Yttrande från europeiska datatillsynsmannenom förslaget till Europaparlamentets och rådets direktiv om kvalitets- och säkerhetsnormer för organ av mänskligt ursprung avsedda för transplantation

(2009/C 192/02)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

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

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41,

med beaktande av den begäran om ett yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 som översändes till datatillsynsmannen den 8 december 2008.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

Förslaget till direktiv om kvalitets- och säkerhetsnormer för mänskliga organ avsedda för transplantation

1. Den 8 december 2008 antog kommissionen ett förslag till Europaparlamentets och rådets direktiv om kvalitets- och säkerhetsnormer för organ av mänskligt ursprung avsedda för transplantation (nedan kallat *förslaget*) [1]. Kommissionen översände förslaget till datatillsynsmannen för samråd i enlighet med artikel 28.2 i förordning (EG) nr 45/2001.

2. Förslaget syftar till att garantera höga kvalitetsnormer för mänskliga organ avsedda för transplantation, för att garantera en hög hälsoskyddsnivå för människor. I förslaget

   — fastställs grundläggande kvalitets- och säkerhetskrav för medlemsstaternas transplantationssystem, och föreskrivs att en behörig nationell myndighet ska inrättas eller utses för att garantera att dessa krav efterlevs; för detta ändamål kommer nationella kvalitetsprogram att upprättas för tillvaratagande och överföring av mänskliga organ i alla länder, inbegripet – bland annat – ett system för *rapportering om allvarliga komplikationer och biverkningar* samt en *spårbarhetsmekanism* för att alla organ ska kunna spåras från donation till mottagande och tvärtom,

   — föreskrivs skydd av givarna och mottagarna; särskilt avseende levande givare inbegriper förslaget åtgärder för utvärdering av givarens hälsa och omfattande information om riskerna med donation, införande av register för levande donatorer samt åtgärder för att garantera altruistiska och frivilliga donationer av organ från levande donatorer,

   — underlättas samarbete mellan medlemsstaterna och *gränsöverskridande utbyte av organ* (också mellan medlemsstaterna och tredjeländer), standardisering av insamling av relevanta uppgifter om kännetecken hos ett organ och införande av en mekanism för överföring av dessa uppgifter.

3. Genomförandet av det föreslagna systemet för organdonation och transplantation kräver att de behöriga organisationerna och hälso- och sjukvårdspersonal i de olika medlemsstaterna behandlar personuppgifter som rör organgivarnas och mottagarnas hälsa (hälsouppgifter). Dessa uppgifter anses vara känsliga och omfattas av strängare dataskyddsbestämmelser i enlighet med artikel 8 i direktiv 95/46/EG som rör särskilda kategorier av uppgifter.

4. Mer specifikt behandlas givarnas uppgifter i de tillvaratagande organisationer som utför karakteriseringen av givaren och organet och således fastställer huruvida organet i fråga är lämpligt för transplantation (en förteckning över dessa uppgifter finns i bilagan till förslaget). Mottagarnas (patienternas) uppgifter behandlas i de transplantationscentrum där operationen faktiskt kommer att äga rum. Trots att mottagaren inte får någon information om givarens uppgifter (och tvärtom) finns ett krav på att de nationella behöriga myndigheterna behåller full spårbarhet avseende organet från givaren till mottagaren (och tvärtom) vilket bör vara möjligt också i fall av gränsöverskridande utbyte av organ.

Samråd med datatillsynsmannen

5. Datatillsynsmannen välkomnar att kommissionen samråder med honom och att det hänvisas till dessa samråd i förslagets ingress i enlighet med artikel 28 i förordning (EG) nr 45/2001.

[1] KOM(2008) 818 slutlig.

6. Förslaget kommer att främja organdonationer och transplantationsförfaranden i slutgiltigt syfte att öka tillgången på organ och minska dödligheten bland dem som står på organväntelistorna. Det kompletterar den befintliga lagstiftningsramen när det gäller användningen av biologiska material av mänskligt ursprung ([1]). Det kan vidare ses som en del av den övergripande EG-strategin för att fastställa olika slags gemensamma normer när det gäller att tillhandahålla hälso- och sjukvårdstjänster i medlemsstaterna med det grundläggande målet att främja dessa tjänsters gränsöverskridande tillgänglighet i hela Europa ([2]). I enlighet med vad Europeiska datatillsynsmannen redan framfört i sitt yttrande om patienträttigheter vid gränsöverskridande hälso- och sjukvård stöder han en sådan strategi. Han understryker emellertid åter behovet av ett samordnat och enhetligt perspektiv när det gäller uppgiftsskydd inom de olika hälso- och sjukvårdsrelaterade initiativen. ([3])

7. Förslaget har redan beaktat de behov av uppgiftsskydd som uppstår både vad gäller givare och mottagare av organ. Den viktigaste delen är kravet att givarens och mottagarens identitet ska vara konfidentiell (skälen 11 och 16, artiklarna 10 och 17). Dessutom finns ett antal allmänna hänvisningar till uppgiftsskydd i några delar av förslaget (skäl 17, artiklarna 16, 4.3 a, 15.3 och 19.1 a samt bilagan) samt mer specifika hänvisningar till behovet av att samarbeta med de nationella dataskyddsmyndigheterna (artiklarna 8 f och 20.2).

8. Europeiska datatillsynsmannen välkomnar ovan nämnda innehåll. Han önskar emellertid uttrycka sina farhågor när det gäller vissa av bestämmelserna som inte är klart definierade eller klart utformade och därför leder till tvetydigheter som eventuellt skulle kunna påverka medlemsstaternas enhetliga genomförande av förslaget.

9. Mer specifikt är den ibland motsägelsefulla användningen av begreppen ”organspårbarhet” och ”givar- och mottagaranonymitet” något som kräver ytterligare klarläggande och förtydligande. I samband med detta bör behovet av att anta förstärkta säkerhetsåtgärder för skydd av givarens och mottagarens personuppgifter på medlemsstatsnivå ytterligare understrykas för att garantera en förstärkt uppgiftsskyddsnivå i de olika europeiska länderna och garantera uppgiftsskydd vid gränsöverskridande utbyte av organ (inom eller utanför Europa).

10. Detta yttrande kommer att ytterligare klargöra ovan nämnda frågor i syfte att förbättra det nuvarande uppgiftsskyddet vad gäller innehållet i förslaget både i fråga om tydlighet och konsekvens.

([1]) Denna ram inkluderar direktiven 2002/98/EG, 2004/33/EG, 2005/61/EG och 2005/62/EG för blod och blodprodukter samt direktiven 2004/23/EG, 2006/17/EG och 2006/86/EG för mänskliga vävnader och celler.

([2]) Se förslaget till Europaparlamentets och rådets direktiv om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård, KOM(2008) 414 slutlig.

([3]) Europeiska datatillsynsmannens yttrande av den 2 december 2008 om förslaget till direktiv om tillämpning av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

II. **KLARLÄGGANDE AV BEGREPPEN SPÅRBARHET OCH ANONYMITET**

Tillämpligheten av direktiv 95/46/EG

11. Enligt artikel 2 a i direktiv 95/46/EG om skydd av personuppgifter avses med *personuppgifter* följande: ”varje upplysning som avser en identifierad eller identifierbar fysisk person; en identifierbar person är en person som kan identifieras, direkt eller indirekt, framförallt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet”.

12. Biologiska material av mänskligt ursprung såsom organ, vävnader, celler eller blod kan definieras som material som kan utvinnas från människokroppen. Det kan ifrågasättas om dessa material i sig kan anses som personuppgifter. Det är emellertid odiskutabelt att sådana material kan användas som *källor* till personlig information om innehavaren. Utvinning av sådan information är ofta syftet med bearbetningen av biologiska material. Och även utan ett sådant syfte åtföljs de biologiska materialen ofta av sådan erhållen information. I dessa situationer gäller bestämmelserna i direktiv 95/46/EG ([4]). Det vill säga så länge som innehavaren av det biologiska materialet är en *identifierad* eller *identifierbar* (fysisk) person.

13. I skäl 26 i direktiv 95/46/EG förklaras hur man fastställer om en person är identifierbar: ”alla hjälpmedel [bör] beaktas som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan *person*”. I samma skäl förklaras vidare att bestämmelserna i direktiv 95/46/EG inte är tillämpliga om informationen gäller en person som inte eller inte längre är identifierbar – sådana uppgifter anses vara *anonyma*.

14. I rekommendation (2006) 4 har Europarådet behandlat den specifika frågan om biologiska materials identifierbarhet och gjort en åtskillnad mellan identifierbara och icke identifierbara biologiska material ([5]).

15. Enligt rekommendationen är *identifierbara biologiska material* ”sådana biologiska material som ensamma eller i kombination med tillhörande uppgifter möjliggör identifiering av de berörda personerna antingen direkt eller genom användning av en kod” ([6]) I det senare fallet kan användaren av de biologiska materialen antingen ha tillgång till koden (*kodat material*) eller inte ha tillgång till koden som då kontrolleras en tredje part (*kopplat anonymiserat material*). I yttrande 4/2007 använde arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (nedan kallad *arbetsgruppen*) i fråga om personuppgifter begreppet *spårbara pseudonymiserade uppgifter* för att beskriva

([4]) Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, yttrande nr 4/2007 om begreppet personuppgifter, s. 9.

([5]) Rekommendation Rec(2006) 4 från ministerkommittén till medlemsstaterna om forskning om biologiska material av mänskligt ursprung.

([6]) Artikel 3(i) i rekommendation Rec(2006) 4.

indirekt identifierbar information om personer som fortfarande kan utnyttjas för att spåra och identifiera dessa personer under förutbestämda villkor ([1]). *Nyckelkodade uppgifter* nämns som ett exempel där personuppgifter öronmärks genom en kod medan den nyckel som gör kopplingen mellan koden och de gemensamma identifikationskoderna för personerna förvaras separat. Om de koder som används är unika för varje specifik person är en identifikation möjlig genom den nyckel som används för att göra kodningen.

16. Rekommendationen hänvisar även till *icke identifierbart biologiskt material* (eller *icke kopplat anonymiserat material*) som ”det biologiska material som ensamt eller i kombination med tillhörande uppgifter inte med rimliga ansträngningar möjliggör identifieringen av de berörda personerna” ([2]). Dessa skulle då verkligen anses som anonyma uppgifter enligt vad som fastställs i direktiv 95/46/EG.

17. Det framgår av ovanstående att direktiv 95/46/EG är tillämpligt på insamling, förvaring och behandling av identifierbara organ och efterföljande utvinning av information från dessa organ så länge som det är möjligt att, med beaktande av alla hjälpmedel som rimligen kan komma att användas, identifiera vederbörande. Såsom framgår nedan kommer organens permanenta spårbarhet enligt vad som planeras i det föreslagna direktivet, att göra det möjligt att identifiera personerna under hela processen.

Spårbarhet kontra anonymitet för mänskliga organ

18. Biologiska materials spårbarhet är möjligheten att spåra innehavaren av materialen och på så sätt identifiera honom eller henne. Med andra ord så fort det är möjligt att antingen direkt eller indirekt spåra innehavarna av biologiska material kan dessa anses som indentifierbara och vice versa. Begreppen *spårbarhet* och *på ett identifierbart sätt* är därför i princip starkt kopplade till varandra. Spårbarhet och anonymitet kan däremot inte föreligga samtidigt vad gäller dessa uppgifter. De är varandras motsatser. Om en viss information verkligen är anonym är det inte möjligt att identifiera och spåra personerna.

19. När det gäller det aktuella förslaget är spårbarhet ett obligatoriskt krav som ska fastställas inom ramen för medlemsstaternas nationella kvalitetsprogram i två riktningar, dvs. både till givarna och till mottagarna. Detta betyder att även om information en om givarna och mottagarna är konfidentiell så är den organrelaterade informationen identifierbar. Detta tas också upp i förslagets definition av spårbarhet i artikel 3: ”den behöriga myndighetens möjligheter att lokalisera och identifiera organ under varje steg av kedjan från donation till transplantation eller bortskaffande, vilket under särskilda omständigheter i detta direktiv är tillåtet för att identifiera givaren och organisationen för tillvaratagande, identifiera mottagarna på transplantationscentrum, lokalisera och identifiera alla relevanta uppgifter som inte är personuppgifter om de produkter och material som kommer i kontakt med detta organ”.

20. Vidare anges följande i artikel 10.1 i förslaget om spårbarhet: ”Medlemsstaterna ska se till att alla organ som tas tillvara och allokeras inom medlemsstaten kan spåras från givare till mottagare och omvänt för att skydda givarnas och mottagarnas hälsa.” I artikel 10.3 anges även följande: ”Medlemsstaterna ska se till att a) den behöriga myndigheten eller andra organ som deltar i kedjan från donation till transplantation eller bortskaffande bevarar de uppgifter som är nödvändiga för att garantera spårbarhet i alla steg i kedjan från donation till transplantation eller bortskaffande i enlighet med nationella kvalitetsprogram, b) de uppgifter som krävs för att garantera fullständig spårbarhet ska bevaras i minst 30 år efter donationen. Dessa uppgifter får lagras i elektronisk form”.

21. Även om spårbarhetsförfarandet är underkastat genomförandeåtgärder (se artikel 25 i förslaget) verkar ett system med indirekt identifiering av givare och mottagare vara den mest troliga lösningen, som överensstämmer eller åtminstone är kompatibel med direktiv 2004/23/EG ([3]) om vävnader och celler och den europeiska identifieringskod som fastställs där ([4]). I sådant fall gäller den behandling som rör givare och mottagare inom ramen för förslaget kopplat

([1]) Yttrande 4/2007, s. 18, från arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter.

([2]) Artikel 3(ii) i rekommendation Rec(2006) 4.

([3]) Eftersom organgivare mycket ofta är vävnadsgivare finns det ett behov av att spåra och rapportera oväntade biverkningar även i systemet för övervakning av vävnader, vilket kräver kompatibilitet med den indirekta metod för identifiering som används i det systemet. Se vidare: Europaparlamentets och rådets direktiv 2004/23/EG av den 31 mars 2004 om fastställande av kvalitets- och säkerhetsnormer för donation, tillvaratagande, kontroll, bearbetning, konservering, förvaring och distribution av mänskliga vävnader och celler, EUT L, 102/48, 7.4.2004, och kommissionens direktiv 2006/86/EG av den 24 oktober 2006 om tillämpning av Europaparlamentets och rådets direktiv 2004/23/EG med avseende på spårbarhetskrav, anmälan av allvarliga biverkningar och komplikationer samt vissa tekniska krav för kodning, bearbetning, konservering, förvaring och distribution av mänskliga vävnader och celler, EUT L 294/32, 25.10.2006.

([4]) Koden innehåller ett unikt identifikationsnummer för varje donation, vilket tillsammans med identifikationen för vävnadsinrättningen och produkten gör att givaren och mottagaren kan spåras. I artikel 10 i direktiv 2006/86/EG anges i synnerhet att ”En individuell europeisk identifikationskod skall tilldelas allt donerat material vid vävnadsinrättningen, för att säkerställa korrekt identifiering av givaren och spårbarhet för allt donerat material och för att ange de viktigaste egenskaperna och särdragen hos vävnaderna och cellerna.” Som anges i bilaga VII till det direktivet har koden två delar: a) uppgifter om givaren, inklusive ett unikt identifikationsnummer för donationen och angivande av vävnadsinrättningen samt b) produktbeskrivning, inklusive produktkod, delpartinummer och utgångsdatum.

anonymiserat biologiskt material eller, med användning av dataskyddsterminologi, spårbara pseudonymiserade uppgifter (se ovan punkt 15) som omfattas av bestämmelserna i direktiv 95/46/EG.

22. Det noteras dock att trots kraven på tydlig spårbarhet och identifierbarhet så används på vissa ställen i förslaget termen ”anonymitet” eller ”avidentifiering” vid hänvisning till uppgifter om givare och mottagare. Som framgår av tidigare punkter är detta motsägelsefullt och mycket förvirrande ([1])

23. I artikel 10.2 i förslaget, som fastställer behovet av ett identifieringssystem, anges i synnerhet följande: ”Medlemsstaterna ska se till att man för identifiering av givare tillämpar ett system, varigenom varje donation och vart och ett av de tillhörande organen kan identifieras. Medlemsstaterna ska se till att detta system för identifiering av givare utformas så att inga personuppgifter (eller så få som möjligt) behöver samlas in, hanteras eller användas. Särskilt bör man utnyttja möjligheten till pseudonymisering eller avidentifiering” ([2]). Europeiska datatillsynsmannen anser att de termer som är understrukna i detta stycke står i motsättning till begreppet spårbarhet, eftersom det inte finns någon möjlighet att få fram spårbara och identifierbara uppgifter när givarna och mottagarna avidentifieras. Dessutom är det anmärkningsvärt att stycket i fråga avser identifiering av givaren medan identifiering av mottagaren (som också är en del av processen) inte nämns alls.

24. Detta motsatsförhållande framgår ännu tydligare i artikel 17 om avidentifiering av givare och mottagare, där följande anges: ”Medlemsstaterna ska vidta alla nödvändiga åtgärder för att se till att givarnas och mottagarnas alla personuppgifter som sammanställs enligt bestämmelserna i detta direktiv har gjorts anonyma så att givaren och mottagaren inte längre kan identifieras.” Den artikeln står helt i strid med förslagets artiklar om spårbarhet.

Konfidentialitet i stället för anonymitet

25. Europeiska datatillsynsmannen uppfattar det så att termen anonymitet egentligen används för att understryka behovet av ökad *konfidentialitet* ([3]) när det gäller uppgifter om givare och mottagare, dvs. att uppgifterna endast ska vara åtkomliga för dem som bemyndigats att få tillgång till dem. Europeiska datatillsynsmannen förmodar att avidentifiering i synnerhet används för att ange ett indirekt identifikationssystem för givare och mottagare ([4]), vilket också kan härledas från det sätt som termen används på i direktiv 2004/23/EG om vävnader och celler. Som tidigare nämnt är dock inte anonymitet den korrekta termen.

26. Ett exempel på hur både dataskydd och spårbarhet kan hanteras under transplantationsprocessen återfinns i Europarådets tilläggsprotokoll till konventionen om mänskliga rättigheter och biomedicin ([5]). Där används begreppet konfidentialitet i stället för anonymitet. Artikel 23.1 i protokollet anger i synnerhet att alla personuppgifter med anknytning till den person från vilken organ eller vävnad tagits och alla uppgifter som rör mottagaren ska anses vara konfidentiella. Sådana uppgifter får bara insamlas, behandlas och vidarebefordras enligt de regler som gäller för tystnadsplikt och skydd av personuppgifter. Punkt 2 i samma artikel anger vidare att bestämmelserna i punkt 1 ska tolkas utan att det påverkar tillämpningen av bestämmelser som, under förutsättning att lämpliga skyddsåtgärder finns, möjliggör insamling, behandling och vidarebefordran av nödvändiga uppgifter om den person från vilken organ eller vävnader tagits eller om mottagaren av organ eller vävnader i den mån som detta krävs för medicinska ändamål, inklusive spårbarhet, i enlighet med artikel 3 i detta protokoll.

27. På grundval av ovanstående rekommenderar Europeiska datatillsynsmannen att språket i vissa delar av förslaget ändras så att tvetydighet undviks och så att det klart framgår att uppgifterna inte är anonyma, men bör behandlas enligt stränga regler för konfidentialitet och säkerhet. Europeiska datatillsynsmannen rekommenderar i synnerhet följande ändringar:

([1]) Denna anmärkning framfördes också av Europeiska datatillsynsmannen i kommentarerna av den 19.9.2006 om offentligt samråd om framtida åtgärder på området donation och transplantation av organ.

([2]) Egen understrykning.

([3]) Säkerställande av att uppgifter endast är åtkomliga för dem som bemyndigats tillgång (ISO-definition, källa: http://www.wikipedia.org).

([4]) Beroende på sammanhang används termen ”avidentifiering” ibland för att ange indirekt identifierbara uppgifter, t.ex. när det gäller statistik. Detta är däremot inte korrekt ur dataskyddssynpunkt, vilket förklarades av Europeiska datatillsynsmannen i hans yttranden om förslaget till Europaparlamentets och rådets förordning om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet (KOM(2007) 46 slutlig) och förslaget till Europaparlamentets och rådets förordning om europeisk statistik (KOM(2007) 625 slutlig).

([5]) Europarådet, tilläggsprotokoll till konventionen om mänskliga rättigheter och biomedicin avseende transplantation av organ och vävnader av mänskligt ursprung, Strasbourg, 24.1.2002, se http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=186&CM=8&DF=2/13/2009&CL=ENG för en tabell över ratificeringsläget. Se även: Europarådet, konvention om skydd av människan och mänsklig värdighet vid biologisk och medicinsk tillämpning: konventionen om mänskliga rättigheter och biomedicin, Oviedo, 4.4.1997, se http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=2/13/2009&CL=ENG för en tabell över ratificeringsläget.

— Skäl 16 sista meningen: ”I linje med stadgan och med hänsyn till konventionen om de mänskliga rättigheterna och biomedicin bör program för organtransplantation bygga på principerna om frivillig donation utan ersättning, givarens oegennytta samt solidaritet mellan givare och mottagare, samtidigt som stränga regler för konfidentialitet och säkerhet garanteras till skydd för givarnas och mottagarnas personuppgifter.”

— I artikel 10.2: ”Medlemsstaterna ska se till att man för identifiering av givare och mottagare tillämpar ett system, varigenom varje donation och vart och ett av de tillhörande organen kan identifieras. Medlemsstaterna ska se till att detta system för identifiering av givare och mottagare utformas och väljs ut så att så få personuppgifter som möjligt används, särskilt med hjälp av metoder för pseudonymisering, och att nödvändiga tekniska och organisatoriska åtgärder finns på plats till skydd för dessa uppgifter.”

— Artikel 17 kan utgå, genom att dess innehåll (med tanke på behoven av konfidentialitet) införlivas med en ny punkt i artikel 16 om Skydd av personuppgifter, konfidentialitet och säkerhet vid databehandling (se punkt 36 nedan).

28. Dessutom föreslår Europeiska datatillsynsmannen att behovet av *förstärkt skydd* av givarnas och mottagarnas uppgifter utvecklas ytterligare genom tillämpning av *stränga säkerhetsåtgärder* både på nationell och gränsöverskridande nivå. Detta kommer att diskuteras i de senare delarna av detta yttrande.

III. **TONVIKT PÅ NATIONELLA ÅTGÄRDER FÖR UPPGIFTSSKYDD**

Grundläggande säkerhetsbehov och -krav

29. Som framgår av förslaget försiggår behandlingen av personuppgifter från givare och mottagare i huvudsak på nationell nivå, dvs. i medlemsstaternas centrum för tillvaratagande och transplantation. Det är på den nivån som registret över levande donatorer finns. Även om spårbarhetsmekanismen ännu inte har definierats kan det förväntas att kodning också kommer att ske på nationell nivå även om ett europeiskt kodsystem används, eftersom identifiering av givare och mottagare endast är möjlig via de nationella behöriga myndigheterna.

30. Därför är det av yttersta vikt att genomföra en politik för informationssäkerhet på grundval av *strikta och sunda säkerhetsåtgärder* vid de relevanta nationella myndigheterna, särskilt för att uppfylla de konfidentialitetskrav avseende givarna och mottagarna som fastställs i förslaget samt för att garantera *integritet* ([1]), *ansvarighet* ([2]) *och tillgänglighet* ([3]) i fråga om dessa uppgifter. Politiken för informationssäkerhet bör alltså omfatta aspekter som rör fysisk och logisk säkerhet och bl.a. inriktas på att kontrollera inmatning, tillgång, registrering, överföring och vidarebefordran av uppgifter samt datamedier och lagringskontroll.

31. När det gäller konfidentialitet kan medicinska uppgifter om mottagarna ([4]), liksom uppgifter som används för att beskriva givarna och för uppföljning (även i förhållande till ”marginella givare” ([5])), röja känslig information om dem som kan påverka dem socialt, yrkesmässigt och/eller i privatlivet. Skyddet av givarens personuppgifter är av än större vikt när levande givare eller personer som har givit samtycke till att donera ett eller flera av sina organ efter sin död skulle kunna bli offer för handel med mänskliga organ och vävnader om denna information röjs. Integriteten för de uppgifter som rör organen är också mycket viktig, eftersom ett enda misstag i den överförda informationen kan vara livshotande för mottagaren. Detsamma gäller exaktheten i fråga om givarens hälsouppgifter före transplantationen, eftersom dessa uppgifter används för att fastställa om organet är lämpligt eller ej. Eftersom så många olika organisationer är involverade i det övergripande systemet för donation och transplantation, bör det när det gäller ansvarighet finnas möjlighet att göra dessa enheter medvetna om och beredda att ta ansvar för sitt handlande, t.ex. i ett fall när uppgifter om givare avslöjas för obehöriga eller när de medicinska uppgifterna om ett organ inte är korrekta. Eftersom hela systemet bygger på överföring av uppgifter om organ och spårbarhetsmekanismen från givare till mottagare bör slutligen dessa uppgifter vid behov och utan

([1]) Säkerställande av att uppgifterna är fullständiga, att de bibehålls identiskt under en åtgärd (t.ex. överföring, lagring eller hämtning), att uppgifterna bevaras för sitt avsedda ändamål eller, beroende på åtgärd, vad som förväntas i fråga om uppgifternas kvalitet. Kort sagt, dataintegritet är en garanti för att uppgifterna är enhetliga och korrekta (källa: http://www.wikipedia.org). och säkerställer att uppgifterna endast är åtkomliga för och kan ändras av dem som är bemyndigade att göra detta (källa: http://searchdatacenter.techtarget.com).

([2]) Förpliktelse att stå till ansvar för vidtagna åtgärder. oavvislighet: säkerställande av att uppgifterna översänds och mottas av de parter som hävdar att de har sänt och mottagit dem: det begrepp som säkerställer att en part i en tvist inte kan förneka eller vederlägga ett uttalandes giltighet (källa: http://www.wikipedia.org).

([3]) Den grad i vilken uppgifterna omedelbart är tillgängliga (källa: http://www.pcmag.com).

([4]) Det måste också noteras att det faktum att ett organ transplanteras till en mottagare i sig utgör känsliga personuppgifter om personens hälsa.

([5]) Potentiella givare, som inte är idealiska givarkandidater, men som kan komma i fråga under vissa omständigheter, t.ex. för äldre mottagare. Se vidare: Kommissionens arbetsdokument: följedokument till förslag till Europaparlamentets och rådets direktiv om kvalitets- och säkerhetsnormer för mänskliga organ som är avsedda för transplantation samt (*Meddelande från kommissionen: handlingsplan om donation och transplantation av organ (2009–2015): bättre samarbete mellan medlemsstaterna, konsekvensanalys,*) 8.12.2008.

dröjsmål vara tillgängliga för de behöriga personerna (i annat fall skulle bristen på tillgänglighet äventyra själva systemets funktion).

32. I *detta* avseende bör det inrättas lämpliga *mekanismer för tillstånd* i enlighet med särskilda *strategier för kontroll av tillgång*, när det gäller såväl nationella databaser som gränsöverskridande utbyte av organ. Dessa strategier bör inledningsvis definieras på organisatorisk nivå, särskilt med avseende på förfaranden för identifiering av givare och mottagare (t.ex. vem som har tillgång till vilka uppgifter och under vilka omständigheter). På detta sätt kan man fastställa *tillgångsrättigheter* och olika *tillgångsscenarier* där dessa rättigheter kan utövas (t.ex. de omständigheter under vilka en organisation för tillvaratagande kan lämna ut uppgifter till den behöriga myndigheten samt förfarandena för detta, eventuella fall där givarens identitet måste lämnas ut till mottagaren samt förfarandena för detta osv.). För att strategierna ska vara effektiva bör de personer som deltar i behandlingen vara bundna av särskilda *sekretessregler*.

33. När dessa strategier har fastställts kan de genomföras på teknisk nivå och användarnas tillgång till *system* och applikationer kan således kontrolleras i enlighet med de i förväg fastställda tillgångsrättigheterna. Beprövad teknik såsom *kryptering* och *digitala certifikat* [1] (t.ex. på grundval av *system med infrastruktur för kryptering av öppna nycklar* [2]) kan användas i detta syfte. *Rollbaserade autentiseringsmekanismer* kan också användas för att begränsa användarnas tillgångsrättigheter på grundval av deras funktion (t.ex. bör endast läkare ha rätt att ändra medicinska uppgifter om mottagare och givare i nationella databaser).

34. Kontrollen av tillgång bör kompletteras med möjligheten att *arkivera* användarnas åtgärder (t.ex. läs- och skrivrättigheter när det gäller tillträde till medicinska uppgifter), särskilt när elektroniska system används. Det bör också finnas hårdvaru- och programvarubaserade *säkerhetsåtgärder* för att se till att databaser över givare och organ är *fullt funktionsdugliga* som ett centralt inslag i det föreslagna donations- och transplantationssystemet. Tillgång till uppgifter bör betraktas som en av hörnstenarna i systemet. I detta avseende bör politiken för informationssäkerhet grundas på en *sund riskanalys och -bedömning* och även inbegripa inslag såsom hantering av incidenter och driftskontinuitet. Alla dessa inslag bör bevaras och förbättras genom regelbundna övervaknings- och översynsprocesser. *Oberoende granskningar* kan också effektivisera och förbättra systemet, varvid särskild uppmärksamhet ska ägnas åt pseudonymisering, spårbarhet och praxis för uppgiftsöverföring.

35. Datatillsynsmannen skulle vilja att det lades större tonvikt vid behovet av sådana åtgärder i *samband* med förslaget till direktiv.

Förbättrade säkerhetsbestämmelser i förslaget

36. I *artikel* 16 i förslaget om skydd av personuppgifter, sekretess och säkerhet i behandlingen anges det att ”(m)edlemsstaterna ska se till att den grundläggande rätten till skydd av personuppgifter skyddas fullt ut och effektivt inom all verksamhet för organtransplantation, enligt gemenskapslagstiftningen om skydd av personuppgifter, såsom i direktiv 95/46/EG och i synnerhet enligt artiklarna 8.3, 17 och 28.2 i det direktivet”. Datatillsynsmannen rekommenderar att det läggs till ett *andra stycke* i denna artikel med en beskrivning av de grundläggande principerna för att säkerställa säkerhet på medlemsstatsnivå och med minst en hänvisning till följande punkter:

— Det bör inrättas en informationssäkerhetspolitik för genomförandet av tekniska och organisatoriska åtgärder i syfte att säkerställa konfidentialitet, integritet, ansvarighet och tillgänglighet när det gäller givares och mottagares personuppgifter.

— Det bör fastställas en särskild politik för konfidentialitet och tillgångskontroll i alla medlemsstater med angivande av tillgångsrättigheter, roller och ansvar för alla inblandade parter (givare, organisationer för tillvaratagande, transplantationscentrum, mottagare, nationella behöriga myndigheter, gränsöverskridande behöriga myndigheter) i hela spårbarhetskedjan. Det bör finnas särskilda garantier för datakonfidentialitet för de personer som deltar i behandlingen, särskilt om dessa personer inte är bundna av sjukvårdssekretess (t.ex. uppförandekoder för sekretess och åtgärder inriktade på medvetenhet).

— Behovet av säkerhetsmekanismer (t.ex. kryptering och digitala certifikat) i de nationella databaserna bör beskrivas i korta drag. Särskilt när det gäller givarregister bör principen med inbyggda skyddsmekanismer för den personliga integriteten (”privacy by design”) tillämpas för att alla nödvändiga säkerhetskrav ska inbegripas från och med de inledande skedena.

— Det bör också inrättas förfaranden för att skydda dataskyddsrättigheter för givare och mottagare, särskilt rätten till tillgång och rättelse samt rätten till information. Det bör även ägnas särskild uppmärksamhet åt fall där givare vill återkalla sitt samtycke eller inte godkänns som givare (efter karakterisering av organet och givaren). I detta fall bör det fastställas ett särskilt förfarande och en tidsfrist för lagring av deras uppgifter.

---

[1] Den elektroniska motsvarigheten till ett ID-kort som autentiserar den person som en digital signatur härrör från (källa: http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html).

[2] Infrastruktur för kryptering av öppna nycklar (Public Key Infrastructure – PKI) består av hårdvara, mjukvara, människor, politik och förfaranden för att skapa, hantera, lagra, distribuera och återkalla digitala certifikat (källa: http://www.wikipedia.org).

— Informationssäkerhetspolitiken bör också inbegripa åtgärder som syftar till att garantera integritet för och oavbruten tillgång till uppgifterna. Utöver riskbedömning bör inslag såsom hantering av incidenter och driftskontinuitet beaktas i informationssäkerhetspolitiken.

— Informationssäkerhetspolitiken bör vara föremål för regelbunden övervakning och översyn, däribland oberoende granskningar.

37. Datatillsynsmannen rekommenderar att ovan nämnda inslag ska införas i artikel 16 och därefter specificeras ytterligare som en del av genomförandeåtgärderna i artikel 25, särskilt punkt 1 a, b och c.

IV. **SÄKERHETSÅTGÄRDER FÖR GRÄNSÖVERSKRIDANDE UTBYTE AV ORGAN**

Harmonisering mellan medlemsstaterna när det gäller säkerhetsfrågor

38. Gränsöverskridande utbyte av organ kommer i praktiken alltid att innebära behandling av personuppgifter, eftersom även om dessa är kodade kan organen fortfarande (indirekt) identifieras genom de nationella behöriga myndigheterna.

39. Datatillsynsmannen har redan framfört sin åsikt om säkerhetsbehoven när det gäller skyddet av personuppgifter inom gränsöverskridande hälso- och sjukvård i Europa och har bland annat framhållit behovet av att harmonisera informationssäkerhetspolitiken mellan medlemsstaterna i syfte att uppnå en sund dataskyddsnivå ([1]). Datatillsynsmannen rekommenderar att denna aspekt också ska nämnas i det nuvarande förslaget och särskilt i skäl 17 där bestämmelsen i direktiv 95/46/EG om säkerhet vid behandling omnämns.

Inrättande av systemet för spårbarhet

40. I detta särskilda fall är den kommande spårbarhetsmekanismen en viktig parameter för den gränsöverskridande datasäkerheten. Utöver de säkerhetsåtgärder som tillämpas i medlemsstaterna bör därför särskild uppmärksamhet ägnas åt möjligheterna till pseudonymisering för att identifiera givare och mottagare (t.ex. typ av kodifiering, möjlighet till dubbel kodifiering etc.) och bibehållandet av kompatibilitet med systemet för identifiering av vävnader och celler.

41. Datatillsynsmannen rekommenderar att det görs en särskild hänvisning till detta i artikel 25 i förslaget till direktiv om genomförandeåtgärder, och att punkt 1 b ändras på följande sätt: ”Förfaranden för att säkerställa full spårbarhet för organ, bl.a. krav på märkning, samtidigt som konfidentialiteten för givare och mottagare skyddas under hela spårbarhetsförfarandet och kompatibiliteten med systemet för identifiering av vävnader och celler bibehålls.”

Organutbyte med tredjeländer

42. Säkerhetsbehoven är ännu viktigare när uppgifter utbyts med tredjeländer där en tillräcklig dataskyddsnivå inte alltid kan säkerställas. Ett särskilt system för överföring av personuppgifter till tredjeland fastställs i artiklarna 25 och 26 i direktiv 95/46/EG. Datatillsynsmannen är medveten om att dataskyddskraven inte får hindra en snabb och effektiv överföring av organ, vilket är en nödvändighet i systemet för organdonation och ofta även kan vara en fråga om liv eller död. Möjligheterna att tillåta en överföring trots att det i tredjelandet saknas en tillräcklig nivå för skyddet av personuppgifter i allmänhet bör därför undersökas. Man bör därmed beakta att riskerna troligen är lägre än på nationell nivå på grund av att individen identifieras indirekt på gränsöverskridande nivå samt att de nationella behöriga myndigheterna utövar en övergripande tillsyn av systemet ([2]).

43. Datatillsynsmannen anser därför att den behöriga myndighet som ansvarar för godkännande av sådana överföringar ska rådgöra med den nationella dataskyddsmyndigheten för att, mot bakgrund av de tänkbara undantag som anges i artikel 26 i direktiv 95/46/EG, utvecklade de ramar som krävs för en säker, snabb och effektiv överföring av uppgifter om organ till och från tredjeländer. Datatillsynsmannen rekommenderar att det görs en hänvisning till detta i artikel 21 om organutbyte med tredjeländer eller i det relevanta skäl 15.

Genomförandeåtgärder

44. Datatillsynsmannen uppmanar slutligen lagstiftaren att, med beaktande av artikel 25, se till att alla berörda parter, däribland datatillsynsmannen och arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, alltid hörs när genomförandeåtgärder som påverkar dataskydd och -säkerhet övervägs.

V. **SLUTSATSER**

45. Datatillsynsmannen har noterat initiativet för att garantera höga kvalitets- och säkerhetsnormer för organ av mänskligt ursprung avsedda för transplantation, vilket kan anses utgöra en del av gemenskapens övergripande strategi för att fastställa gemensamma standarder i syfte att främja gränsöverskridande tillgänglighet till hälso- och sjukvårdstjänster i hela Europa.

46. I förslaget har man redan tagit upp de dataskyddsbehov som uppstår för givare och mottagare av organ, särskilt när det gäller kravet på att deras identiteter ska förbli konfidentiella. Datatillsynsmannen beklagar dock att några av dessa bestämmelser är vaga, tvetydiga eller alltför allmänna och rekommenderar därför ett antal ändringsförslag för att förbättra förslagets dataskyddsrelaterade innehåll.

([1]) Europeiska datatillsynsmannens yttrande av den 2 december 2008 om förslaget till direktiv om tillämpning av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

([2]) Se yttrande 4/2007 från arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, sidan 18, om pseudonymiserade och kodade uppgifter.

47. För det första noterar datatillsynsmannen de befintliga motsättningarna mellan begreppen spårbarhet och anonymitet som används i förslaget. Av denna anledning rekommenderar datatillsynsmannen specifika språkliga ändringar i vissa delar av förslaget (dvs. i skäl 16, artikel 10.2 och i artikel 17) för att undvika oklarheter och uttryckligen återspegla det faktum att uppgifterna inte är anonyma utan bör behandlas enligt stränga sekretess- och säkerhetsbestämmelser.

48. Datatillsynsmannen rekommenderar dessutom en större betoning på behovet av att det antas stränga säkerhetsbestämmelser på nationell nivå. Detta skulle kunna ske genom att man i artikel 16 lägger till ett andra stycke där de grundläggande principerna för att säkerställa säkerhet på medlemsstatsnivå beskrivs och ytterligare specificerar dessa principer som en del av genomförandeåtgärderna i artikel 25.1. De föreslagna säkerhetsprinciperna omfattar följande:

a) Anta en informationssäkerhetspolitik för att säkerställa konfidentialitet, integritet, ansvarighet och tillgänglighet när det gäller givares och mottagares personuppgifter.

b) Fastställa en särskild politik för konfidentialitet och tillgångskontroll samt garantier för datakonfidentialitet för de personer som deltar i behandlingen.

c) Överväga säkerhetsmekanismer för de nationella databaserna på grundval av principen med inbyggda skyddsmekanismer för den personliga integriteten (”privacy by design”).

d) Inrätta förfaranden för att skydda dataskyddsrättigheterna för givare och mottagare, särskilt rätten till tillgång och rättelse samt rätten till information, med särskild uppmärksamhet på fall där givare vill återkalla sitt samtycke eller inte godkänns som givare.

e) Fastställa åtgärder för att garantera integritet för och oavbruten tillgång till uppgifterna.

f) Säkerställa regelbunden uppföljning och oberoende granskning av de införda säkerhetsstrategierna.

49. När det gäller gränsöverskridande utbyte av organ rekommenderar datatillsynsmannen att behovet av en harmoniserad informationssäkerhetspolitik mellan medlemsstaterna ska nämnas i skäl 17 i förslaget. Dessutom bör särskild uppmärksamhet ägnas åt möjligheterna till pseudonymisering när det gäller identifiering av givare och mottagare och åt bibehållande av kompatibilitet med systemet för identifiering av vävnader och celler. Datatillsynsmannen rekommenderar att det görs en särskild hänvisning till detta i artikel 25.1 b i förslaget.

50. När det gäller utbyte av organ med tredjeland rekommenderar datatillsynsmannen att det i artikel 21 eller i det relevanta skäl 15 i förslaget ska nämnas att den behöriga myndigheten ska samråda med den nationella dataskyddsmyndigheten i syfte att utveckla de ramar som krävs för en säker, snabb och effektiv överföring av uppgifter om organ till och från tredjeländer.

51. Slutligen rekommenderar datatillsynsmannen att alla berörda parter, däribland datatillsynsmannen och arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, alltid hörs när genomförandeåtgärder som påverkar dataskydd och –säkerhet övervägs.

Utfärdat i Bryssel den 5 mars 2009

Peter HUSTINX

Europeiska datatillsynsmannen