personuppgiftsombuden har här en viktig roll och det har märkts tydligt i vilka fall ombuden varit aktiva i arbetet med att ta fram ny information till patienterna.

När det gäller IT-säkerheten har syftet med inspektionerna varit att granska huruvida de personuppgiftsansvariga följer de meddelade säkerhetsföreskrifterna. Vid inspektionerna har kunnat konstateras att läkemedels- och forskningsföretagen har en hög säkerhetsnivå och ett väl utvecklat säkerhetstänkande. När det gäller den forskning som bedrivs vid universitet/sjukhus eller liknande har det varit svårare att bedöma säkerheten eftersom projekten i många fall inte påbörjats eller varit på en ännu blygsam nivå. Där har inspektionerna fått inriktas på att diskutera vilken säkerhetsnivå som planeras. I flera fall har personuppgiftsansvaret varit oklart, vilket har inneburit att det inte heller funnits någon självklart huvudansvarig för IT-säkerheten.

Det är vanligt att personuppgifter datorbehandlas utanför den personuppgiftsansvariges direkta kontroll – exempelvis av ett privat företag – och då saknas i flera fall avtal som reglerar säkerheten. Även om de enskilda forskarna som regel är noggranna med att skydda uppgifterna måste det vara klart vem som ytterst ansvarar för säkerheten.

Mot bakgrund av vad som angivits har Datainspektionen utformat denna rapport för att klargöra Datainspektionens roll och närmare förklara vad besluten i förhandskontrollärendena innebär. Vidare redogörs för skillnaden mellan den prövning som görs i de forskningsetiska kommittéerna och Datainspektionens bedömning, främst när det gäller kraven på vad ett informerat samtycke skall innefatta

I anslutning till varje avsnitt redovisas de iakttagelser som Datainspektionen har gjort i samband med tillsynen.

3. Personuppgiftslagen

3.1 Allmänt

Personuppgiftslagen (PuL) trädde i kraft hösten 1998 men började gälla fullt ut den 1 oktober 2001. Lagen gäller när man behandlar (på något sätt hanterar) personuppgifter helt eller delvis automatiserat, det vill säga helt eller delvis i datorformat. Lagen grundar sig på ett EG-direktiv¹ och syftet är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. En viktig förändring med den nya lagstiftningen är att det tidigare tillståndsförfarandet är borttaget. Datainspektionen meddelar inte längre tillstånd att föra personregister. Det är istället de personuppgiftsansvariga själva som har ansvar för att tolka och följa reglerna i personuppgiftslagen.

I personuppgiftslagen har tonvikt lagts vid den enskildes samtycke och rätt till insyn. De personuppgiftsansvariga har ålagts en omfattande informations-skyldighet gentemot de registrerade.

Forskning på människor styrs av en relativt omfattande reglering, såväl internationell som nationell. Exempel på sådan är Helsingforsdeklarationen, Good Clinical Practice, forskningsetiska riktlinjer och Läkemedelsverkets föreskrifter. I den mån personuppgifter behandlas inom ramen för ett forskningsprojekt gäller *dessutom* personuppgiftslagen. Den som ägnar sig åt forskning måste således även följa personuppgiftslagens bestämmelser.

Om personuppgifter om genetiska anlag kommer att behandlas inom ramen för en forskningsstudie skall alltid anmälan för förhandskontroll ske, se avsnitt 5.

I personuppgiftslagen förekommer en del begrepp som det finns anledning att närmare förklara.

3.2 Några grundläggande begrepp

3.2.1 *Behandling*

Begreppet behandling av personuppgifter omfattar alla åtgärder som kan vidtas med sådana uppgifter såsom insamling, registrering, organisering, lagring, bearbetning och utlämnande genom översändande.

¹ Europaparlamentets och rådets direktiv 94/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

3.2.2 Personuppgift

Personuppgifter är enligt lagens definition all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Uppgifter om avlidna eller ännu inte födda personer omfattas följaktligen inte av personuppgiftslagen.

Varje information som kan hänföras direkt eller indirekt till en fysisk person är en personuppgift. Det krävs bara att en fysisk person kan identifieras med hjälp av uppgifterna. Kodade uppgifter omfattas därmed också av lagen så länge det finns en kodnyckel bevarad med vars hjälp det är möjligt att identifiera enskilda individer. Det saknar betydelse var och hos vem kodnyckeln förvaras. Detsamma gäller krypterade uppgifter.

Om det inte längre finns någon som helst möjlighet att koppla uppgifterna till en enskild person är det dock inte längre fråga om personuppgifter och personuppgiftslagen är följaktligen inte tillämplig. Det kan vara aktuellt i de sällsynta fall då kodnycklarna har förstörts eftersom det inte finns något behov av att i efterhand kunna härleda resultaten till enskilda personer.

Även om kodnyckeln har förstörts kan det dock ibland ändå vara möjligt att identifiera enskilda individer. I vissa fall kan nämligen uppgifter direkt hänföras till en så begränsad grupp personer att en enskild individ med hjälp av andra uppgifter enkelt kan identifieras. Uppgifterna får då betraktas som personuppgifter.

Datainspektionens iakttagelser:

En vanlig missuppfattning var att endast namn och personnummer utgör personuppgifter och att kodade uppgifter inte är personuppgifter.

I en av de inspekterade studierna framkom att det inte längre fanns någon koppling till enskilda individer när de genetiska analyserna utfördes.

Någon framförde farhågor för att det kan bli svårt att rekrytera deltagare i studien om det står i informationen att personuppgifter skall behandlas trots att det endast är fråga om kodade uppgifter.

Datainspektionens synpunkter:

Att koda personuppgifterna är en säkerhetsåtgärd som dock inte innebär att materialet är avidentifierat. Så länge det finns en möjlighet att identifiera enskilda individer är det ändå fråga om personuppgifter i lagens mening. Det finns därmed också ett behov av att skydda uppgifterna.

Utförs de genetiska analyserna först när det inte längre finns någon koppling till enskilda individer är det inte nödvändigt att anmäla den aktuella forskningsstudien för förhandskontroll. Personuppgiftslagen är dock tillämplig på den personuppgiftsbehandling som utförs fram till dess att kodnycklarna förstörs.

3.2.3 Personuppgiftsansvar

Personuppgiftsansvarig är enligt lagens definition den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Så snart personuppgifter behandlas finns det en eller flera som är ansvariga för den behandlingen. Vem som är personuppgiftsansvarig bestäms utifrån de faktiska omständigheterna i det enskilda fallet. Man måste bedöma vem eller vilka som faktiskt har bestämt över personuppgiftsbehandlingen.

Det är oftast inte en fysisk person som är personuppgiftsansvarig för en viss behandling. Istället brukar det vara en juridisk person – exempelvis ett bolag – som ytterst bestämmer vilka uppgifter som skall behandlas och vad de skall användas till. När det gäller forskningsstudier som utförs på sjukhus är det i många fall inte landstinget som är personuppgiftsansvarigt utan istället ett universitet eller ett forskningsinstitut. Varje enskild studie måste dock bedömas för sig.

Det är den personuppgiftsansvarige som har ansvaret för att all behandling av personuppgifter sker i enlighet med bestämmelserna i personuppgiftslagen och därtill anknytande reglering. Den personuppgiftsansvarige ansvarar för säkerheten vid behandlingen. Den personuppgiftsansvarige är vidare skyldig att ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat².

Datainspektionens iakttagelser:

Frågan om vem som egentligen är personuppgiftsansvarig för personuppgiftsbehandlingen i forskningsprojekten var ofta föremål för utredning redan i samband med att behandlingen anmäldes för förhandskontroll. Ofta angavs en enskild forskare – exempelvis kontaktpersonen för studien – som personuppgiftsansvarig. I de fall anmälan hade passerat personuppgiftsombudet innan den skickades in till Datainspektionen verkade dock frågan som regel ha utretts av personuppgiftsombudet. I flera fall visade det sig dock i efterhand att någon

² 48 § personuppgiftslagen

annan än den som uppgetts vara personuppgiftsansvarig i anmälan om förhandskontroll, var ansvarig för behandlingen.

Många gånger angav forskarna sig själva eller den egna kliniken som personuppgiftsansvarig. Vid en närmare granskning visade det sig dock ofta att det var ett universitet eller ett forskningsinstitut som var personuppgiftsansvarigt.

Datainspektionens synpunkter:

När en anmälan om förhandskontroll ges in till Datainspektionen skall frågan om vem som är personuppgiftsansvarig för den aktuella studien vara utredd och klar. Det är den eller de personuppgiftsansvariga själva som känner till de faktiska omständigheterna i det enskilda fallet och som kan göra en korrekt bedömning.

Det är av största vikt att reda ut frågan eftersom det har betydelse för vem som har det skadeståndsrättsliga ansvaret enligt PuL för att behandlingen sker i enlighet med lagen och för att de känsliga personuppgifterna är tillräckligt skyddade. Det bör därför finnas rutiner i organisationen för att sprida information om personuppgiftslagen. En god rutin kan vara att låta samtliga anmälningar passera personuppgiftsombudet. Det är dock angeläget att betona att varje behandling alltid måste bedömas för sig.

3.2.4 Känsliga personuppgifter

Känsliga personuppgifter är sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse och medlemskap i fackförening. Vidare är personuppgifter som rör hälsa och sexualliv känsliga. Det har i lagen inte gjorts någon åtskillnad mellan olika typer av sjukdomar utan alla personuppgifter som rör hälsa anses känsliga.

Enligt huvudregeln³ är det förbjudet att behandla känsliga personuppgifter utan den registrerades samtycke. Förbudet är straffsanktionerat.⁴ Det finns dock flera undantag från förbudet. Det är alltid tillåtet att behandla känsliga personuppgifter med den registrerades samtycke, varom mer nedan. Utan samtycke är det tillåtet bland annat för hälso- och sjukvårdsändamål. Vidare kan det undantagsvis vara tillåtet att, under vissa förutsättningar, behandla känsliga personuppgifter utan samtycke för särskilt angelägna forskningsprojekt.

³ 13 § personuppgiftslagen

⁴ 49 § b) personuppgiftslagen

Datainspektionens iakttagelser:

Det förekom att uppgifter om vissa sjukdomar inte uppfattades som känsliga personuppgifter.

Datainspektionens synpunkter:

Alla personuppgifter som rör hälsa är känsliga i lagens mening. Vissa sjukdomar kan i och för sig upplevas som särskilt känsliga men personuppgiftslagen gör ingen skillnad mellan sjukdomar.

4. När får man använda känsliga personuppgifter i forskningen?

4.1 Utan samtycke endast i vissa fall

Under vissa förutsättningar är det tillåtet att behandla känsliga personuppgifter för forskningsändamål utan att de registrerade samtyckt till behandlingen. Ett grundläggande krav är att den aktuella behandlingen är nödvändig för det aktuella forskningsändamålet. Forskning innebär sådan verksamhet som bedrivs vid etablerade institutioner såsom universitet eller privata väletablerade forskningsinstitut. Det måste finnas ett samhällsintresse av att forskningen bedrivs och den skall vara vetenskaplig. Samhällsintresset av det forskningsprojekt där behandlingen ingår skall klart överväga risken för otillbörligt intrång i enskildas personligas integritet. En avvägning skall således ske och en helhetsbedömning göras av samtliga omständigheter. Vid bedömningen beaktas bland annat följande; projektets vikt, behovet av personuppgifter, säkerheten vid behandlingen, kostnaden och tidsåtgången för att inhämta samtycke, i vilken utsträckning den enskilde kan skadas av att samtycke begärs, om information kan lämnas, eventuell strykningrätt, det vill säga rätten att förklara samt hur pass svårt det är att identifiera enskilda personer.

Om en forskningsetisk kommitté har godkänt personuppgiftsbehandlingen anses avvägningen som beskrivits ovan ha skett och behandlingen är automatiskt tillåten enligt PuL. En forskningsetisk prövning har förutsatts vara regel när det gäller denna typ av behandlingar och tillämpningen skall vara restriktiv. I de fall en forskningsetisk kommitté inte har godkänt behandlingen skall anmälan för förhandskontroll göras om deltagarna i projektet inte heller har samtyckt till personuppgiftsbehandlingen.

Datainspektionens iakttagelser:

Det var ovanligt att de forskningsetiska kommittéerna uttryckligen tog ställning till den personuppgiftsbehandling som förekom inom ramen för studien.

Samtliga studier som inspekterats uppgavs vara genomförda med stöd av informerat samtycke till personuppgiftsbehandlingen. Datainspektionen har bara mottagit någon enstaka anmälan rörande studier som är tänkta att genomföras utan samtycke från de registrerade.

Datainspektionens synpunkter:

I sina beslut tar etikkommittéerna sällan uttryckligen ställning till personuppgiftsbehandlingen i de forskningsprojekt som de granskar. Det framgår oftast inte heller av ansökan eller övriga handlingar om behandlingen av personuppgifter har omfattats av etikkommitténs bedömning. Detta innebär

att Datainspektionen ofta i sina beslut efter förhandskontroll förutsätter att behandlingen av personuppgifter inte har godkänts av den etiska kommittén. Om det förekommer att de etiska kommittéerna faktiskt tar ställning också till personuppgiftsbehandlingen inom ramen för studien skulle det underlätta handläggningen om detta också framgick av beslutet. Eftersom en personuppgiftsbehandling som godkänts av en etisk kommitté utan vidare är tillåten enligt personuppgiftslagen skall Datainspektionen därför inte i samband med förhandskontrollen göra en ny prövning enligt personuppgiftslagen. Observera att detta inte påverkar skyldigheten att anmäla genetiska forskningsstudier för förhandskontroll. En anmälan måste alltså göras även om Datainspektionen efter anmälan inte gör någon ny prövning.

4.2 Med informerat samtycke

Om känsliga personuppgifter skall användas i en forskningsstudie med stöd av informerat samtycke från deltagarna måste informationen och samtycket uppfylla vissa krav som anges i personuppgiftslagen.

4.2.1 *Forskningsetisk prövning av informerat samtycke*

När en forskningsetisk kommitté granskar ett projekt är det ovanligt att kommittén granskar deltagarinformationen och samtycket med utgångspunkt från personuppgiftslagen. Det finns inga formella krav på att de forskningsetiska kommittéerna skall göra en sådan prövning. De riktlinjer som finns för den forskningsetiska prövningen⁵ innehåller visserligen krav på vad ett informerat samtycke skall innefatta. För närvarande finns dock, såvitt framgått, inga rekommendationer om att också beakta personuppgiftslagens särskilda krav. Konsekvensen blir att informationen till patienter granskas av såväl Datainspektionen som den forskningsetiska kommittén, delvis utifrån skilda utgångspunkter. Även om kommittén har godkänt informationen innebär det därför inte att den med automatik också uppfyller kraven i personuppgiftslagen.

De flesta studier som anmäls för förhandskontroll görs med stöd av informerat samtycke – godkänt av etikkommitté – från de registrerade. Det finns därför anledning att närmare precisera vilka krav personuppgiftslagen ställer på ett informerat samtycke.

⁵ Se exempelvis Riktlinjer för etisk värdering av medicinsk humanforskning i Sverige, Forskningsetisk policy och organisation i Sverige, MFR – Rapport 2 2000

4.2.2 Samtycke enligt personuppgiftslagen

Ett samtycke som uppfyller personuppgiftslagens krav skall vara

- frivilligt
- särskilt och
- informerat, det vill säga lämnat efter det att information om behandlingen givits.

Att ett samtycke skall vara särskilt innebär att ett generellt samtycke till behandling av personuppgifter inte kan godtas. Den enskilde skall informeras om en eller flera behandlingar och därefter samtycka till dessa specificerade behandlingar.

Samtycket skall vidare vara en

- otvetydig viljeyttring.

Det senare innebär bland annat att så kallat *tyst samtycke* där den registrerade informeras om en viss behandling och ges en viss frist att motsätta sig behandlingen, inte kan godtas.

När det gäller underåriga skall vårdnadshavarna ge sitt informerade samtycke till den personuppgiftsbehandling som skall utföras inom ramen för studien. En bedömning får ske från fall till fall huruvida den underårige har sådan mognad att han eller hon själv också skall informeras om och ge sitt samtycke till behandlingen.

Personuppgiftslagen innehåller inget krav på skriftligt samtycke. Det är dock den personuppgiftsansvarige som vid en eventuell tvist har bevisbördan för att ett giltigt samtycke inhämtats.

Datainspektionens iakttagelser:

I den skriftliga deltagarinformation som användes betonades utan undantag att deltagandet är frivilligt och att den som tackar nej inte riskerar att gå miste om sjukvårdande behandling, något som är ett forskningsetiskt krav. Därmed uppfylldes också personuppgiftslagens krav på frivillighet.

Det var mycket vanligt att deltagarna samtyckte enbart till att delta i studien som sådan.

Det förekom att så kallat tyst samtycke använts i forskningsprojekt.

I ett fall kodades inte uppgifterna trots att detta angavs i patientinformationen. Forskarna hade tillgång till fullständigt namn och personnummer.

Datainspektionens synpunkter:

För att samtycket skall uppfylla personuppgiftslagens krav måste samtycket uttryckligen omfatta själva personuppgiftsbehandlingen. Det är således inte tillräckligt att de registrerade samtycker enbart till att delta i studien som sådan. De registrerade måste dessutom ge sitt godkännande till den personuppgiftsbehandling som skall ske inom ramen för studien.

Ett tyst samtycke kan inte godtas.

Om det anges i patientinformationen att forskarna endast skall ha tillgång till kodade uppgifter måste de ansvariga för studien naturligtvis hålla sig till det. Skall en förändring ske måste nytt informerat samtycke inhämtas.

Under förutsättning att de registrerade personerna har informerats om och givit sitt samtycke till det är det tillåtet att behandla fullständigt namn och personnummer inom ramen för en studie. Däremot kan det finnas andra regler – exempelvis för kliniska läkemedelsprövningar – som säger att deltagarnas identitet inte skall vara känd för forskarna.

4.2.3 Information

Innan de registrerade lämnar sitt uttryckliga samtycke till personuppgiftsbehandlingen skall de ha fått information som omfattar följande uppgifter:

- Vem som är personuppgiftsansvarig (observera att det oftast inte är en fysisk person)⁶,
- ändamålen med behandlingen av personuppgifterna samt
- all övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter i samband med behandlingen, såsom uppgift om mottagarna av personuppgifterna (till vem eller vilka utanför den personuppgiftsansvariges organisation som uppgifterna kan komma att lämnas ut), skyldighet att lämna uppgifter och rätten att ansöka om information (så kallat registerutdrag) och få rättelse av eventuellt felaktiga personuppgifter.⁷

⁶ se avsnitt 3.2.3

⁷ 26 § personuppgiftslagen

Om personuppgifter kommer att överföras till tredje land⁸ skall den enskilde informeras om och ge sitt samtycke till överföringen.

Datainspektionens iakttagelser:

I de inspekterade projekten var den ursprungliga informationen, det vill säga den version av patientinformationen som sändes in tillsammans med anmälan om förhandskontroll, bristfällig såtillvida att en, flera eller samtliga ovanstående uppgifter saknades.

Efter Datainspektionens förhandskontrollbeslut hade många projektansvariga försökt anpassa informationen till patienter efter synpunkterna i beslutet. Trots detta förekom det att informationen ändå inte uppfyllde samtliga krav i personuppgiftslagen.

Det märktes tydligt i vilka fall personuppgiftsombuden hade varit aktiva i arbetet med att ta fram ny patientinformation. I dessa fall uppfyllde informationen till de registrerade i stort sett alltid personuppgiftslagens krav.

I en tredjedel av de granskade forskningsstudierna hade de ansvariga för studien inte försökt ändra informationen överhuvudtaget, se även avsnitt 5.5. Det innebär att deltagarna i dessa forskningsstudier inte fick all den information som de hade rätt till innan de tog ställning till om de skulle delta i studien eller inte.

Datainspektionens synpunkter:

Påbörjas ett projekt utan att de registrerade fått korrekt information och utan att ett giltigt samtycke har inhämtats är den behandling av känsliga personuppgifter som utförs inom ramen för forskningsstudien inte tillåten enligt personuppgiftslagen.

Personuppgiftsombuden har uppenbarligen en viktig roll och det tycks vara en god rutin att involvera ombuden i arbetet med patientinformationen.

Nedan följer en närmare förklaring till de uppgifter som skall finnas i en korrekt patientinformation.

Personuppgiftsansvar

Personuppgiftsansvarig är *den som ensam eller tillsammans med andra bestämmer ändamålen med och medel för studien.*

⁸ se avsnitt 4.2.5

Under avsnitt 3.2.3 ovan finns en mer utförlig redogörelse för vad personuppgiftsansvaret innebär.

Datainspektionens iakttagelser:

I samband med inspektionerna visade det sig i flera fall att det fanns anledning att ifrågasätta vem som egentligen var personuppgiftsansvarig.

I informationen till patienterna saknades många gånger uppgift om vem som var personuppgiftsansvarig. Det var vanligt att endast kontaktpersonernas namn finns med.

Rutinerna för hanteringen av de kliniska data och resultaten av de genetiska analyserna som registrerades för den aktuella forskningsstudien varierade mycket. Ibland antecknades även resultatet av de genetiska analyserna i patientjournalen. I andra fall var det mycket klart uttalat att inga resultat skulle återföras till sjukvården och att de uppgifter som rörde den aktuella studien skulle hållas strikt åtskilda från den vanliga journalen.

Datainspektionens synpunkter:

Det är angeläget för samtliga inblandade att ha klart för sig hur ansvaret fördelas bland annat eftersom den personuppgiftsansvarige har ett skadeståndssanktionerat ansvar för att personuppgifter behandlas i enlighet med personuppgiftslagen. Den enskilde måste naturligtvis få information om vem som ytterst ansvarar för behandlingen av personuppgifterna innan han eller hon tar ställning till ett eventuellt deltagande i forskningsstudien.

En patientjournal ingår i ett vårdregister och för dessa uppgifter är sjukvårdshuvudmannen personuppgiftsansvarig. Ett vårdregister får endast innehålla de uppgifter som enligt lag eller annan författning skall antecknas i en patientjournal. I en patientjournal skall antecknas uppgifter som behövs i och för vården. Om andra uppgifter – än sådana som behövs i och för vården – tillförs journalen, är vårdregisterlagen inte tillämplig på just den behandlingen. Är det huvudsakliga ändamålet med behandlingen forskning gäller istället personuppgiftslagen. En sjukvårdshuvudman som saknar bestämmande inflytande över en behandling som görs i anledning av en forskningsstudie blir inte personuppgiftsansvarig för uppgifterna enbart därför att sjukvårdens datorer används. Vem som äger databasen saknar betydelse för frågan om vem som är personuppgiftsansvarig. Det finns anledning för de personuppgiftsansvariga att i större utsträckning än hittills överväga vilka rutiner som är lämpliga (se även avsnitt 6.2 om personuppgiftsbiträde).

Det är tveksamt om det överhuvudtaget är lämpligt ur integritetssynpunkt att anteckna resultatet av de genetiska analyserna i patientjournalen, särskilt med hänsyn till att försäkringsbolag brukar begära att få ta del av blivande försäk-

ringstagares journaluppgifter. Redan uppgiften om att en person har lämnat sitt samtycke till deltagande i en viss studie kan innebära en risk för att personen diskrimineras på grund av sitt genetiska arv⁹. En strikt uppdelning är kanske att föredra, särskilt med tanke på att det är oklart vilken framtida betydelse uppgifter om genetiska anlag kan få. Frågan har uppmärksammats av regeringen som anser att frågan om dokumentation och journalföring behöver klargöras. En parlamentarisk kommitté har fått i uppdrag bland annat att överväga frågan om vem som skall ha rätt att ta del av resultatet från genetiska undersökningar¹⁰.

För den enskilde är det givetvis av stor vikt att känna till hur uppgifterna hanteras.

Ändamålet med behandlingen

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålen måste bestämmas redan när uppgifterna samlas in. Att ändamålen skall vara särskilda innebär att en alltför allmänt hållen ändamålsbestämning inte kan godtas. Det skall framgå av informationen för vilka ändamål personuppgifterna skall användas.

Datainspektionens iakttagelser:

Som regel framgick ändamålet av patientinformationen (se dock avsnitt 4.2.6 om biobanker).

Mottagare

Mottagare är *den till vilken personuppgifter lämnas ut*. Därmed avses de personer och andra *utanför* den personuppgiftsansvariges organisation som kommer att ha tillgång till personuppgifterna.

Datainspektionens synpunkter:

Den som tackar ja till att delta i ett forskningsprojekt skall ha klart för sig vad som händer med de känsliga personuppgifterna och vilka som får del av dessa. Det kan ha en väsentlig betydelse för den enskilde vilka som har tillgång till uppgifterna. Det är tillräckligt att ange vilka kategorier av mottagare som personuppgifterna lämnas ut till.

⁹ Se Regeringens proposition 2001/02:44 Biobanker inom hälso- och sjukvården m.m. s. 35

¹⁰ dir. 2001:20

Rätt till information/ registerutdrag

Den personuppgiftsansvarige är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller inte.¹¹ Om personuppgifter behandlas skall den sökande få skriftlig information – ett så kallat registerutdrag – där det framgår vilka uppgifter om den sökande som behandlas, varifrån dessa uppgifter har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare uppgifterna lämnats ut. Skyldigheten att lämna registerutdrag omfattar samtliga uppgifter om den registrerade som den personuppgiftsansvarige behandlar. Undantag från informationsplikten gäller dock bland annat i de fall som sekretess och tystnadsplikt gäller gentemot den registrerade.

Genom rätten till registerutdrag får den enskilde möjlighet att kontrollera om han eller hon är registrerad och, om så är fallet, att de registrerade personuppgifterna är riktiga. Rätten till registerutdrag är dessutom en förutsättning för att den enskilde i praktiken skall kunna få felaktiga uppgifter rättade. Det är därför inte tillräckligt att den enskilde, efter begäran om så kallat registerutdrag, bara får generell information om vilken typ av uppgifter som registrerats.

Datainspektionens iakttagelser:

Det framfördes invändningar om att det är svårt för den enskilde att tillgodogöra sig exempelvis resultat av laboratorieanalyser.

Vid kliniska läkemedelsprövningar var rutinen att försökspersonernas identitet inte var känd för den personuppgiftsansvarige. Den personuppgiftsansvarige fick endast tillgång till kodade uppgifter och kodnyckeln förvarades inte hos det ansvariga bolaget. En vanlig rutin var därför att den registrerade istället fick vända sig till sin behandlande läkare som hjälpte till att ordna ett så kallat registerutdrag. Det framkom också att vissa personuppgiftsansvariga lät en biobank administrera registerutdrag. I något fall skulle den enskilde inte få reda på resultatet av den genetiska undersökningen.

Datainspektionens synpunkter:

Den enskilde har rätt till insyn och skall få del av alla uppgifter som den personuppgiftsansvarige behandlar, även sådana som är svåra att förstå.

¹¹ 26 § personuppgiftslagen

Det är den personuppgiftsansvarige som är skyldig att lämna registerutdrag. Denne har dock möjlighet att själv bestämma lämpliga rutiner för att administrera registerutdrag.

Om den enskildes identitet inte skall vara känd för läkemedelsföretagen kan det vara en lämplig rutin att låta patienten vända sig exempelvis till sin behandlande läkare eller till biobanken istället.

Rätten till rättelse

Den personuppgiftsansvarige är skyldig att på begäran av den enskilde snarast rätta felaktiga personuppgifter. Den personuppgiftsansvarige har dock alltid skyldighet att se till att de personuppgifter som behandlas är riktiga och skall också på eget initiativ rätta felaktiga uppgifter.

Datainspektionens iakttagelser:

Det förekom att forskare invände att det är svårt för den enskilde att tolka och ha synpunkter på exempelvis laboratoriesvar eller på resultaten av de genetiska analyserna.

Datainspektionens synpunkter:

Det är i och för sig svårt att ha invändningar mot exempelvis laboratoriesvar och det torde inte heller vara särskilt vanligt att registrerade personer begär rättelse av just den typen av uppgifter. Rätten till rättelse hänger samman med den personuppgiftsansvariges skyldighet att alltid tillse att de personuppgifter som behandlas är riktiga. En uppgift är riktig om den stämmer överens med de verkliga förhållandena. Det kan dock vara svårt att bestämma vilka de verkliga förhållanden är som den registrerade uppgiften skall spegla. Ledning får då sökas i ändamålen med behandlingen. Framställs en begäran om rättelse bör den personuppgiftsansvarige skyndsamt utreda om anmärkningen är befogad. Vid oenighet kan den registrerade vända sig till Datainspektionen.

4.2.4 Särskilt om överföring till tredje land

Tredje land är enligt definitionen i personuppgiftslagen en stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet. Definitionen av tredje land har betydelse för frågan om överföring av personuppgifter till utlandet. Enligt huvudregeln¹² är det förbjudet att överföra personuppgifter som är under behandling till tredje land om inte landet har en adekvat nivå för skyddet av personuppgifterna. Det finns dock flera undantag

¹² 33 § personuppgiftslagen

från bestämmelsen. Det är alltid tillåtet att föra över personuppgifter till tredje land med den registrerades samtycke. EG-kommissionen meddelar beslut om vilka länder som anses ha en adekvat skyddsnivå. Datainspektionen kan meddela undantag från förbudet i enskilda fall under förutsättning att det finns tillräckliga garantier för de registrerades rättigheter.

Förbudet är straffsanktionerat.¹³

Datainspektionens iakttagelser:

Internationellt samarbete var vanligt på forskningsområdet och det förekom ofta att personuppgifter – i vart fall kodade sådana – överfördes till utlandet.

Det förekom att det framgick av anmälan för förhandskontroll att personuppgifter skulle överföras till tredje land men att deltagarinformationen saknade uppgift om detta.

Vissa lämnade ingen information till de registrerade eftersom det bara var kodade uppgifter som lämnades ut.

Många personuppgiftsansvariga hade som rutin att alltid inhämta skriftligt samtycke till att personuppgifter överfördes till tredje land.

Datainspektionens synpunkter:

Den personuppgiftsansvarige som inte tänker inhämta samtycke måste hålla sig väl underrättad om till vilka länder det är tillåtet att föra över personuppgifter. I annat fall skall den enskilde ge sitt samtycke också till att uppgifter överförs till tredje land. Vidare bör det alltid framgå av informationen om uppgifter överförs till andra länder, även i de fall samtycke inte krävs.

Som tidigare påpekats är även kodade uppgifter personuppgifter.

4.2.5 Särskilt om biobanker

Datainspektionens iakttagelser:

I flera av projekten använde sig de personuppgiftsansvariga av material från någon av de biobanker som finns. Det förekom att de ansvariga för studien hänvisade till det ursprungliga samtycke som de registrerade lämnat när de donerade blod eller vävnad. De ansåg därför att de inte behövde inhämta något nytt samtycke.

¹³ 49 § c) personuppgiftslagen

Datainspektionens synpunkter:

Problem uppstår i de fall där personuppgifter och prover från biobanker används och de ansvariga för studien inte har för avsikt att inhämta nya samtycken från provgivarna. Det går som regel inte att stödja sig på det ursprungliga samtycke som lämnades när patienterna donerade sina blodprov. I allmänhet är det ursprungliga ändamålet för generellt utformat för att kunna godtas; exempelvis ”framtida forskning”. Patienterna måste lämna sitt samtycke till den personuppgiftsbehandling som görs inom ramen för en specifik studie och till att personuppgifter om genetiska anlag behandlas. De personer som donerat sitt blod har för övrigt knappast kunnat förutse att deras uppgifter skulle användas för genetisk forskning.

Har inget korrekt samtycke inhämtats måste det finnas annat stöd i personuppgiftslagen för behandlingen; exempelvis att den är tillåten efter en intresseavvägning, se ovan under avsnitt 4.1. Finns inget sådant lagstöd måste antingen nytt samtycke inhämtas eller så måste den personuppgiftsansvarige upphöra med behandlingen.

Det är värt att notera att den nya biobankslag¹⁴ som träder i kraft den 1 januari 2003 endast är tillämplig på hanteringen av vävnadsproverna och inte på den personuppgiftsbehandling som sker i register eller på annat sätt i anslutning till biobankerna. Det innebär att personuppgiftslagen även i fortsättningen kommer att vara tillämplig på denna personuppgiftsbehandling.

4.2.6 Uppgifter om släktingar

I de granskade studierna förekom det att uppgifter om släktingars sjukdomar behandlades. Eftersom samtycket skall vara individuellt skall som huvudregel också släktingarna ge sitt informerade samtycke till behandlingen.

¹⁴ lag 2002:297 om biobanker inom hälso- och sjukvården

5. Förhandskontroll

5.1 Varför förhandskontroll?

Enligt EG-direktivet – som personuppgiftslagen bygger på – skall medlemsstaterna bestämma vilka behandlingar som kan innebära särskilda risker för de registrerades fri- och rättigheter och säkerställa att dessa behandlingar kontrolleras innan de påbörjas.¹⁵ I direktivet anges att vissa typer av personuppgiftsbehandlingar på grund av sin natur, sin omfattning eller sitt ändamål kan innebära särskilda risker för att de registrerades fri- och rättigheter kränks. Medlemsstaterna är därför skyldiga att föreskriva att tillsynsmyndigheterna eller den som utför tillsyn i samråd med tillsynsmyndigheten företar en förhandskontroll av dessa behandlingar innan de utförs.

Det har i Sverige ansetts oförenligt med EG-direktivet att införa en bestämmelse om att inga behandlingar behöver kontrolleras på förhand. Regeringen har därför fått bemyndigande att meddela föreskrifter om att sådana behandlingar som innebär särskilda risker för otillbörligt intrång i den personliga integriteten skall anmälas för förhandskontroll till tillsynsmyndigheten; det vill säga till Datainspektionen.

Anmälningsskyldigheten är straffsanktionerad. Den som genomför en behandling utan att göra anmälan till Datainspektionen kan – förutom i ringa fall – dömas till böter eller fängelse.¹⁶ Det är den fysiska person som gjort sig skyldig till förfarandet som döms till straff oavsett om han eller hon själv är personuppgiftsansvarig.

5.2 Vilka behandlingar skall anmälas för förhandskontroll?

Följande automatiserade behandlingar av personuppgifter skall anmälas till Datainspektionen senast tre veckor innan de påbörjas.¹⁷

1. Behandling av känsliga personuppgifter för forskningsändamål utan samtycke från de registrerade och som inte godkänts av en forskningsetisk kommitté
2. Behandling av personuppgifter om genetiska anlag som framkommit efter genetisk undersökning oavsett om uppgifterna är att anse om

¹⁵ Artikel 20.1 EG-direktivet

¹⁶ 49 § d) personuppgiftslagen (1998:204)

¹⁷ 10 § personuppgiftsförordningen

känsliga eller inte och oavsett om behandlingen sker med samtycke eller inte.

Detta innebär att ett forskningsprojekt där man avser att använda uppgifter om genetiska anlag (en genetisk forskningsstudie) *alltid* skall anmälas till Datainspektionen för förhandskontroll. Om en forskningsstudie innebär att man behandlar endast andra känsliga ¹⁸ personuppgifter än uppgifter om genetiska anlag behöver anmälan för förhandskontroll bara göras om personuppgiftsbehandlingen *inte* sker med informerat samtycke *och* inte heller har godkänts av en forskningsetisk kommitté. Även om det inte krävs att Datainspektionen förhandskontrollerar personuppgiftsbehandlingen måste personuppgiftslagen bestämmelser naturligtvis tillämpas när forskningsstudien utförs. Det är den personuppgiftsansvarige som ansvarar för att reglerna i personuppgiftslagen följs.

Anmälningsskyldigheten gäller dock inte för sådan behandling av personuppgifter som regleras genom särskilda föreskrifter i lag eller förordning.

Det är den personuppgiftsansvarige som skall göra anmälan senast tre veckor innan den planerade behandlingen skall påbörjas.

Datainspektionens iakttagelser:

Det framkom vid inspektionerna att det fanns studier som redan hade påbörjats när anmälan för förhandskontroll lämnades in till Datainspektionen. När beslutet fattades hade forskningsstudierna redan avslutats. Vidare fanns det personuppgiftsansvariga som hade genomfört flera forskningsstudier utan att förhandsanmäla dessa till Datainspektionen.

Datainspektionens synpunkter:

Syftet med bestämmelsen om förhandskontroll är att behandlingarna skall granskas innan de påbörjas. Om behandlingen anmäls när forskningsstudien redan påbörjats eller till och med avslutats fyller förhandskontrollen ingen funktion. Det finns anledning att anta att det finns ett mörkertal av genstudier som genomförs utan att anmälas till Datainspektionen.

5.3 Vad skall anmälan innehålla?

Anmälan görs på särskild blankett som tillhandahålls av Datainspektionen. Till anmälan bifogas i förekommande fall kopior av skriftlig information och

¹⁸ för definition av begreppet ”känsliga personuppgifter” se avsnitt 3.2.4

samtyckesformulär till de registrerade samt slutligt beslut i den forskningsetiska kommittén.

5.4 Handläggningen vid Datainspektionen

När en anmälan kommer in till Datainspektionen meddelar inspektionen – under förutsättning att anmälan är komplett – beslut inom tre veckor. Behöver anmälan kompletteras förlängs handläggningstiden. Om patientinformationen och samtycket uppfyller kraven i personuppgiftslagen kan Datainspektionen fatta beslut i ärendet direkt utan att avvakta beslutet från den forskningsetiska kommittén. I annat fall har Datainspektionen som rutin att begära in kopia av slutligt beslut i den forskningsetiska kommittén. Skälet är att om inget giltigt samtycke kommer att inhämtas kan det istället bli aktuellt att tillämpa avvägningsnormen. Om det framgår av den forskningsetiska kommitténs beslut att kommittén har godkänt personuppgiftsbehandlingen är behandlingen utan vidare tillåten¹⁹.

Datainspektionens iakttagelser:

Vid inspektionerna framfördes önskemål om att påskynda handläggningen hos Datainspektionen eftersom tidsutdräkten förorsakar stora kostnader. Vidare uppgav man att det förekommer att den etiska kommittén ibland kräver att få kopia av Datainspektionens beslut innan den fattar sitt beslut samtidigt som Datainspektionen begär kopia av beslutet i den etiska kommittén.

Datainspektionens synpunkter:

De personuppgiftsansvariga har möjlighet att själva påskynda handläggningen genom att redan i samband med den ursprungliga etikansökan ha en deltagarinformation och ett samtycke som uppfyller personuppgiftslagens krav.²⁰

Datainspektionen hade tidigare som rutin att alltid begära in kopia av beslutet i den etiska kommittén oavsett om den aktuella informationen och samtycket uppfyllde kraven i personuppgiftslagen eller inte. Uppfyller patientinformationen och samtycket personuppgiftslagens krav fattar Datainspektionen numera beslut utan att avvakta etikkommitténs beslut.

¹⁹ se avsnitt 4.1

²⁰ se avsnitt 4.2.2 ff

5.5 Vad innebär Datainspektionens beslut?

Datainspektionens beslut innebär att inspektionen gör en bedömning av om den planerade personuppgiftsbehandlingen är förenlig med personuppgiftslagen eller inte. Om Datainspektionen konstaterar att behandlingen inte uppfyller kraven i personuppgiftslagen lämnar inspektionen synpunkter på vad som krävs för att behandlingen skall vara laglig. Behandlingen är således laglig *först när den personuppgiftsansvarige har rättat sig efter synpunkterna i beslutet*. Ansvar för att åtgärda eventuella brister och anpassa behandlingen till lagens krav ligger hos den personuppgiftsansvarige. Datainspektionen har befogenhet att ingripa, ytterst genom att vid vite förbjuda en viss olaglig behandling. Någon generell uppföljning av meddelade beslut sker inte, utan eventuella brister kan konstateras först vid en tillsyn mot den personuppgiftsansvarige. Beslutet innebär således inte att behandlingen automatiskt är godkänd.

Datainspektionens iakttagelser:

En synpunkt som framfördes är att det inte är nödvändigt att beakta Datainspektionens beslut. Det är främst forskningsetikkommitténs beslut och – vid kliniska prövningar – Läkemedelsverkets godkännande som anses ha relevans.

Det förekom att forskare hade uppfattat Datainspektionens beslut som ett tillstånd och valt att inte följa de anvisningar som inspektionen hade lämnat. Eftersom studien var ”godkänd” ansåg man sig inte behöva vidta några ytterligare åtgärder. Det förekom också att man inte hade förstått beslutet i andra avseenden. I många fall hade dock de personuppgiftsansvariga gjort stora ansträngningar för att följa Datainspektionens beslut och hade kompletterat informationen på olika sätt. Besluten missförstods således inte generellt.

Datainspektionens synpunkter:

Varje personuppgiftsansvarig som behandlar personuppgifter är skyldig att följa personuppgiftslagens bestämmelser. Iakttas inte personuppgiftslagens krav är behandlingen olaglig.

Besluten har under 2002 fått en förändrad utformning. Syftet med förändringen är att besluten skall bli tydligare. Redan innan förändringen kunde många personuppgiftsansvariga tillgodogöra sig besluten och anpassade informationen till personuppgiftslagens bestämmelser. Någon skillnad mellan nya och gamla beslut har inte märkts vid inspektionerna.

5.6 Säkerhetsföreskrifter

Datainspektionen får meddela beslut om säkerhetsföreskrifter i enskilda fall²¹ för att skydda de personuppgifter som behandlas. Så sker idag regelmässigt i de ärenden som anmälts för förhandskontroll. Genom beslutet får den personuppgiftsansvarige preciserat vilka åtgärder han eller hon måste vidta för att uppfylla säkerhetskraven. Datainspektionen har möjlighet att förena beslutet med vite. Beslutet om säkerhetsföreskrifter går att överklaga hos allmän förvaltningsdomstol. För närvarande meddelar Datainspektionen beslut om säkerhetsföreskrifter i samtliga ärenden som anmälts för förhandskontroll; alla personuppgiftsansvariga får likartade föreskrifter. De uppgifter som lämnas i anmälan är som regel för knapphändiga för att det skall vara möjligt att göra en individuell bedömning. På sikt kan det bli aktuellt med en förändring mot en mer individuell prövning. Beslut om säkerhetsföreskrifter kommer i så fall att meddelas i endast de fall där det bedöms att behov finns, vilket är en anpassning till personuppgiftslagen.

²¹ 32 § personuppgiftslagen

6. IT-säkerhet

6.1 Allmänt

Den personuppgiftsansvarige har enligt personuppgiftslagen ansvaret för att vidta de tekniska och organisatoriska åtgärder som krävs för att skydda personuppgifterna. Åtgärderna skall åstadkomma en lämplig säkerhetsnivå med beaktande bland annat av hur pass känsliga personuppgifter som behandlas.

Datainspektionens iakttagelser:

Syftet med inspektionerna var bland annat att kontrollera om de personuppgiftsansvarige följde de meddelade säkerhetsföreskrifterna. Vilka dessa är framgår av bilaga 2.

När det gäller läkemedelsföretagen konstaterades att dessa överlag hade ett väl utvecklat säkerhetstänkande och hög säkerhet. Det fanns goda rutiner för hur information om IT-säkerhet spreds i organisationen.

När det gäller de projekt som bedrevs vid universitet och sjukhus var det svårare att bedöma säkerheten eftersom många studier ännu inte hade påbörjats. De enskilda forskarna fick istället beskriva hur de hade planerat IT-säkerheten. Ofta hade forskarna inte fått någon IT-säkerhetsinformation på initiativ av den personuppgiftsansvarige. Det var den enskilde forskaren som valde vilken nivå han eller hon ville ha på säkerheten. Många gånger var det bara en person som skulle komma att ha tillgång till uppgifterna och det fanns inget behov av att exempelvis följa upp loggar. Det var stora variationer mellan sjukhusen. I de fall det fanns en egen säkerhetsansvarig vid institutionen/avdelningen brukade som regel den personen ha kontroll på hur uppgifter hanterades.

Datainspektionens synpunkter:

Det är den personuppgiftsansvarige som har ansvaret för att sprida information om IT-säkerhet i organisationen och för att ge tydliga instruktioner. I flera fall var det inte tydligt för de inblandade vem som var personuppgiftsansvarig vilket medförde att information och närmare instruktioner om IT-säkerheten inte gavs till de berörda forskarna.

6.2 Personuppgiftsbiträde

Personuppgiftsbiträde är *den som behandlar personuppgifter för den personuppgiftsansvariges räkning.*

Om en personuppgiftsansvarig anlitar en självständig företagare, en juridisk person eller en myndighet för att utföra en behandling av personuppgifter

kommer den anlitade antingen att betraktas som personuppgiftsbiträde eller personuppgiftsansvarig (tillsammans med den som lämnade uppdraget). Huruvida den anlitade blir att betrakta som personuppgiftsbiträde eller personuppgiftsansvarig hänger samman med om han eller hon har befogenhet att självständigt eller tillsammans med den som lämnade uppdraget bestämma över för vilka ändamål och hur personuppgifter skall behandlas. Även uppdragstagare kan ha en så pass självständig ställning att de blir att betrakta som personuppgiftsansvariga.

När ett personuppgiftsbiträde anlitas skall den personuppgiftsansvarige försäkra sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas för att skydda de personuppgifter som behandlas och se till att biträdet verkligen vidtar åtgärderna. Det skall dessutom alltid finnas ett skriftligt avtal som reglerar personuppgiftsbitrådets behandling av personuppgifter för den ansvariges räkning. I avtalet skall det finnas en särskild föreskrift om bitrådets skyldighet att vidta säkerhetsåtgärder.

Vid elektronisk överföring av personuppgifter till personuppgiftsbiträden skall uppgifterna vara krypterade. Det räcker inte att koda uppgifterna.

När ett personuppgiftsbiträde behandlar personuppgifter för helt andra ändamål än de den personuppgiftsansvarige bestämt, har den personuppgiftsansvarige ansvaret för att så har kunnat ske, t.ex. för brister i säkerheten eller givna instruktioner.

Datainspektionens iakttagelser:

Det var vanligt att kliniskt verksamma forskare rekryterade patienter och utförde studier på den egna kliniken men att ett universitet eller forskningsinstitut i själva verket var personuppgiftsansvarig. Ibland användes sjukhusets datorer och nätverk för att bearbeta forskningsdata och ibland var forskaren uppkopplad mot universitetets server.

Inte i något av de fall där projekten genomfördes på klinik men personuppgiftsansvaret låg hos universitet eller institut fanns det – såvitt framkom – något avtal med sjukhuset/landstinget om säkerheten.

Överföringen av personuppgifter skedde oftast inte elektroniskt utan på papper eller manuellt.

Vid kliniska provningar anlidades som regel kliniskt verksamma läkare som var behjälpliga med att samla in patientdata. Det förekom också att läkemedelsföretag lät utomstående företag behandla personuppgifter för deras räkning utan att ha avtal som reglerade säkerheten.

Datainspektionens synpunkter:

I de fall personuppgifter behandlas utanför den ansvariges direkta kontroll på sätt som ofta sker skall det finnas ett skriftligt avtal²² som reglerar ansvaret för säkerheten. Det är otillfredsställande att så många behandlingar av känsliga personuppgifter utförs utan att ansvaret är klarlagt.

²² 30 § personuppgiftslagen

7. Övrigt

7.1 Skydd för företagshemlig information?

En handling som ges in i ett ärende hos en myndighet blir en allmän handling så snart den anses ha kommit in till myndigheten. Följden blir att om den skriftliga patientinformationen bifogas anmälan för förhandskontroll blir informationen en allmän handling så snart den kommer in till Datainspektionen. Enligt huvudprincipen är allmänna handlingar offentliga. Det finns dock en rad undantag från den bestämmelsen. För Datainspektionens del finns en särskild bestämmelse om skydd för enskilds personliga eller ekonomiska förhållanden. Enligt 9 kap 6 § sekretesslagen gäller sekretess hos Datainspektionen i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ankommer på inspektionen för uppgift om enskilds personliga eller ekonomiska förhållanden om det kan antas att den enskilde eller någon honom närstående lider men om uppgiften röjs. Den bestämmelsen täcker även företagshemlig information. En förutsättning för att sekretess skall gälla är att bolaget kan antas lida men om uppgiften röjs. När en person begär att få del av en allmän handling sker alltid en sekretessprövning. Inga handlingar lämnas således ut utan att Datainspektionen först gör en sekretessprövning.

Datainspektionens iakttagelser:

I samband med inspektionerna hos de privata företagen framkom att den patientinformation som gavs in tillsammans med anmälan för förhandskontroll ofta innehöll företagshemlig information. Informationen innehöll som regel detaljerade uppgifter om kommande projekt och det uppgavs vara angeläget att dessa uppgifter inte kommer i orätta händer.

Datainspektionens synpunkter:

Datainspektionen skall ta hänsyn till att deltagarinformationen kan innehålla företagshemligheter vid sin prövning av om en handling skall lämnas ut eller inte. Varje ärende prövas individuellt. För tydlighetens skull kan de personuppgiftsansvariga upplysa om att det, enligt deras uppfattning, är fråga om företagshemlig information redan i samband med att anmälan ges in.

Bilaga 1

Tillsynsobjekt

Akademiska sjukhuset, Uppsala

AstraZeneca AB

Eli Lilly AB

Göteborgs universitet

Karolinska Institutet vid Huddinge universitetssjukhus

Novartis Sverige AB

Pfizer AB

Quintiles AB

Region Skåne, Universitetssjukhuset MAS

Region Skåne, Universitetssjukhuset Lund

Sequenom AB

Uman Genomics AB

Umeå universitet

Utförrarstyrelsen för Sahlgrenska universitetssjukhuset, Sahlgrenska universitetssjukhuset

Bilaga 2

Följande säkerhetsföreskrifter meddelas idag regelmässigt för de behandlingar som anmälts för förhandskontroll.

- Åtkomstskydd:

När datorutrustning och löstagbara datamedier inte står under uppsikt skall utrustningen och medierna låsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall skall personuppgifterna krypteras.

I bärbara datorer skall personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.

- Säkerhetskopia:

Personuppgifterna skall regelbundet överföras till säkerhetskopior. Kopiorna skall förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas efter en störning.

- Behörighetskontroll:

Ett tekniskt system för behörighetskontroll skall styra åtkomsten till personuppgifterna om datorn används av mer än en person. Behörigheten skall begränsas till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord skall vara personliga och får inte överlätas på någon annan. Det skall finnas rutiner för tilldelning av behörigheter.

- Loggning:

Åtkomst till personuppgifter skall kunna följas upp i efterhand genom en maskinell logg eller liknande maskinellt underlag om datorn används av mer än en person. Av detta underlag skall framgå vem som har haft åtkomst, tidpunkten för åtkomsten samt till vilken persons uppgifter åtkomsten har skett. Underlaget skall kontrolleras i tillräcklig utsträckning.

- Datakommunikation:

Anslutning för extern datakommunikation skall skyddas med motringning eller annan teknisk funktion som säkerställer att uppkopplingen är behörig.

Personuppgifter som överförs via datakommunikation utanför lokaler som kontrolleras av den personuppgiftsansvarige skall skyddas med kryptering.

- Utplåning:

När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre skall användas för sitt ändamål skall lagringsmedierna förstöras. Alternativt skall personuppgifterna raderas på sådant sätt att de inte kan återskapas.

- Reparation och service:

När reparation och service av datorutrustning utförs av annan än den personuppgiftsansvariges skall avtal om säkerheten träffas med serviceföretaget.

Vid servicebesöket skall lagringsmedier som innehåller personuppgifter avlägsnas. Är detta inte möjligt skall servicen ske under den personuppgiftsansvariges överinseende.



Datainspektionen

Besöksadress: Fleminggatan 14, plan 9
Postadress: Box 8114, 104 20 Stockholm
Beställningar: 08-657 61 42 (telefonsvarare)
Webbplats: datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Fax: 08-652 86 52
Tel: 08-657 61 00

Pris: 50 kr + moms