



Behandling av känsliga personuppgifter i forskningen

DATAINSPEKTIONENS RAPPORT 2003:1

Innehållsförteckning

1. Inledning	2
2. Sammanfattning	3
3. Personuppgiftslagen	4
3.1 Allmänt	4
3.2 Definitioner	5
3.2.1 <i>Behandling</i>	5
3.2.2 <i>Personuppgift</i>	5
3.2.3 <i>Känsliga personuppgifter</i>	7
3.2.4 <i>Personuppgiftsansvar</i>	7
3.2.5 <i>Personuppgiftsombud</i>	9
3.3 Några grundläggande krav	9
3.3.1 <i>Särskilt om ändamål</i>	10
3.3.2 <i>Bevara inte personuppgifter längre än nödvändigt</i>	10
4. När är det tillåtet att behandla känsliga personuppgifter för forskningsändamål?	12
4.1 Med informerat samtycke	12
4.1.1 <i>Forskningsetisk prövning av informerat samtycke</i>	12
4.1.2 <i>Samtycke enligt personuppgiftslagen</i>	13
4.1.3 <i>Information</i>	15
4.1.4 <i>Närmare om den information som skall lämnas före samtycke</i>	16
4.1.5 <i>Särskilt om överföring till tredje land</i>	20
4.1.6 <i>Särskilt om biobanker</i>	21
4.1.7 <i>Uppgifter om släktingar</i>	22
4.1.8 <i>Personuppgifter om genetiska anlag</i>	23
4.2 Efter en intresseavvägning	24
5. IT-säkerhet	26
Bilagor	

1. Inledning

År 2001 genomförde Datainspektionen ett tillsynsprojekt där behandlingar av känsliga personuppgifter för forskningsändamål var föremål för granskning. Syftet med projektet var att granska om de legala förutsättningarna för att behandla känsliga personuppgifter var uppfyllda, om informationen till de registrerade uppfyllde personuppgiftslagens krav på information och om IT-säkerheten var tillfyllest.

Projektet inleddes i mars 2001 och under våren 2001 genomfördes fältinspektioner vid tre sjukhus i Stockholmsområdet; Karolinska sjukhuset, Södersjukhuset och Huddinge sjukhus. Personuppgiftsansvarig var i dessa fall Karolinska institutet.

Under oktober och november 2001 genomfördes enkätinspektioner som riktades till samtliga universitet och universitetssjukhus som antingen hade anmält personuppgiftsombud till Datainspektionen eller hade anmält personuppgiftsbehandlingar för forskningsändamål till inspektionen. Totalt ingick närmare 100 forskningsstudier i granskningen. De forskningsstudier som valdes ut var sådana där känsliga personuppgifter – exempelvis uppgift om hälsa, sexuell läggning eller politiska åsikter – behandlades. Urvalet gjordes med målsättningen att flertalet institutioner vid varje universitet/universitetssjukhus skulle ingå i granskningen. Vilka personuppgiftsansvariga som ingått framgår av bilaga 1. Den enkät som användes finns i bilaga 2.

2. Sammanfattning

I samband med inspektionerna framkom att det var vanligt med missuppfattningar om vad som är personuppgifter överhuvudtaget. Främst rådde tveksamhet om när uppgifterna kan betraktas som avidentifierade. Många forskningsstudier hade påbörjats innan personuppgiftslagen trädde i kraft och det var vanligt att de ansvariga för studierna hänvisade till gamla datalagstillstånd trots att dessa hade upphört att gälla. Informationen till de registrerade uppfyllde sällan personuppgiftslagens krav trots forskningsetisk prövning. Ett viktigt skäl var antagligen att personuppgifterna i många fall samlats in innan personuppgiftslagen trädde i kraft. Vidare framkom det att det inte var ovanligt att känsliga personuppgifter behandlades, trots att de inte längre behövdes eftersom projekten hade avslutats för länge sedan. Kunskapen om personuppgiftslagen tycktes överlag vara dåligt spridd i organisationerna.

När det gäller IT-säkerheten var det mycket vanligt att rutiner för uppföljning och kontroll av loggar saknades, något som skall finnas när flera personer har tillgång till känsliga personuppgifter. Det förekom också att enskilda forskare inte kände till om det fanns någon generell IT-säkerhetspolicy.

Rapporten har utformats med hänsyn till att kunskapen om personuppgiftslagen inte tycks vara särskild utbredd. Även om personuppgifterna i flera fall samlats in under den tid datalagen gällde skall personuppgiftslagen tillämpas i idag. Rapporten innehåller – förutom en genomgång av vissa grunder i personuppgiftslagen – en redogörelse för under vilka förutsättningar det är tillåtet att behandla känsliga personuppgifter för forskningsändamål, särskilt med avseende på de krav personuppgiftslagen ställer på informationen till de registrerade.

Datainspektionens synpunkter redovisas i särskilda texttrutor.

Stockholm i april 2003

3. Personuppgiftslagen

3.1 Allmänt

Personuppgiftslagen 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. Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagen grundar sig på ett EG-direktiv¹. En viktig förändring är att det tidigare tillstånds- och licensförfarandet togs bort när personuppgiftslagen infördes. Datainspektionen meddelar inte längre tillstånd att föra personregister. Det är istället de personuppgiftsansvariga – de som ytterst ansvarar för hur personuppgifterna hanteras² – som själva har ansvar för att tolka och följa reglerna i personuppgiftslagen. Viktigt att notera är att samtliga datalagstillstånd som meddelats för att föra personregister *upphörde att gälla den 1 oktober 2001*. Det innebär att den som tidigare har haft tillstånd för ett visst personregister och som fortsätter att föra registret är skyldig att anpassa behandlingen till bestämmelserna i personuppgiftslagen.

I personuppgiftslagen har tonvikt lagts vid den enskildes samtycke och rätt till insyn. De personuppgiftsansvariga har ålagts en omfattande informationskyldighet gentemot de registrerade. Personuppgiftslagen ställer alltså högre krav på den information som skall lämnas till de registrerade.

Datainspektionens iakttagelser:

I många av de granskade forskningsstudierna angav de ansvariga för studien att behandlingen av personuppgifter gjordes i enlighet med tillstånd som hade meddelats enligt datalagen.

Datainspektionens synpunkter:

Inspektionerna genomfördes strax efter det att personuppgiftslagen hade trätt i kraft fullt ut och samtliga licenser/tillstånd enligt datalagen hade upphört att gälla. Uppenbarligen hade information om förändringarna inte nått ut i

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.

² För utförlig definition av begreppet, se avsnitt 3.2.4

organisationerna. Det är den personuppgiftsansvarige som är skyldig att se till att kunskap om personuppgiftslagen sprids i organisationen.

3.2 Definitioner

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.

Datainspektionens iakttagelser:

Det framgick av enkätsvaren att många inte kände till vad begreppet behandling av personuppgifter innebär.

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 omfattas inte av personuppgiftslagen.

All information som direkt eller indirekt kan hänföras till en fysisk person är en personuppgift. 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. Så länge kodnyckeln finns kvar är uppgifterna inte avidentifierade i personuppgiftslagens mening.

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 skall i dessa fall betraktas som personuppgifter.

Datainspektionens iakttagelser:

En vanlig missuppfattning var att kodade uppgifter inte var personuppgifter.

I flera forskningsstudier användes enligt uppgift helt anonyma uppgifter; det vill säga ingen koppling till enskilda individer fanns kvar.

Det var vanligt att det stod i den skriftliga information som lämnades till deltagarna i forskningsstudien att endast avidentifierade uppgifter skulle användas trots att det fanns kodnycklar bevarade.

I en enkät uppgavs att ”personuppgifterna förvaras inlåsta i skrivbordslåda” Om det fanns en koppling – exempelvis med kod – mellan dessa uppgifter och uppgifter som registrerats i datorformat framgick inte.

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 personuppgiftslagens mening. Det finns därmed också ett behov av att skydda uppgifterna.

Materialet är inte avidentifierat så länge det finns en kodnyckel kvar. Att kodnyckeln förvaras separat saknar betydelse för frågan om det är personuppgifter eller inte. Det spelar inte heller någon roll om kodlistan bevaras i pappersform eller på datamedium.

Har uppgifterna lämnats helt anonymt och det inte går att identifiera någon enskild person är det inte fråga om personuppgifter. Personuppgiftslagen är därmed inte tillämplig på den aktuella behandlingen. Det förutsätter givetvis att de uppgifter som lämnas inte är så unika att de ändå går att härleda till enskilda personer.

Det finns anledning att betona att personuppgiftslagen inte innehåller något absolut förbud mot att behandla personuppgifter. Frågan om uppgifterna är avidentifierade eller inte har betydelse för frågan om personuppgiftslagen blir tillämplig på behandlingen eller inte. Under förutsättning att personuppgiftslagens bestämmelser iakttas är det tillåtet att behandla personuppgifter för forskningsändamål. I de allra flesta forskningsstudier *måste* det finnas en möjlighet att härleda resultaten till enskilda personer.

3.2.3 Känsliga personuppgifter

Känsliga personuppgifter enligt personuppgiftslagen 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 uttryckliga samtycke, varom mer i avsnitt 4.1. Utan samtycke är det tillåtet att behandla känsliga personuppgifter 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, se avsnitt 4.2.

Datainspektionens iakttagelser:

I samtliga granskade forskningsstudier behandlades känsliga personuppgifter; främst sådana som rörde hälsa. Det förekom också att uppgifter om politiska åsikter och om sexualliv behandlades.

Det förekom att en del av de forskare som behandlade uppgifter om vissa sjukdomar ansåg att dessa inte var känsliga personuppgifter.

Datainspektionens synpunkter:

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

3.2.4 Personuppgiftsansvar

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

³ 13 § personuppgiftslagen

⁴ 49 § b) personuppgiftslagen

Så snart personuppgifter behandlas finns det en eller flera som är ansvariga för 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 behandlingen. Vanligtvis är det den juridiska person som behandlar personuppgifter i sin verksamhet, som bestämmer vilka uppgifter som skall behandlas och vad de skall användas till. När det gäller forskningsstudier som utförs på sjukhus är det dock ofta inte landstinget som är personuppgiftsansvarigt utan istället ett universitet eller ett forskningsinstitut.

Det är den personuppgiftsansvarige som har ansvaret för att all behandling av personuppgifter utförs i enlighet med bestämmelserna i personuppgiftslagen och därtill anknytande reglering. Den personuppgiftsansvarige ansvarar också 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 orsakat⁵.

Datainspektionens iakttagelser:

I enkäterna uppgavs vanligtvis att en enskild forskare – exempelvis kontaktpersonen för studien – var personuppgiftsansvarig. I de fall enkäten hade passerat personuppgiftsombudet innan den skickades in till Datainspektionen förekom att ombudet korrigerat uppgiften. Det var också vanligt att den egna kliniken uppgavs vara personuppgiftsansvarig trots att det i själva verket var exempelvis ett universitet.

Datainspektionens synpunkter:

Det är viktigt att ha klart för sig vem som är personuppgiftsansvarig för en aktuell studie eftersom det har betydelse bland annat för vem som har det skadeståndsrättsliga ansvaret för att de känsliga personuppgifterna behandlas i enlighet med personuppgiftslagen. Ansvaret för att sprida information om personuppgiftslagen ligger hos den personuppgiftsansvarige. Har den personuppgiftsansvarige utsett ett personuppgiftsombud kan ombudet informera om personuppgiftslagen och hjälpa till med klargöranden.

⁵ 48 § personuppgiftslagen

3.2.5 Personuppgiftsombud

Personuppgiftsombud är den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Den personuppgiftsansvarige har möjlighet att förordna ett personuppgiftsombud. Det finns ingen skyldighet att förordna ett personuppgiftsombud, det är frivilligt. Personuppgiftsombudet har till uppgift dels att se till att den personuppgiftsansvarige behandlar personuppgifter på ett korrekt sätt och i enlighet med god sed, dels att påpeka eventuella brister. Ombudet skall föra en förteckning över de behandlingar som den personuppgiftsansvarige genomför. En viktig uppgift för personuppgiftsombudet är att ge råd om och sprida information om personuppgiftslagens bestämmelser.

Datainspektionens iakttagelser:

I stort sett samtliga personuppgiftsansvariga som ingick i tillsynsprojektet hade förordnat personuppgiftsombud. Många av de forskare som fyllde i enkäterna uppgav att de själva eller någon annan huvudansvarig för studien var personuppgiftsombud trots att enkäterna förmedlats genom respektive ombud. I flera fall hade personuppgiftsombuden nyligen utsetts och hade förmodligen inte hunnit bli kända i organisationen.

Datainspektionens synpunkter:

Personuppgiftsombuden har till uppgift bland annat att sprida information om personuppgiftslagen. Ansvar för att så sker ligger dock alltid på den personuppgiftsansvarige, oavsett om ombud förordnats eller inte.

3.3 Några grundläggande krav

I personuppgiftslagen uppställs ett antal grundläggande krav som gäller för all behandling av personuppgifter. Personuppgifter får exempelvis bara behandlas om det är lagligt och skall alltid behandlas på ett korrekt sätt. Fler personuppgifter skall inte behandlas än som är nödvändigt med hänsyn till ändamålen. Vidare får personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifter får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Personuppgifter får inte bevaras under längre tid än nödvändigt.

3.3.1 Särskilt om ändamål

Personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålen skall bestämmas redan när uppgifterna samlas in. Att ändamålen skall vara *särskilda* innebär att de inte får vara alltför allmänt hållna. Det är inte heller tillåtet att behandla personuppgifter för ändamål som är oförenliga med de ursprungliga. När det gäller forskning görs det dock undantag från detta krav eftersom behandling för forskningsändamål inte skall anses vara oförenlig med det ursprungliga ändamålet.

Datainspektionens iakttagelser:

I flera fall användes personuppgifter som ursprungligen samlats in för andra ändamål i forskningsstudierna.

Datainspektionens synpunkter:

I de fall forskningsstudierna och personuppgiftsbehandlingen inom ramen för dessa skall göras med stöd av informerats samtycke är det viktigt att veta vilka ändamål den enskilde har fått information om och lämnat sitt samtycke till. Skall personuppgifterna behandlas för nya ändamål måste den enskilde som regel informeras på nytt.

3.3.2 Bevara inte personuppgifter längre än nödvändigt

Personuppgifter får inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Därefter skall uppgifterna av-identifieras eller utplånas. När det gäller behandling av personuppgifter för forskningsändamål finns ofta krav på att uppgifterna skall sparas längre tid än forskningsstudien pågår, ibland upp till 15 år. Så snart uppgifterna inte längre behövs skall dock behandlingen upphöra. Fortsätter den personuppgiftsansvarige att behandla personuppgifter efter att de inte längre behövs är behandlingen inte tillåten enligt personuppgiftslagen.

Observera att arkivlagen⁶ innehåller bestämmelser om att vissa handlingar inte skall gallras. Riksarkivet har med stöd av arkivlagen utfärdat föreskrifter och allmänna råd om gallring av handlingar i statliga myndigheters forskningsverksamhet (RA-FS 1999:1).

⁶ Arkivlag 1990:782

Datainspektionens iakttagelser:

I flera av de inspekterade projekten hade känsliga personuppgifter sparats trots att de inte längre behövdes. De ansvariga för studien uppgav att de nu hade för avsikt att gallra uppgifterna.

Det förekom också att de forskare som besvarade enkäterna skrev att uppgifterna skulle sparas tills vidare. I vissa fall var det fråga om longitudinella undersökningar.

Ett vanligt svar var att det ännu inte var bestämt hur länge uppgifterna fick sparas.

Det fanns också någon ansvarig som uppgav sig inte känna till vilka regler som fanns för hur länge uppgifter kunde bevaras.

Datainspektionens synpunkter:

När det gäller personuppgifter som används för forskningsändamål kan dessa behöva sparas under mycket lång tid. Så snart uppgifterna inte behövs, och det inte heller finns stöd i annan lagstiftning för att bevara uppgifterna, måste de dock gallras.

Det skall finnas rutiner för när uppgifter gallras. Den personuppgiftsansvarige har ett ansvar för att fungerande rutiner finns och för att känsliga personuppgifter inte sparas i onödan.

4. När är det tillåtet att behandla känsliga personuppgifter för forskningsändamål?

4.1 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.

4.1.1 *Forskningsetisk prövning av informerat samtycke*

Det finns inga formella krav på att de forskningsetiska kommittéerna skall granska den deltagarinformation och det samtycke som används i en forskningsstudie med utgångspunkt från personuppgiftslagen. De riktlinjer som finns för den forskningsetiska prövningen⁷ innehåller visserligen krav på vad ett informerat samtycke skall innefatta. För närvarande finns dock, såvitt känt, inga rekommendationer om att också beakta personuppgiftslagens särskilda krav vid den forskningsetiska granskningen. Även om etikkommittén har godkänt informationen innebär det därför inte att den med automatik också uppfyller kraven i personuppgiftslagen.

Den föreslagna lagen om etikprövning av forskning som avser människor⁸ kommer, om den träder i kraft, att innehålla bestämmelser om vilka grundkrav som ställs på ett informerat samtycke.

Datainspektionens iakttagelser:

De som besvarade enkäterna hade inte uppmanats att skicka med kopia av besluten i den forskningsetiska kommittén. Några hade ändå gjort det.

Det fanns exempel på beslut där den etiska kommittén hade skrivit att studien granskats och godkänts enligt personuppgiftslagen.

Huvuddelen av de studier som ingick i granskningen genomfördes med informerat samtycke – enligt uppgift godkänt av etikkommitté – från de registrerade. Trots att informationen granskats av etisk kommitté uppfyllde den sällan samtliga personuppgiftslagens krav. Därför följer en närmare redogörelse för vilka krav personuppgiftslagen ställer på ett informerat samtycke.

⁷ Se exempelvis *Riktlinjer för etisk värdering av medicinsk humanforskning i Sverige, Forskningsetisk policy och organisation i Sverige*, MFR – Rapport 2 2000

⁸ Prop. 2002/03:50

4.1.2 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 fler 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.

För att det skall vara tillåtet att behandla känsliga personuppgifter måste samtycket dessutom vara

- uttryckligt.

När det gäller underåriga skall vårdnadshavarna ge sitt informerade samtycke till den personuppgiftsbehandling som skall utföras inom ramen för forskningsstudien. Man får bedöma 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 att samtycket skall vara skriftligt. Det är dock vid en eventuell tvist den personuppgiftsansvarige som har bevisbördan för att samtycke inhämtats.

Datainspektionens iakttagelser:

Den skriftliga deltagarinformation som användes i de granskade forskningsstudierna innehöll utan undantag uppgift om att deltagandet var frivilligt och i förekommande fall att den som tackade nej inte riskerade att gå miste om sjukvårdande behandling.

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

I en forskningsstudie informerades deltagarna om att deras intervjuvar skulle bearbetas i dator. Däremot lämnades ingen information om att känsliga personuppgifter också skulle hämtas från sjukvårdens register.

I flera enkätsvar uppgavs att deltagarna i forskningsstudierna lämnat sitt samtycke genom att frivilligt fylla i och sända in de enkäter som de fått sig till-sända.

I ett fall uppgavs att patienterna givit sitt muntliga samtycke till att besvara frågeformulär som använts vid psykologisk behandling. Svaren användes sedan i en forskningsstudie. Studien hade godkänts av forskningsetisk kommitté.

Det förekom att endast muntligt samtycke inhämtades; framförallt i de forskningsstudier där det var fråga om intervjuundersökningar.

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 utföras inom ramen för studien. De skall informeras om behandlingen och lämna sitt samtycke därtill.

Genomförs fler behandlingar än de registrerade känner till – exempelvis att också journaluppgifter inhämtas – föreligger inget giltigt samtycke.

Att samtycka genom att frivilligt lämna uppgifter – exempelvis genom att besvara en enkät – kan vara godtagbart endast under förutsättning att de registrerade fått tydlig *information om att uppgiftslämnandet innebär att de också godkänner personuppgiftsbehandlingen*. Om deltagarna inte fått sådan information uppfyller samtycket inte kraven på att vara uttryckligt.

Har patienter frivilligt besvarat frågor som ingår i psykologiska tester i behandlingssyfte innebär det inte att de kan anses ha godkänt att de känsliga personuppgifterna också används för forskningsändamål. Om samtycke skall åberopas som grund för en sådan personuppgiftsbehandling måste de registrerade ha fått information om att uppgifterna skall användas också i en forskningsstudie. I annat fall måste det finnas annat stöd i lag för behandlingen, exempelvis att den är tillåten efter en intresseavvägning (se avsnitt 4.2).

Muntligt samtycke är tillåtet enligt personuppgiftslagen, men ett skriftligt samtycke kan vara att föredra ur bevissynpunkt.

4.1.3 Information

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

- vem som är personuppgiftsansvarig (som regel inte en fysisk person),
- 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 vilka personuppgifter/kategorier av personuppgifter som behandlas, uppgift om mottagarna av personuppgifterna (till vem eller vilka uppgifterna kan komma att lämnas ut), skyldighet att lämna uppgifter och rätten att ansöka om information (så kallat registerutdrag) och få rättelse.⁹

Det är straffbart att lämna osanna uppgifter i informationen till de registrerade.¹⁰

Om personuppgifter kommer att överföras till tredje land, det vill säga länder utanför EU och EES, skall den enskilde informeras om och ge sitt samtycke till överföringen, se vidare under avsnitt 4.1.5.

Datainspektionens iakttagelser:

Det förekom att endast muntlig information och muntligt samtycke inhämtades. Vilken information som lämnades framgick i dessa fall inte av enkätsvaren.

I en genetisk forskningsstudie fanns ingen tydlig information om att det blodprov som lämnades skulle användas för genetiska analyser eller att personuppgifter om genetiska anlag skulle behandlas. I samma studie behandlades personuppgifter om brott. Studien hade tidigare varit föremål för Datainspektionens tillsyn – enligt datalagen – och då påpekades att patientinformationen var bristfällig.

Det var inte ovanligt att informationen innehöll hänvisningar till och uppfyllde de krav som gällde enligt datalagen. Detta gällde även vissa behandlingar som påbörjats efter den 1 oktober 1998 då personuppgiftslagen trädde i kraft.

I vissa enkätsvar lämnades ingen motivering till varför de registrerade inte fick någon information.

⁹ 26 § personuppgiftslagen

¹⁰ 49 § a) personuppgiftslagen

I de fall ett mycket stort antal personer ingick i studien lämnades information i tidningsannonser.

Hos några personuppgiftsansvariga hade personuppgiftsombuden tagit fram ett separat informationsblad som skulle bifogas informationen om själva forskningsstudien. I dessa fall uppfyllde informationen oftast personuppgiftslagens krav.

Datainspektionens synpunkter:

Om en forskningsstudie påbörjas utan att de registrerade fått korrekt information och utan att ett giltigt samtycke har inhämtats och behandlingen inte heller är tillåten efter en intresseavvägning enligt 19 § personuppgiftslagen¹¹ är den behandling av känsliga personuppgifter som utförs inom ramen för studien inte tillåten enligt personuppgiftslagen.

Från och med den 1 oktober 2001 gäller personuppgiftslagen fullt ut för alla behandlingar av personuppgifter. Samtliga datalagstillstånd har *upphört att gälla*. De personuppgiftsansvariga skall på eget ansvar följa personuppgiftslagens regler för information och samtycke. Personuppgiftslagen har mer långtgående krav när det gäller vilken information som de registrerade skall få. Det innebär att den patientinformationen som hittills använts i många forskningsstudier är otillräcklig och behöver kompletteras om ytterligare patienter skall inkluderas i studien.

Personuppgiftsombuden har en viktig roll i arbetet med att sprida information om personuppgiftslagen.

4.1.4 Närmare om den information som skall lämnas före samtycke

Nedan följer en närmare förklaring till de uppgifter som deltagarna i en forskningsstudie skall få information om innan de lämnar sitt uttryckliga samtycke till personuppgiftsbehandlingen.

a) Personuppgiftsansvar

Personuppgiftsansvarig är såsom redogjorts för tidigare (se avsnitt 3.2.4) den som ensam eller tillsammans med andra bestämmer ändamålen med och medel för studien.

¹¹ se avsnitt 4.2

I den information som deltagarna i en forskningsstudie får innan de lämnar sitt samtycke skall det finnas uppgift om den personuppgiftsansvariges identitet. Detta innebär att man skall lämna uppgift om namn och kontaktuppgifter beträffande den juridiska (eller i undantagsfall fysiska) person som är personuppgiftsansvarig.

Datainspektionens iakttagelser:

I patientinformationen saknades nästan alltid uppgift om vem som var personuppgiftsansvarig. Ofta fanns uppgift om vid vilken klinik/sjukhus studien bedrevs och vilka som var kontaktpersoner. Däremot framgick inte vem som var ytterst ansvarig enligt personuppgiftslagen.

Datainspektionens synpunkter:

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

b) Ändamålet med behandlingen

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål, se avsnitt 3.3.1. 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:

Ändamålet med forskningsstudien framgick i de flesta fall av den skriftliga informationen även om ändamålen inte alltid var tillräckligt preciserade. Det förekom dock att det inte framgick att de lämnade uppgifterna skulle användas i en forskningsstudie.

Det förekom också att uppgifterna skulle sparas för ännu inte angivna framtida ändamål. I en studie skulle exempelvis en del av lämnade blodprover sparas "för ev. framtida analyser". Det framgick inte om blodproverna skulle avidentifieras innan de användes för nya analyser. Enligt patientinformationen kunde det bli aktuellt med DNA-analyser.

Det fanns flera liknande exempel där blodprover skulle sparas för liknande inte specificerade ändamål, exempelvis ”för framtida forskning”.

Datainspektionens synpunkter:

Ändamålen skall vara specificerade redan när uppgifterna samlas in. Den enskilde skall informeras om för vilka specifika ändamål personuppgifterna skall behandlas. Skall uppgifterna behandlas för andra ändamål än de ursprungliga skall som regel de registrerade informeras på nytt och lämna sitt uttryckliga samtycke till behandlingen. Ändamål som ”för framtida forskning” är inte tillräckligt specificerade för att det ursprungliga samtycket skall anses omfatta även den personuppgiftsbehandling som kommer att göras i framtida forskning. Om inget nytt samtycke inhämtas måste behandlingen vara tillåten efter en intresseavvägning (se avsnitt 4.2).

Om sparade blodprover förses med koder som gör det möjligt att koppla resultaten av analyserna till enskilda individer är det fråga om personuppgifter när resultaten behandlas. Personuppgiftslagen är därmed tillämplig på behandlingen. Skall nya analyser utföras för andra ändamål än de ursprungliga måste de registrerade informeras på nytt och lämna ett nytt samtycke. Är det fråga om genetiska analyser – behandling av personuppgifter om genetiska anlag – skall dessutom anmälan för förhandskontroll göras innan behandlingen av personuppgifter påbörjas.¹²

Om blodproverna är fullständigt avidentifierade när de nya analyserna utförs gäller dock inte personuppgiftslagen.

c) 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 iakttagelser:

Uppgift om mottagare saknades ofta i informationen till deltagarna i forskningsstudierna. Det framgick inte om skälet var att det endast var berörda forskare som skulle ha tillgång till uppgifterna.

¹² Se Datainspektionens rapport 2002:4 *Personuppgifter i genforskning – uppföljning av förhandskontroller*

Datainspektionens synpunkter:

Den som tackar ja till deltagande i en forskningsstudie skall ha fått 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.

d) 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.¹³ 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 var vanligt att de registrerade inte informerades om sin rätt till registerutdrag.

Datainspektionens synpunkter:

Den enskilde har med personuppgiftslagen fått en utökad rätt till insyn och har rätt att få del av alla uppgifter som den personuppgiftsansvarige behandlar (med undantag för de fall när sekretess gäller gentemot den enskilde).

¹³ 26 § personuppgiftslagen

Det är den personuppgiftsansvarige som är skyldig att se till att det finns rutiner för att lämna registerutdrag.

e) Rätten till rättelse

Den personuppgiftsansvarige är skyldig att på begäran av den enskilde snarast rätta personuppgifter som är felaktiga eller på något annat sätt har behandlats i strid med personuppgiftslagen. 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:

Information om rätten till rättelse var den uppgift som oftast saknades i den information som lämnades till deltagarna i forskningsstudierna.

Datainspektionens synpunkter:

Rätten till rättelse hänger samman med den personuppgiftsansvariges skyldighet att alltid se till att de personuppgifter som behandlas är riktiga. En uppgift är riktig om den stämmer överens med de verkliga förhållandena. Framställs en begäran om rättelse bör den personuppgiftsansvarige skyndsamt utreda om anmärkningen är befogad. Vid oenighet kan den registrerade vända sig till Datainspektionen.

4.1.5 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 huvudregeln¹⁴ är det förbjudet att överföra personuppgifter som är under behandlingen till tredje land om inte landet har en adekvat nivå för skyddet av personuppgifterna. Det finns dock flera undantag från bestämmelsen. Det är alltid tillåtet att överföra personuppgifter till tredje land med den registrerades samtycke. Datainspektionen kan meddela undantag från förbudet i enskilda fall under förutsättning att det finns tillräckliga garantier för de registrerades rättigheter. Regeringen får meddela undantag

¹⁴ 33 § personuppgiftslagen

från förbudet i enskilda fall om det behövs med hänsyn till ett viktigt allmänt intresse.¹⁵

Förbudet är straffsanktionerat.¹⁶

Datainspektionens iakttagelser:

I enkäten efterfrågades inte om uppgifter överfördes till tredje land. Det framkom dock ändå att uppgifter i vissa forskningsstudier skulle överföras till utlandet. I dessa fall framgick det av informationen till de registrerade.

I ett fall skulle avidentifierade blodprover sändas till USA för genetisk analys.

Datainspektionens synpunkter:

Den personuppgiftsansvarige som inte tänker inhämta samtycke till en överföring till ett tredje land måste hålla sig väl underrättad om till vilka länder det är tillåtet att överföra 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 till deltagarna i forskningsstudien om uppgifter överförs till andra länder, även i de fall samtycke inte krävs.

Såsom tidigare påpekats är även kodade eller krypterade uppgifter personuppgifter.

4.1.6 Särskilt om biobanker

Datainspektionens iakttagelser:

I några fall skulle blodprover sparas för framtida ej specificerade forskningsändamål. Avsikten var förmodligen att bygga upp någon form av biobank.

Datainspektionens synpunkter:

Patienterna måste lämna sitt samtycke till den personuppgiftsbehandling som görs inom ramen för en specifik studie. Ett ändamål som ”framtida forskning”

¹⁵ 35 § personuppgiftslagen

¹⁶ 49 § c) personuppgiftslagen

är alltför allmänt hållet för att kunna godtas. Om nya analyser skall utföras på donerat blod måste de registrerade informeras om det nya ändamålet och ge sitt samtycke till den personuppgiftsbehandlingen.

Har inget korrekt samtycke inhämtats måste det finnas annat stöd i personuppgiftslagen för behandlingen; exempelvis att den är tillåten efter en intresseavvägning, se avsnitt 4.2. Om det inte finns sådant lagstöd måste antingen nytt samtycke inhämtas eller så måste den personuppgiftsansvarige upphöra med behandlingen.

Det är värt att notera att den nya biobankslag¹⁷ som trädde i kraft den 1 januari 2003 endast är tillämplig på hanteringen av vävnadsproverna och inte på den personuppgiftsbehandling som utförs i register eller på annat sätt i anslutning till biobankerna. Det innebär att personuppgiftslagen även i fortsättningen är tillämplig på denna personuppgiftsbehandling. Socialstyrelsen har utfärdat föreskrifter och allmänna råd till lagen om biobanker.¹⁸

4.1.7 Uppgifter om släktingar

Datainspektionens iakttagelser:

Det förekom att uppgifter om släktingars hälsa skulle behandlas.

Datainspektionens synpunkter:

Eftersom samtycket skall vara individuellt skall som huvudregel också släktingarna ge sitt informerade samtycke till behandlingen.

¹⁷ lag 2002:297 om biobanker inom hälso- och sjukvården

¹⁸ SOSFS 2002:11

4.1.8 Personuppgifter om genetiska anlag

Datainspektionens iakttagelser:

Personuppgifter om genetiska anlag behandlades inom ramen för flera studier. Anmälan för förhandskontroll hade oftast inte gjorts. Det var dock oklart om de aktuella behandlingarna hade påbörjats innan personuppgiftslagen trädde i kraft.

I ett projekt fick patienterna lämna ett extra blodprov som skulle användas för genetiska analyser i USA. Såvitt framgick skulle dock genanalyserna utföras först när materialet var avidentifierat.

I ett fall framgick av patientinformationen att de registrerade skulle lämna blodprover och att ”ärftliga faktorer” skulle analyseras. Det framgick inte om analyserna skulle ske på avidentifierat material.

I ett fall skulle sambandet mellan brottslighet och genetiska markörer för personlighet studeras. Av patientinformationen – enligt uppgift godkänd av forskningsetisk kommitté – framgick inte tydligt att personuppgifter om genetiska anlag skulle behandlas. I enkäten uppgavs att förhandskontroll skett. Det visade sig dock att Datainspektionen inspekterat den aktuella studien, som påbörjats innan personuppgiftslagen trädde i kraft.

Datainspektionens synpunkter:

De behandlingar som påbörjats efter att personuppgiftslagen trätt i kraft skulle ha anmälts för förhandskontroll.¹⁹

Om genetiska analyser utförs på helt avidentifierat material – det vill säga att det inte längre finns någon som helst möjlighet att koppla resultaten till en enskild person – behandlas inga personuppgifter om genetiska anlag och anmälan för förhandskontroll behöver heller inte göras. Personuppgiftslagen är dock tillämplig på eventuell behandling av personuppgifter som görs fram till dess att proverna avidentifierats.

¹⁹ För vidare information om anmälan för förhandskontroll se Datainspektionens rapport 2002:4 *Personuppgifter i genforskning – uppföljning av förhandskontroller*.

4.2 Efter en intresseavvägning

Under vissa förutsättningar är det tillåtet att behandla känsliga personuppgifter för forskningsändamål utan att de registrerade har samtyckt till behandlingen. Ett grundläggande krav är i sådana fall att den aktuella behandlingen är *nöd- vändig* för det aktuella forskningsändamålet. Med forskning avses verksamhet som bedrivs vid etablerade institutioner såsom universitet eller privata väletablerade forskningsinstitut. Det måste vidare 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 göras. Vid avvägningen skall man göra en helhetsbedömning 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 strykningsrätt samt hur pass svårt det är att identifiera enskilda personer. I de flesta fall bör information lämnas; exempelvis via anslag eller annonser.

Om en forskningsetisk kommitté har godkänt personuppgiftsbehandlingen anses avvägningen som beskrivits ovan ha gjorts och behandlingen är automatiskt tillåten enligt personuppgiftslagen. 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.

Det är enligt 19 § personuppgiftslagen tillåtet att lämna ut personuppgifter som skall användas i sådana forskningsstudier som uppfyller förutsättningarna ovan, om inte bestämmelser om sekretess eller tystnadsplikt hindrar ett utlämnande.

Om den föreslagna etikprövningslagen²⁰ träder i kraft införs en obligatorisk etikprövning av forskning där känsliga personuppgifter skall behandlas utan uttryckligt samtycke från forskningspersonerna. Enligt lagförslaget kommer att etikprövningsnämnderna att ha till uppgift att tillämpa avvägningsnormen.²¹

Datainspektionens iakttagelser:

Flera studier genomfördes utan de registrerades samtycke. De skäl som angavs var exempelvis att antalet registrerade var för stort (i ett fall 1,3 miljoner personer!), att det inte hade bedömts lämpligt att oroa personer lång tid efter

²⁰ Prop. 2002/03:50

²¹ Prop. 2002/03:50 s. 173

att de behandlats för sin sjukdom eller att de flesta hade avlidit. I något fall uppgavs skälet vara att det var länge sedan de registrerade hade kontakt med sjukvården och att de dessutom inte skulle intervjuas.

I stort sett samtliga studier hade enligt uppgift godkänts av forskningsetisk kommitté. Det fanns dock några studier som inte hade granskats och där känsliga personuppgifter – hälsouppgifter – behandlades utan att informationen och samtycket uppfyllde personuppgiftslagens krav.

Det förekom att forskare som besvarade enkäterna inte lämnade någon motivering till att de registrerades samtycke inte inhämtades. Dessa studier uppgavs vara godkända av forskningsetisk kommitté.

Datainspektionens synpunkter:

I de fall en personuppgiftsbehandling som genomförs utan de registrerades samtycke har godkänts av en forskningsetisk kommitté, är behandlingen utan vidare tillåten enligt personuppgiftslagen. En förutsättning är givetvis att den forskningsetiska kommittén verkligen har tagit ställning till personuppgiftsbehandlingen.

Personuppgiftslagens bestämmelser är inte tillämpliga om de uppgifter som behandlas i forskningsstudien avser avlidna personer.

Behandlas känsliga personuppgifter i en forskningsstudie utan att ett korrekt samtycke har inhämtats och utan att behandlingen har godkänts av en etisk kommitté är behandlingen inte förenlig med personuppgiftslagen, såvida behandlingen inte bedöms vara tillåten efter en intresseavvägning.

För att det skall vara tillåtet att behandla känsliga personuppgifter utan samtycke från de registrerade måste det finnas tungt vägande skäl för att samtycke inte skall hämtas in. Det räcker inte att det exempelvis är besvärligt och tidsödande att inhämta samtycke. En helhetsbedömning av samtliga omständigheter skall göras och samhällsintresset av forskningsstudien måste *klart överväga* integritetsintresset. Man bör också notera att även om en intresseavvägning utfaller på ett sådant sätt att samtycke till personuppgiftsbehandlingen inte behöver inhämtas, måste deltagarna i forskningsstudien ändå få den information som krävs enligt personuppgiftslagen, det vill säga samma information som skall lämnas före ett samtycke.²² Hur denna information skall lämnas får avgöras efter vad som är mest lämpligt i det enskilda fallet.

²² Se avsnitt 4.1.3

5. IT-säkerhet

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. I de fall känsliga personuppgifter behandlas ställs högre krav på säkerheten.

Syftet med inspektionerna var bland annat att kontrollera om de personuppgiftsansvariga hade en tillräcklig nivå på IT-säkerheten.

Datainspektionens iakttagelser:

Frågorna om IT-säkerheten besvarades i vissa fall av personuppgiftsombuden och i vissa fall av de enskilda forskarna.

En genomgående brist var att det saknades rutiner för att följa upp loggar.

Många gånger var det bara en person som hade tillgång till uppgifterna och då fanns inget behov av att följa upp loggar. Inte heller i de fall där det fanns mer än en användare gjordes dock någon uppföljning. En vanlig förklaring var att det endast var kodade uppgifter som behandlades.

Det förekom att de enskilda forskarna inte kände till vilka generella rutiner för IT-säkerhet som fanns.

Datainspektionens synpunkter:

Det är den personuppgiftsansvarige som har ansvaret för att sprida information om IT-säkerhet i organisationen och för att ge tydliga instruktioner. Det är också den personuppgiftsansvarige som ansvarar för eventuella säkerhetsbrister.

Om flera personer skall ha tillgång till personuppgifterna bör loggar följas upp.

Även kodade uppgifter är personuppgifter.

Bilaga 1

Tillsynsobjekt

Göteborgs universitet

Karolinska institutet

Kommunalförbundet för Sahlgrenska universitetssjukhuset

Lunds universitet

Linköpings universitet

Luleå tekniska universitet

Stockholms universitet

Umeå universitet

Uppsala universitet

Växjö universitet

Örebro universitet

Bilaga 2

Enkät

Personuppgiftsansvarig.....

Adress.....

.....

.....

.....

Personuppgiftsombud.....

.....

Vilken behandling av personuppgifter avser enkätsvaren?

.....

.....

.....

Kontaktperson.....

Telefonnummer:.....Telefax:.....

e-post:.....

Kort beskrivning av forskningsprojektet

.....

.....

.....

.....

.....

.....

1. Har behandlingen av personuppgifter godkänts av en forskningsetisk kommitté

- ja
- nej

2. Behandlas personuppgifter om genetiska anlag?

- ja
- nej

3. Har anmälan för förhandskontroll gjorts till Datainspektionen?

- ja
- nej

Om ja, ange Datainspektionens diarienummer.....

4. Hur många personer omfattar behandlingen?

.....

5. Vilka uppgifter behandlas?

.....

.....

.....

.....

6. Informeras de registrerade om behandlingen av personuppgifter?

- ja
- nej

Om ja, hur?

.....

.....

- Kopia av den skriftliga informationen bifogas

Om nej, varför inte?

.....
.....
.....

7. Sker behandlingen med stöd av de registrerades samtycke?

- ja
- nej

Om ja, hur inhämtas samtycket?

- muntligen från var och en?

- ja
- nej

- skriftligen från var och en?

- ja
- nej

Om nej, varför inte?

.....
.....
.....
.....
.....

- Kopia av samtyckesformuläret bifogas

8. Hur länge skall personuppgifterna bevaras?

.....
.....

IT-SÄKERHET

9. Har en dokumenterad säkerhetspolicy fastställts, och är denna policy allmänt tillgänglig inom organisationen?

- ja
- nej

10. Har en hotbilds- eller riskanalys gjorts som underlag för utformningen av säkerhetsåtgärderna?

- ja
- nej

11. Motsvarar de valda säkerhetsåtgärderna resultaten av hotbilds- eller riskanalyserna?

- ja
- nej

12. Finns det dokumenterade riktlinjer, rutiner och regler angående personalens användning av och åtkomst till information som innehåller personuppgifter?

- ja
- nej

13. Bedöms säkerheten uppfylla Datainspektionens allmänna råd ”Säkerhet för personuppgifter”?

- ja
- nej

14. Hur många personer har åtkomst till personregistret?

.....

15. Finns behörighetskontrollsystem för att reglera åtkomsten till registret/registren?

- ja
- nej

16. Använder varje behörig person egen användaridentitet?

- ja
- nej

17. Förvaras datorn (datorerna) med personregistret i låsta utrymmen dit endast behörig personal har tillträde?

- ja
- nej

18. Loggas åtkomst till personregistret?

- ja
- nej

Om ja, hur ofta kontrolleras loggen?

.....

19. Finns det rutiner för säkerhetskopiering av personregister och förvaring av dessa säkerhetskopior?

- ja
- nej



Datainspektionen

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

Pris: 50 kr + moms