

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om forslag til Europa-Parlamentets og Rådets direktiv om kvalitets- og sikkerhedsstandarder for menneskelige organer til transplantation

(2009/C 192/02)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger,

som henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, særlig artikel 41,

som henviser til anmodningen om en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001, der blev sendt til EDPS den 8. december 2008,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

Forslag til direktiv om kvalitets- og sikkerhedsstandarder for menneskelige organer til transplantation.

1. Kommissionen vedtog den 8. december 2008 et forslag til Europa-Parlamentets og Rådets direktiv om kvalitets- og sikkerhedsstandarder for menneskelige organer til transplantation (i det følgende benævnt: »forslaget») ⁽¹⁾. Forslaget blev af Kommissionen forelagt EDPS med henblik på en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001.
2. Forslaget har til formål at sikre høje standarder for kvaliteten og sikkerheden af menneskelige organer til transplantation med henblik på at sikre et højt beskyttelsesniveau for menneskers sundhed. Forslaget

— fastsætter de grundlæggende kvalitets- og sikkerhedskrav, som er en nødvendighed i medlemsstaternes transplantationssystemer, og indeholder bestemmelser om oprettelse eller udpegelse af en kompetent national myndighed til at sikre, at disse krav overholdes. Med henblik herpå vil der blive fastlagt nationale kvalitetsprogrammer for udtagning og overførsel af menneskelige organer i alle lande, herunder - bl.a. - et system for indberetning af alvorlige uønskede hændelser og bivirk-

ninger samt en sporingsmekanisme for at sikre, at alle organer kan spores fra donation til modtagelse og vice versa.

— sikrer beskyttelse af donorer og recipienter. Navnlig for så vidt angår levende donorer indeholder forslaget foranstaltninger til evaluering af donors helbred og grundig orientering om risikoen forud for donation, indførelse af registre over levende donorer samt foranstaltninger til at sikre uegennyttig og frivillig donation af organer fra levende donorer.

— fremmer samarbejdet mellem medlemsstaterne og udveksling af organer på tværs af grænserne (også mellem medlemsstater og tredjelande), der standardiserer indsamlingen af relevante oplysninger om organets karakteristika og indfører en ordning for formidling af oplysningerne.

3. Gennemførelsen af den foreslåede organdonations- og transplantationsordning kræver, at de autoriserede organisationer og fagfolk inden for sundhedsvæsenet i de forskellige medlemsstater behandler personoplysninger vedrørende organdonorernes og -modtagernes helbred (helbredsoplysninger). Disse oplysninger anses for at være følsomme og er omfattet af de strengere databeskyttelsesregler i artikel 8 i direktiv 95/46/EF om særlige kategorier af oplysninger.

4. Mere specifikt behandles oplysningerne om donorerne på de udtagningssteder, der varetager donor- og organkarakteriseringen og således definerer, hvorvidt det organ, der overvejes, er egnet til transplantation (en liste over disse oplysninger findes i bilaget til forslaget). Recipienternes (patienternes) oplysninger behandles på de transplantationscentre, hvor operationen faktisk finder sted. Selv om der ikke sker nogen formidling af donoroplysningerne til recipienten (og vice versa), er det et krav til de nationale kompetente myndigheder, at der opretholdes fuld sporbarehed for organet fra donor til recipient (og vice versa), hvilket også bør være muligt i tilfælde af udveksling af organer på tværs af grænserne.

Høring af EDPS

5. EDPS hilser det velkommen, at han høres, og at der henvises til denne høring i forslagets præambel, jf. artikel 28 i forordning (EF) nr. 45/2001.

⁽¹⁾ KOM(2008) 818 endelig udg.

6. Forslaget vil fremskynde organdonations- og transplantationsprocedurer med det endelige mål at øge rådigheden over organer og nedbringe dødeligheden på ventelisten til organer. Det supplerer den nuværende lovgivningsramme med hensyn til anvendelsen af biologisk materiale af menneskelig oprindelse⁽¹⁾. Det kan desuden ses som en del af den overordnede EF-tilgang henimod forskellige typer fælles standarder for udveksling af sundhedsydelser i medlemsstaterne med det grundlæggende mål at fremme den grænseoverskridende tilstedeværelse af disse ydelser i hele Europa⁽²⁾. Som allerede anført i udtalelsen om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser støtter EDPS en sådan fremgangsmåde. Han understreger imidlertid igen, at der er behov for et velkoordineret og ensartet databeskyttelsesperspektiv i de forskellige initiativer vedrørende sundhedsydelser⁽³⁾.
7. Forslaget har allerede taget databeskyttelsesbehovene for både donorer og modtagere af organer i betragtning. Det vigtigste element er kravet om, at donorer og recipienters identiteter skal være fortrolig (betragtning 11 og 16 samt artikel 10 og 17). En række generelle henvisninger til databeskyttelse kan desuden findes i nogle dele af forslaget (betragtning 17, artikel 16, artikel 4, stk. 3, litra a), artikel 15, stk. 3, og artikel 19, stk. 1, litra a), bilaget) samt mere specifikke henvisninger til behovet for at samarbejde med de nationale databeskyttelsesmyndigheder (artikel 18, litra f), og artikel 20, stk. 2).
8. EDPS hilser ovennævnte indhold velkomment. Han vil dog gerne give udtryk for betænkeligheder med hensyn til nogle af bestemmelserne, der ikke er klart defineret eller udarbejdet og derfor fører til tvetydigheder, der potentielt kan berøre medlemsstaternes ensartede gennemførelse af forslaget.
9. Mere specifikt er den nogle gange modstridende anvendelse af begreberne »organernes sporbarhed« og »anonymitet for donorer og modtagere« et spørgsmål, der kræver yderlige kortlægning og præcisering. I forbindelse hermed bør behovet for at vedtage øgede sikkerhedsforanstaltninger til beskyttelse af donorer og recipienters oplysninger på medlemsstatsniveau understreges yderligere for at sikre et styrket databeskyttelsesniveau i de forskellige europæiske lande samt sikre databeskyttelse i udvekslingen af organer på tværs af grænserne (inden for og uden for Europa).
10. Denne udtalelse vil uddybe ovennævnte spørgsmål yderligere med det formål at forbedre det nuværende databeskyttelsesrelaterede indhold i forslaget, både med hensyn til klarhed og sammenhæng.
- ## II. PRÆCISERING AF BEGREBERNE SPORBARHED OG ANONYMITET
- Anvendelsesområdet for direktiv 95/46/EF*
11. I henhold til artikel 2, litra a), i direktiv 95/46/EF om beskyttelse af personoplysninger forstås ved »personoplysninger«: »enhver form for information om en identificeret eller identificerbar fysisk person; ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet«.
12. Biologisk materiale af menneskelig oprindelse som f.eks. organer, væv, celler eller blod, kan defineres som materiale, der kan udtages fra det menneskelige legeme. Det er tvivlsomt, om disse materialer som sådan kan betragtes som personoplysninger. Det er dog ubestridt, at sådanne materialer kan anvendes som *kilder* til personoplysninger om deres indehaver. Udledning af sådanne oplysninger er ofte formålet med behandlingen af biologisk materiale. Og selv uden sådant et formål ledsages biologisk materiale ofte af sådanne udledte oplysninger. I disse situationer finder reglerne i direktiv 95/46/EF anvendelse⁽⁴⁾. Det vil sige, så længe indehaveren af det biologiske materiale er en *identificeret* eller *identificerbar* (fysisk) person.
13. Betragtning 26 i direktiv 95/46/EF forklarer, at for at afgøre, om en person er identificerbar »tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person«. Samme betragtning fastslår endvidere, at bestemmelserne i direktiv 95/46/EF ikke gælder, hvis oplysningerne vedrører en person, der ikke eller ikke længere kan identificeres: sådanne oplysninger anses for at være *anonyme*.
14. I henstilling (2006) 4 har Europarådet behandlet det specifikke spørgsmål om biologisk materiales identificerbarhed, idet det skelner mellem identificerbart og ikke-identificerbart biologisk materiale⁽⁵⁾.
15. Ifølge henstillingen er *identificerbart biologisk materiale* de biologiske materialer, der alene eller i kombination med tilknyttede oplysninger tillader identifikation af de berørte personer enten direkte eller gennem brug af kode⁽⁶⁾. I sidstnævnte tilfælde kan brugeren af de biologiske
-
- ⁽¹⁾ Denne ramme omfatter direktiv 2002/98/EF, 2004/33/EF, 2005/61/EF og 2005/62/EF for blod og blodprodukter og direktiv 2004/23/EF, 2006/17/EF og 2006/86/EF for humane væv og celler.
- ⁽²⁾ Se også forslag til Europa-Parlamentets og Rådets direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser, KOM(2000) 414 endelig.
- ⁽³⁾ Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse af 2. december 2008 om forslaget til direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser.
- ⁽⁴⁾ Artikel 29-Gruppen vedrørende Beskyttelse af Personoplysninger, udtalelse 4/2007 om begrebet personoplysninger, s. 9.
- ⁽⁵⁾ Europarådets henstilling Rec(2006) 4 fra Ministerkomitéen til medlemsstaterne om forskning i biologiske materialer af menneskelig oprindelse.
- ⁽⁶⁾ Artikel 3(i) i Rec(2006) 4.

materialer enten have adgang til koden (*kodet materiale*) eller ikke have adgang til koden, der er under en tredjeparts kontrol (*forbundet anonymiseret materiale*). Artikel 29-Gruppen (i det følgende benævnt WP 29) brugte i sin udtalelse 4/2007 om begrebet personoplysninger begrebet *sporbare pseudonymiserede oplysninger* til at beskrive indirekte identificerbare oplysninger om fysiske personer, der stadig kan bruges til at gå tilbage til og identificere de fysiske personer på foruddefinerede betingelser ⁽¹⁾. *Nøglekodede oplysninger* nævnes som et eksempel på personoplysninger, der er øremærkede med en kode, mens nøglen, der skaber forbindelsen mellem koden og de fælles identifikatorer for de fysiske personer holdes adskilt. Hvis de brugte koder er enestående for hver enkelt specifikke person, er identifikation mulig gennem den nøgle, der anvendes til kodningen.

16. I henstillingen henvises der også til *ikke- identificerbart biologisk materiale* (eller *uforbundne anonymiserede materialer*) som de biologiske materialer, der alene eller i kombination med tilknyttede oplysninger ikke ved rimelige bestræbelser tillader identifikation af de berørte personer ⁽²⁾. Disse vil faktisk blive betragtet som anonyme oplysninger som defineret i direktiv 95/46/EF.
17. Det følger af det foregående, at direktiv 95/46/EF finder anvendelse på indsamling, opbevaring og behandling af identificerbare organer og den efterfølgende udledning af oplysninger fra sådanne organer, så længe det stadig er muligt, med passende hensyn til alle midler, der med rimelighed kan tænkes at blive brugt, at identificere den pågældende person. Som det vil fremgå, vil organers stadige sporbarhed, således som det bliver lagt op til det i det foreslåede direktiv, gøre personerne identificerbare gennem hele processen.

Menneskelige organers sporbarhed versus anonymitet

18. Et biologisk materiales sporbarhed er muligheden for at gå tilbage til indehaveren af materialet og derved identificere ham/hende. Sagt med andre ord kan indehaverne af biologisk materiale, når det er muligt at spore dem enten direkte eller indirekte, betragtes som identificerbare og vice versa. Begreberne »sporbarhed« og »identificerbar« er derfor i princippet stærkt forbundet til hinanden. Derimod kan sporbarhed og oplysningers anonymitet ikke forekomme samtidig. De er hinandens modsætninger. Hvis visse oplysninger virkelig er anonyme, er det ikke muligt at identificere og spore personerne.
19. I forbindelse med det foreliggende forslag er sporbarhed et obligatorisk krav, der skal fastsættes inden for rammerne af medlemsstaternes nationale kvalitetsprogrammer på dobbelt vis, dvs. både for donorer og for modtagere. Dette betyder, at selv om oplysninger om donorer og

modtagere holdes fortrolige, er oplysninger vedrørende organer identificerbare. Dette indgår også i forslaget definition af sporbarhed i artikel 3: »sporbarhed«: en kompetent myndigheds mulighed for at lokalisere og identificere organet i et hvilket som helst led i kæden fra donation til transplantation eller anden disponering, idet myndigheden under visse omstændigheder, som angivet i dette direktiv, er bemyndiget til at identificere donoren og udtagningsstedet, identificere recipienten/recipienterne på transplantationscentret/centrene, lokalisere og identificere alle relevante ikke-personlige oplysninger om produkter og materialer, der kommer i kontakt med det pågældende organ.

20. Desuden hedder det i artikel 10, stk. 1, i forslaget om sporbarhed, at »Medlemsstaterne sikrer, med henblik på at beskytte donorer og recipienters sundhed, at alle organer, der udtages og allokeres på deres område, kan spores fra donor til recipient og vice versa«. I artikel 10, stk. 3, hedder det, at »Medlemsstaterne sikrer, at: a) den kompetente myndighed og andre aktører i kæden fra donation til transplantation eller anden disponering opbevarer de oplysninger, der er nødvendige for at sikre sporbarhed i alle led i kæden fra donation til transplantation eller anden disponering i overensstemmelse med de nationale kvalitetsprogrammer, b) oplysninger, der er nødvendige for den fulde sporbarhed, opbevares i mindst 30 år efter donationen. Disse oplysninger kan opbevares i elektronisk form«.
21. Selv om sporbarhedsprocessen er underlagt gennemførelsesforanstaltninger (se artikel 25 i forslaget) synes en indirekte identifikationsordning for donorer og recipienter den mest sandsynlige løsning, idet den følger eller i det mindste er interoperabel med direktiv 2004/23/EF ⁽³⁾ om væv og celler og den europæiske identifikationskode, der er fastlagt deri ⁽⁴⁾. I et sådant tilfælde vedrører behandlingen i

⁽³⁾ Eftersom organdonorer meget ofte er vævsdonorer, er der behov for også at spore og rapportere enhver uventet bivirkning i vævsbevareningssystemet, og derfor er der krav om interoperabilitet med den indirekte identifikationsmetode, der bruges i dette system. Se også: Europa-Parlamentets og Rådets direktiv 2004/23/EF af 31. marts 2004 om fastsættelse af standarder for kvaliteten og sikkerheden ved donation, udtagning, testning, behandling, præservering, opbevaring og distribution af humane væv og celler, EUT L 102/48 af 7.4.2004 og Kommissionens direktiv 2006/86/EF af 24. oktober 2006 om gennemførelse af Europa-Parlamentets og Rådets direktiv 2004/23/EF for så vidt angår krav til sporbarhed, indberetning af alvorlige bivirkninger og uønskede hændelser og visse tekniske krav til kodning, behandling, præservering, opbevaring og distribution af humane væv og celler, EUT L 294/32, 25.10.2006.

⁽⁴⁾ Denne kode indeholder et enkelt identifikationsnummer for hver donation, der sammen med vævscentret og produktidentifikationen kan spore tilbage til donorerne og recipienterne. I henhold til artikel 10 i direktiv 2006/86/EF tildeles alt doneret materiale »på vævscentret en fælles europæisk identifikationskode med henblik på at sikre, at donoren kan identificeres, og at alt doneret materiale kan spores, og for at oplyse om vævs og cellers vigtigste karakteristika og egenskaber«. Som beskrevet i bilag VII til dette direktiv har koden to dele: a) donationsidentifikation, herunder et enkelt id-nummer for donationen og identifikationen for vævscentret og b) produktidentifikation, herunder produktkode, sublotnummer og udløbsdato.

⁽¹⁾ Artikel 29-Gruppen vedrørende Beskyttelse af Personoplysninger, udtalelse 4/2007, s. 18.

⁽²⁾ Artikel 3(ii) i Rec(2006) 4.

forbindelse med donorer og recipienter i forbindelse med forslaget forbundne anonymiserede biologiske materialer eller i databeskyttelsesterminologi sporbare pseudonymiserede data (jf. ovenfor i punkt 15), for hvilke bestemmelserne i direktiv 95/46/EF finder anvendelse.

22. Det noteres imidlertid, at forslaget trods de klare krav om sporbarhed og identificerbarhed i nogle dele bruger udtrykket »anonymitet« eller »anonyme oplysninger« til at henvise til donorer og recipienters oplysninger. Som det fremgår af de foregående punkter, er dette selvmodsigende og yderst forvirrende ⁽¹⁾.

23. Mere specifikt hedder det i forslagens artikel 10, stk. 2, der omhandler behovet for et donoridentifikationssystem, at »Medlemsstaterne sørger for, at der indføres et donoridentifikationssystem, som gør det muligt at identificere enhver donation og ethvert organ i tilknytning hertil. Medlemsstaterne påser, at dette donoridentifikationssystem udformes og udvælges i overensstemmelse med målsætningen om ikke eller i mindst muligt omfang at indsamle, behandle eller anvende personoplysninger. Der skal især gøres brug af mulighederne for pseudonymisering eller anonymisering af privatpersoner ⁽²⁾«. EDPS har den opfattelse, at de understregede udtryk i dette stykke er i modstrid med begrebet sporbarhed, eftersom der ikke er mulighed for at have sporbare og identificerbare oplysninger, når donorer og recipienter gøres anonyme. Det er desuden bemærkelsesværdigt, at dette stykke henviser til donoridentifikation, mens recipientidentifikationen (som også er en del af processen) ikke nævnes overhovedet.

24. Førnævnte selvmodsigelse er endnu mere tydelig i artikel 17 om anonymisering af donorer og recipienter, hvori det hedder, at: »Medlemsstaterne træffer alle fornødne foranstaltninger for at sikre, at alle personoplysninger om donorer og recipienter, der behandles inden for rammerne af dette direktiv, anonymiseres, så hverken donorer eller recipienter kan identificeres«. Denne artikel er fuldstændig i konflikt med forslagens artikler om sporbarhed.

Fortrolighed i stedet for anonymitet

25. EDPS forstår, at ordet anonymitet faktisk bruges for at understrege behovet for øget fortrolighed ⁽³⁾ i forbindelse med donor- og recipientoplysningerne, hvilket betyder, at

oplysningerne kun er tilgængelige for dem, der har ret til adgang. EDPS antager, at anonymisering bruges mere specifikt for at angive en indirekte identifikationsordning for donorer og recipienter ⁽⁴⁾, hvilket også kan udledes af den måde, som ordet bruges på i direktiv 2004/23/EF om væv og celler. Som tidligere anført er anonymitet imidlertid ikke det korrekte udtryk at anvende.

26. Et eksempel på, hvordan både databeskyttelse og sporbarhed kan behandles i en transplantationsproces, kan findes i Europarådets tillægsprotokol til konventionen om menneskerettigheder og biomedicin ⁽⁵⁾. Der anvendes begrebet fortrolighed i stedet for anonymitet. Mere specifikt hedder det i artikel 23, stk. 1, i protokollen, at alle personoplysninger vedrørende den person, fra hvem organer eller væv er blevet fjernet, og dem, der vedrører recipienten, skal anses for at være fortrolige. *Sådanne oplysninger må kun indsamles, behandles og formidles i henhold til reglerne om tavshedspligt og beskyttelse af personoplysninger.* Artikel 23, stk. 2, fortsætter således: »bestemmelserne i stk. 1 skal ikke opfattes som en foregribelse af de bestemmelser, der med tilstrækkelige garantier muliggør indsamling, behandling og formidling af nødvendige oplysninger om den person, fra hvem organer eller væv er blevet fjernet, eller recipienten/recipienterne af organer og væv for så vidt dette er påkrævet af medicinske hensyn, herunder sporbarhed, som omhandlet i artikel 3 i denne protokol«.

27. På baggrund af det foregående anbefaler EDPS at ændre sprogbrugen i visse dele af forslaget for at undgå uklarheder og eksplicit afspejle det faktum, at oplysningerne ikke er anonyme, men bør behandles efter strenge fortroligheds- og sikkerhedsregler. Mere specifikt anbefaler EDPS følgende ændringer:

⁽⁴⁾ Ordet »anonymisering« bruges afhængig af konteksten, hvor det nogle gange anvendes om indirekte identificerbare oplysninger som i forbindelse med statistik. Dette er imidlertid ikke korrekt set fra et databeskyttelsessynspunkt, som den tilsynsførende forklarede det i sin udtalelse om forslag til Europa-Parlamentets og Rådets forordning (EF) om fællesskabsstatistikker over folkesundhed og arbejdsmiljø (KOM(2007) 46 endelig) og forslaget til Europa-Parlamentets og Rådets forordning om europæiske statistikker (KOM(2007) 625 endelig).

⁽⁵⁾ Europarådet, tillægsprotokol til konventionen om menneskerettigheder og biomedicin vedrørende transplantation af organer og væv af menneskelig oprindelse, Strasbourg, 24.1.2002, se: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=186&CM=8&DF=2/13/2009&CL=ENG> for ratifikationsoversigt. Se også: Europarådets konvention om beskyttelse af menneskerettigheder og menneskelig værdighed i forbindelse med anvendelse af biologi og lægevidenskab: konvention om menneskerettigheder og biomedicin, Oviedo, 4.4.1997, se: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=2/13/2009&CL=ENG> for ratifikationsoversigt.

⁽¹⁾ Den tilsynsførende fremsatte også denne betragtning i sine bemærkninger af 19.9.2006 om offentlig høring om fremtidige EU-foranstaltninger på området organdonation og -transplantation.

⁽²⁾ Egen understregning.

⁽³⁾ Sikre, at oplysningerne kun er tilgængelige for dem, der har ret til adgang (ISO-definition, kilde: <http://www.wikipedia.org>).

— Betragtning 16, sidste punktum: »I tråd med charteret og for i det nødvendige omfang at tage hensyn til konventionen om menneskerettigheder og biomedicin bør programmer for organtransplantation bygge på principperne om frivillig og vederlagsfri donation, donors altruisme og solidaritet mellem donor og recipient, samtidig med at der gælder strenge fortrolighedsregler, og at der foreligger sikkerhedsforanstaltninger til beskyttelse af donorer og recipienters personoplysninger«.

— Artikel 10, stk. 2: »Medlemsstaterne sørger for, at der indføres et donor- og recipientidentifikationssystem, som gør det muligt at identificere enhver donation og ethvert organ i tilknytning hertil. Medlemsstaterne påser, at dette donor- og recipientidentifikationssystem udformes og udvælges i overensstemmelse med målsætningen om ikke eller i mindst muligt omfang at indsamle, behandle eller anvende personoplysninger og gøre særlig brug af pseudonymiseringsmetoder, samt at de nødvendige tekniske og organisatoriske foranstaltninger foreligger af hensyn til sikkerheden for disse oplysninger«.

— Artikel 17 som sådan bør udgå og dens indhold (med hensyn til fortrolighedsbehov) indgå i et nyt stykke i artikel 16 om beskyttelse af personoplysninger, fortrolighed og behandlingssikkerhed (jf. punkt 36 nedenfor).

28. Som det vil blive drøftet i de følgende dele af denne udtalelse, foreslår EDPS desuden yderligere at skitsere behovet for styrket beskyttelse af donorer og recipienters oplysninger gennem anvendelsen af strenge sikkerhedsforanstaltninger på både nationalt og tværnationalt plan.

III. UNDERSTREGNING AF NATIONALE DATASIKKERHEDSFORANSTALTNINGER

Grundlæggende sikkerhedsbehov og krav

29. Som det fremgår af forslaget, finder behandlingen af donorer og recipienters personoplysninger primært sted på nationalt plan, dvs. i medlemsstaternes udtagings- og transplantationscentre. Det er også på dette plan, at der bliver ført register over levende donorer. Selv om sporingsmekanismen endnu ikke er blevet defineret, kan det forventes, at enhver kodifikationsaktivitet også vil ske på nationalt plan, selv i tilfælde af, at der anvendes et europæisk kodningssystem, eftersom identifikationen af donorerne og recipienterne kun er mulig gennem de nationale kompetente myndigheder.
30. Det er derfor af den største betydning, at der gennemføres en informationssikkerhedspolitik, der bygger på strenge og

sunde sikkerhedsforanstaltninger i de relevante nationale tjenester, navnlig for at opfylde fortrolighedskravene for donorer og recipienter i forslaget samt for at sikre integritet ⁽¹⁾, klar ansvarsfordeling ⁽²⁾, og tilstedeværelse ⁽³⁾ i forbindelse med disse oplysninger. I den forbindelse bør informationssikkerhedspolitikken dække elementer af fysisk og logisk sikkerhed, der bl.a. fokuserer på kontrol med indlæsning af oplysninger, registrering, overførsel og formidling datamedier og kontrol med lagring.

31. Med hensyn til fortrolighed kan recipienternes medicinske oplysninger ⁽⁴⁾ samt oplysninger, der bruges til donorerne karakterisering og opfølgning (også i forhold til »alternative potentielle donorer« ⁽⁵⁾) afsløre følsomme personoplysninger om dem, der også kan berøre deres sociale, faglige og/eller personlige liv. Beskyttelsen af donorerne identifikationsdata er af yderligere betydning, hvor levende donorer eller personer, der har givet deres samtykke til at donere et eller flere af deres organer efter deres død, kunne blive ofre for ulovlig handel med menneskelige organer og væv, såfremt disse oplysninger bliver afsløret. Integritet i oplysningerne vedrørende organer er også meget vigtig, eftersom bare en enkelt fejl i de overførte oplysninger kan blive livstruende for recipienten. Det samme gælder for nøjagtigheden af donorerne sundhedsoplysninger inden transplantationen, eftersom disse oplysninger bruges til at bestemme, om organet er egnet. Med hensyn til klar ansvarsfordeling bør der, siden så mange forskellige organisationer er involveret i den samlede donations- og transplantationsordning, være en måde, hvorpå alle involverede enheder er bevidste om og kan tage ansvar for deres handlinger, f.eks. i tilfælde, hvor donorerne identifikationsoplysninger afsløres over for ikke-autoriserede personer, eller de medicinske oplysninger vedrørende organet ikke er præcise. Endelig bør disse oplysninger, eftersom hele systemet bygger på overførsel af oplysninger vedrørende organer og sporingsmekanismen fra donor til recipient, stå til rådighed for de beføjede personer, når

⁽¹⁾ Sikre, at oplysningerne er »hele« eller fuldstændige, vilkårene, på hvilke oplysninger er identisk opbevaret under en operation (som f.eks. overførsel, opbevaring eller genfindning), bevarelse af oplysninger med henblik på deres anvendelsesformål eller, i forbindelse med specificerede operationer, den på forhånd givne forventning om oplysningernes pålidelighed. Enkelt sagt er dataintegritet en forsikring om, at oplysningerne er kohærente og korrekte (kilde: <http://www.wikipedia.org>). sikre, at oplysninger kun kan blive tilgængelige for eller ændret af dem, der har bemyndigelse dertil (kilde: <http://searchdatacenter.techtarget.com>).

⁽²⁾ Forpligtelse til at stå til ansvar for sine handlinger; uafviselighed: sikre, at oplysningerne er blevet sendt og modtaget af de parter, der hævder at have sendt og modtaget dem: princippet om at sikre, at en part i en tvist ikke kan afvise eller benægte en erklæringens gyldighed (kilde: <http://www.wikipedia.org>).

⁽³⁾ Det omfang, hvori der kan være øjeblikkelig adgang til oplysningerne (kilde: <http://www.wikipedia.org>).

⁽⁴⁾ Det skal noteres, at det blotte faktum, at et organ transplanteres til en recipient, udgør følsomme personoplysninger om denne persons sundhed.

⁽⁵⁾ Potentielle donorer, der ikke er de ideelle donorkandidater, men kan overvejes under visse omstændigheder, f.eks. til ældre recipienter. Se også: Arbejdsdokument fra Kommissionens tjenestegrene — Ledsagedokument til forslag til Europa-Parlamentets og Rådets direktiv om kvalitets- og sikkerhedsstandarder for menneskelige organer til transplantation og Meddelelse fra Kommissionen — Handlingsplan for organdonation og -transplantation (2009-2015): styrket samarbejde mellem medlemslandene, konsekvensanalyse af 8.12.2008.

de er nødvendige, uden forsinkelse (ellers vil manglende oplysninger kompromittere det velfungerende systems resultater).

32. I den forbindelse bør der være passende *godkendelsesordninger*, der følger specifikke *adgangskontrolpolitikker*, både for de nationale databaser og i tilfælde af udveksling af organer på tværs af grænserne. Disse politikker bør først defineres på det organisatoriske plan, navnlig med hensyn til identifikationsprocedurerne for donorerne og recipienterne (f.eks. hvem der har adgang til hvilke oplysninger og under hvilke omstændigheder). På denne måde vil der blive fastsat *adgangsret* sammen med *adgangsscenarier*, hvor denne ret kan udøves (f.eks. omstændigheder og procedure for udtagningsorganisationens afsløring af oplysninger over for den kompetente myndighed, visse — om nogen — tilfælde, hvor donorens identitet skal afsløres over for recipienten og procedurerne for at gøre det osv.). For at politikkerne kan være effektive, bør de involverede personer være bundet af specifikke *fortrolighedsregler*.

33. Når disse politikker er fastlagt, kan de blive gennemført på teknisk plan, dvs. med hensyn til kontrol af brugeradgang til systemer og applikationer i overensstemmelse med de foruddefinerede adgangsbemyndigelser. Velaftestede teknologier som f.eks. *kryptering* og *digitale certifikater* ⁽¹⁾ (f.eks. baseret på *offentlige nøgleinfrastrukturordninger* ⁽²⁾) kan bruges hertil. *Rollebaserede godkendelsesmekanismer* kan også anvendes for at begrænse brugeradgangsretten, der bygger på deres rolle (f.eks. bør kun læger være i stand til at ændre recipienternes og donorerne medicinske oplysninger i de nationale databaser).

34. Adgangskontrol skal suppleres med muligheder for *registrering* af brugeraktioner (f.eks. læse- og skriveadgang til medicinske oplysninger), navnlig når der bruges elektroniske systemer. Der bør også være fysiske og logiske sikkerhedsforanstaltninger for at sikre, at donor- og organdatabaserne er *fuldt operationelle* som et centralt element i det foreslåede donations- og transplantationssystem. Disponibilitet af oplysninger bør betragtes som grundstenen i systemet. I den forbindelse bør informationssikkerhedspolitikken bygge på en *sund risikoanalyse* og *-vurdering* og også omfatte elementer som hændelser og kontinuitetsstyring. Alle disse elementer bør bevares og forbedres gennem regelmæssige kontrol- og revisionsprocesser. *Uafhængige revisioner* kan også øge effektiviteten og forbedringen af systemet med særlig opmærksomhed på pseudonymisering, sporbarhed og dataoverførselspraksis.

⁽¹⁾ Den elektroniske ækvivalent til et id-kort, der bekræfter afsenderen af en digital signatur (kilde: http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html).

⁽²⁾ En offentlig nøgleinfrastruktur (PKI) er et sæt maskinel, programmel, mennesker, politikker og procedurer, der er nødvendige for at skabe, forvalte, opbevare, formidle og inddrage digitale certifikater (kilde: <http://www.wikipedia.org>).

35. EDPS ser gerne, at der lægges mere vægt på behovet for sådanne foranstaltninger i forbindelse med det foreslåede direktiv.

Fremme af forslagens sikkerhedsbestemmelser

36. I artikel 16 i forslaget om beskyttelse af personoplysninger, fortrolighed og behandlingssikkerhed hedder det, at »Medlemsstaterne sikrer, at den grundlæggende ret til beskyttelse af personoplysninger håndhæves til punkt og prikke i forbindelse med alle organtransplantationsaktiviteter i overensstemmelse med EF-retsforordningerne om beskyttelse af personoplysninger, herunder direktiv 95/46/EF, særlig artikel 8, stk. 3, artikel 16, artikel 17 og artikel 28, stk. 2, i samme direktiv«. EDPS anbefaler, at der tilføjes et *stk. 2* i denne artikel, der beskriver de grundlæggende principper for at garantere sikkerheden på medlemsstatsniveau, herunder som et minimum en henvisning til følgende punkter:

— Der bør være en informationssikkerhedspolitik, der gennemfører tekniske og organisatoriske foranstaltninger til at sikre fortrolighed, integritet, klar ansvarsfordeling og disponibilitet i forbindelse med donorer og recipienters personoplysninger.

— En specifik fortroligheds- og adgangskontrolpolitik bør defineres og anvendes i alle medlemsstater, og den bør specificere adgangsbemyndigelser, roller og ansvar for alle involverede parter (donor, udtagningsorganisation, transplantationscenter, recipient, national kompetent myndighed, kompetent myndighed på tværs af grænserne) gennem hele sporbarhedskæden. Der bør være specifikke garantier for fortrolig behandling af oplysningerne for de personer, der er involveret i behandlingen, navnlig hvis disse personer ikke er bundet af forpligtelsen til tavshedspligt inden for sundhedssektoren (f.eks. fortrolighedsadfærdskodeks og foranstaltninger, der er fokuseret på information).

— Behovet for at se på sikkerhedsmekanismer (som f.eks. kryptering og digitale certifikater) i de nationale databaser bør skitseres. Navnlig med hensyn til donorregister bør princippet om »privacy by design« (indbygget databeskyttelse) anvendes for at inddrage alle nødvendige sikkerhedskrav i de indledende gennemførelsesfaser af en sådan udvikling.

— Der bør også fastsættes procedurer for at beskytte donorer og recipienters databeskyttelsesrettigheder, navnlig retten til adgang og berigtigelse samt retten til information. Der bør også ses med særlig opmærksomhed på tilfælde med donorer, der ønsker at trække deres samtykke tilbage eller ikke bliver accepteret (efter donor- og organkarakteriseringen) som donorer. I dette tilfælde bør der defineres en specifik procedure og tidsfrist for opbevaringen af deres oplysninger.

- Informationssikkerhedspolitikken bør også omfatte foranstaltninger til sikring af oplysningernes integritet og uafbrudt disponibilitet. Informationssikkerhedsrisikovurderingens rolle bør suppleres med antagelser af elementer vedrørende hændelser og kontinuitetsstyring.
- Informationssikkerhedspolitikkerne bør underlægges regelmæssig kontrol og revision, herunder uafhængige revisioner.

37. EDPS anbefaler, at ovennævnte elementer indsættes i artikel 16 og derpå yderligere specificeres som en del af gennemførelsesforanstaltningerne i artikel 25, navnlig stk. 1, litra a), b) og c).

IV. SIKKERHEDSFORANSTALTNINGER VEDRØRENDE UDVEKSLING AF ORGANER PÅ TVÆRS AF GRÆNSERNE

Sikkerhedsharmonisering i medlemsstaterne

38. Udvekslingen af organer på tværs af grænserne vil i praksis altid involvere behandling af personoplysninger, eftersom organerne, selv om de er kodede, forbliver (indirekte) identificerbare gennem de nationale kompetente myndigheder.
39. EDPS har allerede udtalt sig om sikkerhedsbehovet for beskyttelse af personoplysninger i forbindelse med grænseoverskridende sundhedsydelser i Europa og bl.a. understreget behovet for at harmonisere informationssikkerhedspolitikker i medlemsstaterne for at opnå et sundt databeskyttelsesniveau⁽¹⁾. Han anbefaler, at dette element også nævnes i det foreliggende forslag og mere specifikt i betragtning (17), hvor bestemmelserne i direktiv 95/46/EF om behandlingssikkerhed er nævnt.

Oprettelse af sporbarhedssystemet

40. I dette specifikke tilfælde er et betydeligt parameter for grænseoverskridende datasikkerhed den sporingsmekanisme, der skal oprettes. Med henblik herpå skal der ud over de sikkerhedsforanstaltninger, der anvendes på medlemsstatsniveau, lægges særlig vægt på de pseudonymiseringsmuligheder, der anvendes til identifikation af donorer og recipienter (f.eks. kodifikationstype, mulighed for dobbelt kodifikation osv.) og til at opretholde interoperabilitet med vævs- og celleidentifikationssystemet.
41. EDPS anbefaler, at der indsættes en specifik henvisning til dette punkt i artikel 25 i det foreslåede direktiv om gennemførelsesforanstaltningerne, der ændrer stk. 1, litra b), således: »procedurer, der har til formål at sikre fuld sporbarhed for organer, herunder mærkningskrav, idet donorer og recipienters fortrolighed beskyttes under hele sporbarhedsprocessen, og der opretholdes interoperabilitet med vævs- og celleidentifikationssystemet.«

Udveksling af organer med tredjelande

42. Sikkerhedsbehovene er endnu mere vigtige, når der udveksles oplysninger med tredjelande, hvor et passende databeskyttelsesniveau ikke altid kan garanteres. En specifik ordning for videregivelse af personoplysninger til tredjelande er fastsat i artikel 25 og 26 i direktiv 95/46/EF. EDPS er klar over, at databeskyttelseskrav ikke skal hindre hurtig og effektiv overførsel af organer, hvilket er en nødvendighed i organdonationssystemet og ofte kan være et spørgsmål om liv eller død. Mulighederne for at tillade overførsler trods manglen på et passende databeskyttelsesniveau generelt i tredjelandet bør derfor undersøges. Der skal derved tages hensyn til, at risici på grund af den indirekte art af personidentifikation på tværnationalt plan sammen med det forhold, at de nationale kompetente myndigheder fører den overordnede kontrol med systemet, højst sandsynligt er lavere end risici på nationalt plan⁽²⁾.

43. Med henblik herpå har EDPS den opfattelse, at den kompetente myndighed, der er ansvarlig for tilladelsen til sådanne overførsler, hører den nationale databeskyttelsesmyndighed for i lyset af de mulige undtagelser, der er omhandlet i artikel 26 i direktiv 95/46/EF, at udarbejde den nødvendige ramme for sikker, men også hurtig og effektiv videregivelse af organoplysninger til og fra tredjelande. EDPS anbefaler, at der indsættes en specifik henvisning til dette punkt i artikel 21 om udveksling af organer med tredjelande eller i den relevante betragtning (15).

Gennemførelsesforanstaltninger

44. Som en afsluttende bemærkning tilskynder EDPS lovgiveren til at sikre, at alle relevante aktører bliver hørt, herunder EDPS og Artikel 29-Gruppen med hensyn til artikel 25 i alle tilfælde, hvor gennemførelsesforanstaltninger vedrørende databeskyttelse og -sikkerhed bliver overvejet.

V. KONKLUSIONER

45. EDPS har noteret sig initiativet til at sikre høje kvalitets- og sikkerhedsstandarder for menneskelige organer til transplantation, der kan ses som en del af den overordnede EF-tilgang henimod fælles standarder til fremme af grænseoverskridende tilstedeværelse af sundhedsydelser i hele Europa.
46. Forslaget har allerede overvejet databeskyttelsesbehovene både for donorer og modtagere af organer, navnlig med hensyn til kravet om at holde deres identiteter fortrolig. EDPS beklager imidlertid, at nogle af disse bestemmelser er vage, tvetydige eller generelle, og han anbefaler derfor en række ændringer til at forbedre forslagens databeskyttelsesrelaterede indhold.

⁽¹⁾ Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse af 2. december 2008 om forslaget til direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser.

⁽²⁾ Se Artikel 29-Gruppen vedrørende Beskyttelse af Personoplysningers udtalelse 4/2007, s. 18, om pseudonymiserede og nøglekodede oplysninger.

47. Som et første punkt noterer EDPS sig den nuværende modsætning mellem begreberne sporbarhed og anonymitet, der bruges i forslaget. I den forbindelse anbefaler han specifikt at ændre sprogbrugen i visse dele af forslaget (nemlig i betragtning (16, artikel 10, stk. 2, og artikel 17) for at undgå uklarheder og eksplicit afspejle det faktum, at oplysningerne ikke er anonyme, men bør behandles efter strenge fortroligheds- og sikkerhedsregler.
48. Derudover anbefaler han at lægge mere vægt på behovet for at vedtage strenge sikkerhedsforanstaltninger på nationalt plan. Dette kan gøres ved at tilføje et stk. 2 i artikel 16, der beskriver de grundlæggende principper for at garantere sikkerhed på medlemsstatsniveau og yderligere specificere disse principper som del af gennemførelsesforanstaltningerne i artikel 25, stk. 1. De foreslåede sikkerhedsprincipper omfatter:
- a) vedtagelse af en informationssikkerhedspolitik til at sikre fortrolighed, integritet, klar ansvarsfordeling og disponibilitet i forbindelse med donorer og recipienters personoplysninger
 - b) definition af en specifik fortroligheds- og adgangskontrolpolitik sammen med garantier for fortrolig behandling af oplysningerne for de personer, der er involveret i behandlingen
 - c) sikkerhedsmekanismer i de nationale databaser på grundlag af princippet om »privacy by design« (indbygget databeskyttelse)
 - d) fastsættelse af procedurer for at beskytte donorer og recipienters databeskyttelsesrettigheder, navnlig retten til adgang og berigtigelse samt retten til information, med særlig vægt på donorer, der ønsker at trække deres samtykke tilbage eller ikke bliver accepteret som donorer.
- e) foranstaltninger til at garantere integritet og uafbrudt disponibilitet
 - f) sikring af regelmæssig kontrol og uafhængige revisioner af gældende sikkerhedspolitikker.
49. Med hensyn til den grænseoverskridende udveksling af organer anbefaler EDPS, at behovet for at harmonisere informationssikkerhedspolitikkerne i medlemsstaterne nævnes i betragtning (17 i forslaget. Derudover skal der lægges særlig vægt på de pseudonymiseringsmuligheder, der anvendes til identifikation af donorer og recipienter og til at opretholde interoperabilitet med vævs- og celleidentifikationssystemet. EDPS anbefaler, at der indsættes en specifik henvisning til dette punkt i artikel 25, stk. 1, litra b), i forslaget.
50. Vedrørende udveksling af organer med tredjelande anbefaler EDPS i artikel 21 eller den relevante betragtning (15) i forslaget at nævne, at den kompetente myndighed hører den nationale databeskyttelsesmyndighed for at udarbejde den nødvendige ramme for sikker, men også hurtig og effektiv videregivelse af organoplysninger til og fra tredjelande.
51. Afslutningsvis anbefaler EDPS, at alle relevante aktører bliver hørt, herunder EDPS og Artikel 29-Gruppen i alle tilfælde, hvor gennemførelsesforanstaltninger vedrørende databeskyttelse og -sikkerhed bliver overvejet.

Udfærdiget i Bruxelles, den 5. marts 2009

Peter HUSTINX

Europæisk Tilsynsførende for Databeskyttelse