

Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Qualitäts- und Sicherheitsstandards für zur Transplantation bestimmte menschliche Organe

(2009/C 192/02)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41,

gestützt auf das dem Europäischen Datenschutzbeauftragten am 8. Dezember 2008 übermittelte Ersuchen um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

Vorschlag für eine Richtlinie über Qualitäts- und Sicherheitsstandards für zur Transplantation bestimmte menschliche Organe

1. Die Kommission hat am 8. Dezember 2008 einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Qualitäts- und Sicherheitsstandards für zur Transplantation bestimmte menschliche Organe (nachstehend „der Vorschlag“) angenommen. ⁽¹⁾ Dieser Vorschlag wurde dem Europäischen Datenschutzbeauftragten (EDSB) von der Kommission gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 zwecks Konsultation übermittelt.
2. Der Vorschlag stellt darauf ab, hohe Qualitäts- und Sicherheitsstandards für zur Transplantation bestimmte menschliche Organe und somit ein hohes Schutzniveau für die menschliche Gesundheit zu gewährleisten. Der Vorschlag
 - enthält die in den Transplantationssystemen der Mitgliedstaaten notwendigen grundlegenden Qualitäts- und Sicherheitsanforderungen und sieht die Schaffung oder Benennung einer zuständigen nationalen Behörde vor, die die Einhaltung dieser Anforderungen sicherstellen soll. Zu diesem Zweck werden in allen Ländern nationale Qualitätsprogramme für die Beschaffung

und den Transfer menschlicher Organe erarbeitet, die u. a. ein System zur *Meldung schwerwiegender Zwischenfälle und unerwünschter Reaktionen* sowie einen *Rückverfolgungsmechanismus* umfassen, um sicherzustellen, dass alle Organe vom Spender bis zum Empfänger und zurück verfolgt werden können;

- sorgt für den Schutz von Spendern und Empfängern. Speziell im Hinblick auf Lebendspender sind in dem Vorschlag Maßnahmen für eine Beurteilung der Gesundheit der Spender und die umfassende Unterrichtung über die Risiken einer Spende, die Einrichtung von *Lebendspenderregistern* sowie Maßnahmen zur Gewährleistung von uneigennützigem und freiwilligen Organ spenden durch Lebendspender vorgesehen;
- erleichtert die Zusammenarbeit zwischen Mitgliedstaaten und den *grenzüberschreitenden Organaustausch* (auch zwischen Mitgliedstaaten und Drittländern), indem die Erhebungen der sachdienlichen Informationen über die Merkmale eines Organs standardisiert werden und ein Mechanismus für die Informationsübermittlung eingerichtet wird.

3. Die Durchführung des vorgeschlagenen Organspende- und Transplantationsprogramms erfordert die Verarbeitung von personenbezogenen Daten über die Gesundheit („Gesundheitsdaten“) der Organspender und -empfänger durch befugte Einrichtungen und Fachkräfte des Gesundheitswesens der verschiedenen Mitgliedstaaten. Diese Daten gelten als sensibel und fallen unter die strengeren Datenschutzvorschriften nach Artikel 8 der Richtlinie 95/46/EG betreffend besondere Kategorien personenbezogener Daten.
4. Konkret werden die Daten der Organspender in den Beschaffungsorganisationen verarbeitet, die die Spender- und Organcharakterisierung vornehmen und somit bestimmen, ob ein geprüftes Organ zur Transplantation geeignet ist (eine Aufstellung dieser Daten ist im Anhang zu dem Vorschlag enthalten). Die Daten des Empfängers (Patienten) werden in den Transplantationszentren verarbeitet, wo die Operation tatsächlich stattfindet. Wenngleich keine Übermittlung der Daten des Spenders an den Empfänger (und umgekehrt) erfolgt, müssen die zuständigen nationalen Behörden die lückenlose Rückverfolgbarkeit der Organe vom Spender zum Empfänger (und zurück) gewährleisten, die auch im Falle eines grenzüberschreitenden Organaustauschs möglich sein sollte.

Konsultation des EDSB

5. Der EDSB begrüßt, dass er im Einklang mit Artikel 28 der Verordnung (EG) Nr. 45/2001 konsultiert wird und dass im Einleitungsteil des Vorschlags auf diese Konsultation hingewiesen wird.

⁽¹⁾ KOM(2008) 818 endgültig.

6. Der Vorschlag wird die Verfahren für die Organspende und -transplantation voranbringen — mit dem Endziel, die Verfügbarkeit von Organen zu verbessern und die Sterblichkeit unter Patienten auf Organwartelisten zu verringern. Er ergänzt den bestehenden Rechtsrahmen für die Verwendung von biologischem Material menschlichen Ursprungs ⁽¹⁾. Außerdem kann er als Teil des Gesamtkonzepts der EG für die Festlegung von verschiedenen Arten gemeinsamer Standards für die Erbringung von Gesundheitsdienstleistungen in den Mitgliedstaaten betrachtet werden, das in erster Linie darauf abstellt, die grenzüberschreitende Verfügbarkeit dieser Dienstleistungen in ganz Europa zu gewährleisten ⁽²⁾. Wie er bereits in seiner Stellungnahme zu den Patientenrechten in der grenzüberschreitenden Gesundheitsversorgung erklärt hat, unterstützt der EDSB ein solches Konzept. Er betont jedoch erneut, dass es eines gut koordinierten und einheitlichen Datenschutzkonzepts in den verschiedenen Initiativen im Bereich des Gesundheitswesens ⁽³⁾ bedarf.
7. In dem Vorschlag wurden die Datenschutzbedürfnisse von Organspendern und -empfängern bereits berücksichtigt. Der wichtigste Aspekt besteht in dem Erfordernis, die Anonymität von Gebern und Empfängern zu wahren (Erwägungsgründe 11 und 16, Artikel 10 und 17). Darüber hinaus enthalten einige Teile des Vorschlags allgemeine Verweise auf den Datenschutz (Erwägungsgrund 17, Artikel 16, Artikel 4 Absatz 3 Buchstabe a, Artikel 15 Absatz 3, Artikel 19 Absatz 1 Buchstabe a und Anhang) sowie speziellere Hinweise auf die Notwendigkeit einer Zusammenarbeit mit den nationalen Datenschutzbehörden (Artikel 18 Buchstabe f und Artikel 20 Absatz 2).
8. Der EDSB begrüßt den obengenannten Inhalt. Er möchte aber seine Bedenken gegen einige der Bestimmungen äußern, die nicht eindeutig definiert oder ausgearbeitet sind und daher zu Unklarheiten führen, die möglicherweise die einheitliche Umsetzung des Vorschlags durch die Mitgliedstaaten beeinträchtigen könnten.
9. Speziell die teilweise widersprüchliche Verwendung der Begriffe „Rückverfolgbarkeit der Organe“ und „Anonymität von Spendern und Empfängern“ ist ein Problem, das weitere Klärung und Präzisierung erfordert. In diesem Zusammenhang sollte weiter herausgestellt werden, dass verstärkte Sicherheitsmaßnahmen zum Schutz der Spender- und Empfängerdaten auf Ebene der Mitgliedstaaten eingeleitet werden müssen, um ein höheres Datenschutzniveau in den verschiedenen europäischen Ländern zu garantieren und den Datenschutz beim grenzüberschreitenden Organ- austausch (innerhalb und außerhalb Europas) sicherzustellen.
10. In dieser Stellungnahme werden die obengenannten Probleme eingehender behandelt, um Klarheit und Kohärenz

des aktuellen datenschutzbezogenen Inhalts des Vorschlags zu verbessern.

II. KLÄRUNG DER BEGRIFFE „RÜCKVERFOLGBARKEIT“ UND „ANONYMITÄT“

Anwendbarkeit der Richtlinie 95/46/EG

11. Gemäß Artikel 2 Buchstabe a der Richtlinie 95/46/EG über den Schutz personenbezogener Daten bezeichnet der Ausdruck „personenbezogene Daten“ „alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Faktoren, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.“
12. Biologisches Material menschlichen Ursprungs (z. B. Organe, Gewebe, Zellen oder Blut) kann definiert werden als Material, das dem menschlichen Körper entnommen werden kann. Es ist fraglich, ob das Material selbst als personenbezogene Daten angesehen werden kann. Jedoch ist unbestritten, dass derartiges Material als *Quelle* für personenbezogene Informationen über dessen Besitzer dienen kann. Mit der Verarbeitung biologischen Materials wird oft die Gewinnung solcher Informationen bezweckt. Auch ohne einen solchen Zweck wird biologisches Material häufig von auf diese Weise gewonnenen Informationen begleitet. In diesen Fällen gelten die Vorschriften der Richtlinie 95/46/EG ⁽⁴⁾. Das trifft zu, sofern der Besitzer des biologischen Materials eine *bestimmte* oder *bestimmbare* (natürliche) Person ist.
13. In Erwägungsgrund 26 der Richtlinie 95/46/EG wird erklärt, wie zu entscheiden ist, ob eine Person bestimmbar ist: „[Es] sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“. In dem gleichen Erwägungsgrund wird weiter erklärt, dass die Vorschriften der Richtlinie 95/46/EG nicht gelten, wenn die Informationen eine Person betreffen, die nicht oder nicht mehr identifizierbar ist; solche Daten gelten als *anonym*.
14. In der Empfehlung(2006) 4 hat der Europarat die spezielle Frage der Identifizierbarkeit von biologischem Material behandelt, wobei er zwischen personenbezogenem und nicht-personenbezogenem biologischen Material unterscheidet ⁽⁵⁾.
15. Gemäß der Empfehlung ist *personenbezogenes biologisches Material* „biologisches Material, das allein oder in Verbindung mit zugeordneten Daten die Identifikation der betroffenen Personen entweder unmittelbar oder mittels eines Schlüssels ermöglicht“ ⁽⁶⁾. In letzterem Fall hat der Benutzer des biologischen Materials entweder Zugang zu dem Schlüssel („verschlüsseltes Material“) oder er hat keinen

⁽¹⁾ Dieser Rahmen umfasst die Richtlinien 2002/98/EG, 2004/33/EG, 2005/61/EG und 2005/62/EG für Blut und Blutprodukte und die Richtlinien 2004/23/EG, 2006/17/EG und 2006/86/EG für menschliche Gewebe und Zellen.

⁽²⁾ Siehe auch den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, KOM(2008) 414 endgültig.

⁽³⁾ Stellungnahme des EDSB vom 2. Dezember 2008 zum Vorschlag für eine Richtlinie über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung.

⁽⁴⁾ Artikel-29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ (S. 9).

⁽⁵⁾ Empfehlung(2006) 4 des Ministerkomitees an die Mitgliedstaaten über Forschung mit humanbiologischem Material.

⁽⁶⁾ Artikel 3 Ziffer i der Empfehlung(2006) 4.

Zugang zu dem Schlüssel, der sich in der Gewalt eines Dritten befindet („nicht vollständig anonymisiertes Material“). In ihrer Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ hat die Artikel-29-Datenschutzgruppe (nachstehend „WP 29“) den Begriff der *rücknehmbar pseudonymisierten Daten* verwendet, um indirekt bestimmbare Informationen über Personen zu beschreiben, bei denen noch die Möglichkeit der Rückverfolgung zu den Personen und der Aufdeckung ihrer Identität besteht, wenn auch nur unter zuvor festgelegten Bedingungen⁽¹⁾. Als Beispiel werden *verschlüsselte Daten* genannt, bei denen personenbezogene Daten durch einen Code gekennzeichnet werden, während der Schlüssel für die Zuordnung des Codes zu den Kennzeichen der Personen gesondert aufbewahrt wird. Wenn für jede Person ein eindeutiger Code verwendet wird, so ist deren Identifizierung mit Hilfe des für die Codierung verwendeten Schlüssels möglich.

16. Die Empfehlung verweist auch auf *nichtpersonenbezogenes Material* (oder „vollständig anonymisiertes Material“) als „biologisches Material, das weder allein noch in Verbindung mit zugeordneten Daten die Identifikation der betroffenen Personen mit vertretbarem Aufwand ermöglicht“⁽²⁾. Dieses Material würde tatsächlich als anonyme Daten im Sinne der Richtlinie 95/46/EG gelten.
17. Daraus folgt, dass die Richtlinie 95/46/EG auf die Gewinnung, Lagerung und Verarbeitung von bestimmaren Organen und die anschließende Gewinnung von Informationen über solche Organe, solange diese möglich ist, Anwendung findet, wobei alle Mittel gebührend zu berücksichtigen sind, die vernünftigerweise eingesetzt werden könnten, um die betreffende Person zu bestimmen. Wie noch gezeigt wird, bedeutet die dauerhafte Rückverfolgbarkeit von Organen, wie sie in dem Richtlinienvorschlag vorgesehen ist, dass die betreffenden Personen während des gesamten Prozesses bestimmbar bleiben.

Rückverfolgbarkeit und Anonymität menschlicher Organe im Vergleich

18. Die Rückverfolgbarkeit von biologischem Material bedeutet die Möglichkeit, das Material bis zu seinem Besitzer zurückzuverfolgen und somit dessen Identität zu bestimmen. Mit anderen Worten: Wenn die Rückverfolgbarkeit der Besitzer von biologischem Material unmittelbar oder mittelbar möglich ist, sind die Besitzer als bestimmbar anzusehen und umgekehrt. Die Begriffe „Rückverfolgbarkeit“ und „bestimmbar“ sind daher im Prinzip eng miteinander verbunden. Hingegen können Rückverfolgbarkeit und Anonymität von Daten nicht gleichzeitig auftreten. Sie stehen im Gegensatz zueinander. Wenn bestimmte Informationen wirklich anonym sind, ist es nicht möglich, sie zurückzuverfolgen und die betreffenden Personen zu bestimmen.
19. Im Rahmen des vorliegenden Vorschlags ist die Rückverfolgbarkeit eine obligatorische Anforderung, die zweifach, d.h. in Bezug auf die Spender und die Empfänger, in die nationalen Qualitätsprogramme der Mitgliedstaaten aufzunehmen ist. Das bedeutet, dass zwar die Informationen über Spender und Empfänger vertraulich bleiben, die organbezogenen Informationen aber identifizierbar sind. Dies

geht auch aus der Definition in Artikel 3 des Vorschlags hervor, wonach Rückverfolgbarkeit „die Möglichkeit einer zuständigen Behörde [ist], das Organ in jeder Phase von der Spende bis zur Transplantation oder Entsorgung zu lokalisieren und zu identifizieren; diese ist unter in dieser Richtlinie spezifizierten Bedingungen ermächtigt, den Spender und die Beschaffungsorganisation zu identifizieren, die Empfänger in den Transplantationszentren zu identifizieren, alle sachdienlichen nicht personenbezogenen Informationen über Produkte und Materialien, mit denen das Organ in Berührung kommt, zu lokalisieren und zu identifizieren“.

20. Ferner heißt es in dem die Rückverfolgbarkeit betreffenden Artikel 10 Absatz 1 des Vorschlags: „Die Mitgliedstaaten stellen sicher, dass alle auf ihrem Hoheitsgebiet beschafften und zugeteilten Organe vom Spender bis zum Empfänger und zurück verfolgt werden können, um die Gesundheit von Spendern und Empfängern zu schützen“. Artikel 10 Absatz 3 besagt: „Die Mitgliedstaaten stellen Folgendes sicher: a) Gemäß den nationalen Qualitätsprogrammen bewahrt die zuständige Behörde oder andere an der Kette von der Spende bis zur Transplantation oder Entsorgung beteiligte Stellen die Daten auf, die zur Sicherstellung der Rückverfolgbarkeit in allen Phasen von der Spende bis zur Transplantation oder Entsorgung erforderlich sind; b) die zur Sicherstellung einer lückenlosen Rückverfolgung erforderlichen Daten werden mindestens 30 Jahre nach der Spende aufbewahrt. Die Datenspeicherung kann elektronisch erfolgen.“
21. Wenngleich der Rückverfolgungsprozess Durchführungsmaßnahmen unterliegt (siehe Artikel 25 des Vorschlags), erscheint ein indirektes Identifikationssystem für Spender und Empfänger als die wahrscheinlichste Lösung, da es der Richtlinie 2004/23/EG⁽³⁾ über menschliche Gewebe und Zellen und dem darin festgelegten europäischen Identifizierungskode⁽⁴⁾ entspricht oder zumindest interoperabel

⁽³⁾ Da Organspender sehr oft Gewebespender sind, müssen alle unerwünschten Reaktionen auch im Rahmen des Gewebeüberwachungssystems zurückverfolgt und gemeldet werden; daher ist Interoperabilität mit der in diesem System verwendeten indirekten Identifizierungsmethode erforderlich. Siehe: Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates vom 31. März 2004 zur Festlegung von Qualitäts- und Sicherheitsstandards für die Spende, Beschaffung, Testung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen (ABl. L 102 vom 7.4.2004, S. 48) und Richtlinie 2006/86/EG der Kommission vom 24. Oktober 2006 zur Umsetzung der Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an die Rückverfolgbarkeit, der Meldung schwerwiegender Zwischenfälle und unerwünschter Reaktionen sowie bestimmter technischer Anforderungen an die Kodierung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen (ABl. L 294 vom 25.10.2006, S. 32).

⁽⁴⁾ Dieser Code umfasst eine einzige Kennnummer für jede Spende, die zusammen mit der Kennung der Gewebebank und der Produktkennung die Rückverfolgung zu den Spendern und Empfängern ermöglicht. Konkret ist nach Artikel 10 der Richtlinie 2006/86/EG „sämtlichem gespendeten Material [...] in der Gewebebank ein einheitlicher europäischer Identifizierungskode zuzuweisen, um eine ordnungsgemäße Identifizierung des Spenders und die Rückverfolgbarkeit des gesamten gespendeten Materials sicherzustellen und Informationen über die Hauptmerkmale und Eigenschaften der Gewebe und Zellen zu liefern“. Gemäß Anhang VII der Richtlinie besteht der Code aus zwei Teilen: a) der Spendenkennung mit einer eindeutigen Kennnummer und der Kennung der Gewebebank und b) der Produktkennung mit dem Produktcode, der Splitnummer und dem Verfallsdatum.

⁽¹⁾ Artikel 29 Datenschutzgruppe: Stellungnahme 4/2007, S. 18.

⁽²⁾ Artikel 3 Ziffer ii der Empfehlung(2006) 4.

mit ihnen ist. In diesem Fall betrifft die Verarbeitung in Bezug auf Spender und Empfänger im Rahmen des Vorschlags nicht vollständig anonymisiertes, biologisches Material bzw. — nach der im Datenschutz üblichen Bezeichnungsweise — rücknehmbar pseudonymisierte Daten (siehe Nummer 15), für die die Bestimmungen der Richtlinie 95/46/EG gelten.

22. Es ist jedoch festzustellen, dass trotz der klaren Anforderungen hinsichtlich der Rückverfolgbarkeit und Identifizierbarkeit in einigen Teilen des Vorschlags die Begriffe „Anonymität“ und „anonyme Daten“ im Zusammenhang mit Spender- und Empfängerdaten verwendet werden. Aus den vorstehenden Darlegungen ergibt sich, dass dies widersprüchlich und äußerst verwirrend ist ⁽¹⁾.
23. So heißt es in Artikel 10 Absatz 2 des Vorschlags, in dem die Notwendigkeit eines Spenderidentifikationssystems festgestellt wird: „Die Mitgliedstaaten sorgen für die Einführung eines Spenderidentifikationssystems, das jede Spende und jedes damit verbundene Organ identifizieren kann. Die Mitgliedstaaten stellen sicher, dass dieses Spenderidentifikationssystem entsprechend dem Ziel gestaltet und ausgewählt wird, keine persönlichen Daten oder so wenige wie möglich zu erheben, zu verarbeiten oder zu verwenden. Insbesondere ist von den Möglichkeiten zur Pseudonymisierung oder Anonymisierung der einzelnen Personen Gebrauch zu machen.“ ⁽²⁾ Nach Ansicht des EDSB stehen die unterstrichenen Ausdrücke in diesem Absatz im Widerspruch zum Konzept der Rückverfolgbarkeit, da es nicht möglich ist, rückverfolgbare und identifizierbare Daten zu haben, wenn Spender und Empfänger anonymisiert werden. Zudem ist es verwunderlich, dass sich dieser Absatz auf die Spenderidentifikation bezieht, während die Empfängeridentifikation (die ebenso Teil des Prozesses ist) mit keinem Wort erwähnt wird.
24. Noch deutlicher werden die obenerwähnten Widersprüche in Artikel 17 betreffend die Anonymisierung von Spendern und Empfängern, in dem es heißt: „Die Mitgliedstaaten treffen alle notwendigen Maßnahmen, um sicherzustellen, dass alle verarbeiteten personenbezogenen Daten von Spendern und Empfängern, die in den Geltungsbereich dieser Richtlinie fallen, anonymisiert werden, so dass weder Spender noch Empfänger identifizierbar bleiben“. Dieser Artikel steht im vollkommenen Widerspruch zu den Artikeln über die Rückverfolgbarkeit in dem Vorschlag.

Vertraulichkeit anstelle von Anonymität

25. Der EDSB geht davon aus, dass der Begriff „Anonymität“ eigentlich verwendet wird, um auf die Notwendigkeit einer höheren *Vertraulichkeit* ⁽³⁾ der Spender- und Empfänger-

daten hinzuweisen, was bedeutet, dass nur Zugangsberechtigte auf diese Informationen zugreifen können. Der EDSB geht weiter davon aus, dass der Begriff „Anonymisierung“ so verwendet wird, dass er ein indirektes Identifikationssystem für Spender und Empfänger ⁽⁴⁾ beinhaltet, was auch aus der Art und Weise abgeleitet werden kann, in der dieser Begriff in der Richtlinie 2004/23/EG über Gewebe und Zellen verwendet wird. Wie aber bereits gesagt, ist „Anonymität“ hier nicht der korrekte Begriff.

26. Ein Beispiel dafür, wie Datenschutz und Rückverfolgbarkeit in einem Transplantationsprozess behandelt werden können, ist in dem Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin betreffend biomedizinische Forschung ⁽⁵⁾ zu finden. Dort wird der Begriff „Vertraulichkeit“ anstelle des Begriffs „Anonymität“ verwendet. So heißt es in Artikel 23 Absatz 1 des Protokolls: „Alle personenbezogenen Daten der Person, bei der Organe oder Gewebe entnommen wurden, sowie die personenbezogenen Daten des Empfängers sind als vertraulich zu betrachten. Sie dürfen nur nach den Regeln des Berufsgeheimnisses und den Vorschriften zum Schutz personenbezogener Daten gesammelt, verarbeitet und weitergegeben werden.“ In Absatz 2 wird Folgendes weiter ausgeführt: „Die Auslegung der Bestimmungen von Absatz 1 lässt die Bestimmungen unberührt, die vorbehaltlich geeigneter Sicherheitsmaßnahmen das Sammeln, die Verarbeitung und Weitergabe der erforderlichen Angaben über die Person, bei der Organe oder Gewebe entnommen wurden, oder über den (die) Empfänger der Organe oder Gewebe erlauben, soweit dies zu medizinischen Zwecken einschließlich der in Artikel 3 dieses Protokolls vorgesehenen Rückverfolgbarkeit erforderlich ist.“
27. Ausgehend von den vorstehenden Bemerkungen empfiehlt der EDSB, die Formulierung einiger Teile des Vorschlags zu ändern, um Mehrdeutigkeit zu vermeiden und deutlich zum Ausdruck zu bringen, dass die Daten nicht anonym sind, aber nach strengen Vertraulichkeits- und Sicherheitsvorschriften verarbeitet werden sollten. Konkret empfiehlt der EDSB die folgenden Änderungen:

⁽⁴⁾ Der Begriff „Anonymisierung“ wird kontextabhängig manchmal in dem Sinne verwendet, dass er indirekt bestimmbare Daten umfasst, z. B. im Fall von Statistiken. Das ist jedoch aus datenschutzrechtlicher Sicht nicht korrekt, wie der EDSB in seiner Stellungnahme zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz (KOM(2007) 46 endgültig) und zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Statistiken (KOM(2007) 625 endgültig) dargelegt hat.

⁽⁵⁾ Europarat, Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin bezüglich der Transplantation von menschlichen Organen und Geweben, Straßburg, 24.1.2002, zum Stand der Ratifizierung siehe <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=186&CM=8&DF=2/13/2009&CL=ENG> Siehe auch Europarat, Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin, Oviedo, 4.4.1997, zum Stand der Ratifizierung siehe auch: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=2/13/2009&CL=ENG>

⁽¹⁾ Diese Feststellung ist auch in den Bemerkungen des EDSB vom 19.9.2006 zur öffentlichen Konsultation über die künftige Tätigkeit der EU im Bereich der Organspende und -transplantation enthalten.

⁽²⁾ Eigene Unterstreichungen.

⁽³⁾ Gewährleistung des Zugangs zu Informationen nur für Zugangsberechtigte (ISO-Definition, Quelle: <http://www.wikipedia.org>).

— Erwägungsgrund 16 letzter Satz: „Gemäß dieser Charta und unter Berücksichtigung des Übereinkommens des Europarates über Menschenrechte und Biomedizin sollten sich Organtransplantationsprogramme auf die Grundsätze der freiwilligen und unentgeltlichen Spende, der Uneigennützigkeit des Spenders und der Solidarität zwischen Spender und Empfänger stützen, wobei zu gewährleisten ist, dass strenge Vertraulichkeitsvorschriften und Sicherheitsmaßnahmen für den Schutz der personenbezogenen Daten von Spendern und Empfängern vorhanden sind.“

— Artikel 10 Absatz 2: „Die Mitgliedstaaten sorgen für die Einführung eines Spender- und Empfängeridentifikationssystems, das jede Spende und jedes damit verbundene Organ identifizieren kann. Die Mitgliedstaaten stellen sicher, dass dieses Spender- und Empfängeridentifikationssystem entsprechend dem Ziel gestaltet und ausgewählt wird, möglichst wenige personenbezogene Daten zu erheben, zu verarbeiten oder zu verwenden, dabei insbesondere Pseudonymisierungsverfahren anzuwenden und zu gewährleisten, dass die für die Sicherheit dieser Daten erforderlichen technischen und organisatorischen Vorkehrungen vorhanden sind.“

— Artikel 17 könnte an sich gestrichen und sein Inhalt (in Bezug auf den Vertraulichkeitsbedarf) in einen neuen Absatz von Artikel 16 betreffend den Schutz personenbezogener Daten, Vertraulichkeit und Sicherheit der Verarbeitung aufgenommen werden (siehe Nummer 36).

28. Wie in den folgenden Teilen dieser Stellungnahme erörtert wird, empfiehlt der EDSB außerdem, die Notwendigkeit eines *stärkeren Schutzes* der Spender- und Empfängerdaten durch die Anwendung *strengerer Sicherheitsmaßnahmen* auf nationaler wie auch auf grenzüberschreitender Ebene noch deutlicher herauszustellen.

III. BETONUNG NATIONALER VORKEHRUNGEN FÜR DIE DATENSICHERHEIT

Grundlegende Sicherheitserfordernisse und -anforderungen

29. Wie aus dem Vorschlag hervorgeht, erfolgt die Verarbeitung von personenbezogenen Daten der Spender und Empfänger hauptsächlich auf nationaler Ebene, d.h. in den Beschaffungs- und Transplantationszentren der Mitgliedstaaten. Auf dieser Ebene wird auch das Lebendspenderregister geführt. Wenngleich der Rückverfolgungsmechanismus noch nicht festgelegt wurde, ist zu erwarten, dass alle Kodierungsmaßnahmen auch auf nationaler Ebene erfolgen werden, selbst wenn ein europäisches Codierungssystem zum Einsatz gelangt, da eine Identifizierung der Spender und Empfänger nur über die zuständigen nationalen Behörden möglich ist.

30. Daher ist es äußerst wichtig, eine Informationssicherheitspolitik auf der Grundlage *strenger und solider Sicherheitsmaßnahmen* in den entsprechenden nationalen Dienststellen zu verfolgen, um die in dem Vorschlag enthaltenen Vertraulichkeitsanforderungen für die Spender und Empfänger zu erfüllen und für diese Daten die Grundsätze der *Integrität* ⁽¹⁾, *Rechenschaftspflicht* ⁽²⁾ und *Verfügbarkeit* ⁽³⁾ zu befolgen. In dieser Hinsicht sollte die Informationssicherheitspolitik Elemente physischer und logischer Sicherheit umfassen und sich unter anderem auf die Kontrolle von Eingabe, Zugriff, Speicherung, Übermittlung und Übertragung von Daten sowie auf die Kontrolle von Datenträgern und -speichern konzentrieren.

31. Was die Vertraulichkeit anbelangt, so können durch die medizinischen Daten der Empfänger ⁽⁴⁾ sowie durch die für die Charakterisierung und Betreuung der Spender verwendeten Daten (auch in Bezug auf einen „erweiterten Spenderkreis“ ⁽⁵⁾) sensible personenbezogene Informationen offengelegt werden, was sich auch auf das soziale, berufliche und/oder private Leben dieser Personen auswirken kann. Der Schutz der Angaben über die Spenderidentität ist außerdem wichtig, wenn Lebendspender oder Personen, die eingewilligt haben, nach ihrem Tod ein oder mehrere Organe zu spenden, zu Opfern des Handels mit menschlichen Organen oder Geweben werden könnten, falls diese Angaben preisgegeben werden. Auch die Integrität der organbezogenen Daten ist äußerst wichtig, da selbst der kleinste Fehler bei den übermittelten Informationen für den Empfänger lebensbedrohlich sein kann. Das Gleiche gilt für die Richtigkeit der vor der Transplantation erhobenen Gesundheitsdaten der Spender, denn anhand dieser Daten wird über die Eignung eines Organs entschieden. Im Hinblick auf die Rechenschaftspflicht sollte in Anbetracht der Tatsache, dass so viele verschiedene

(1) „Datenintegrität“ kann bezeichnen: die Gewährleistung der Unversehrtheit bzw. Vollständigkeit der Daten; den Zustand, in dem die Daten während eines jeden Vorgangs (z. B. Übermittlung, Aufbewahrung oder Abruf) identisch erhalten bleiben; die Aufbewahrung der Daten für ihre beabsichtigte Verwendung oder — in Bezug auf bestimmte Vorgänge — a priori die Erwartung von Datenqualität. Einfach gesagt, bedeutet Datenintegrität die Gewissheit, dass die Daten widerspruchsfrei und richtig sind (Quelle: <http://www.wikipedia.org>); Gewährleistung, dass nur Zugangsberechtigte auf die Informationen zugreifen oder diese ändern können (Quelle: <http://searchdatacenter.techtarget.com>).

(2) Pflicht, über seine Handlungen Rechenschaft abzulegen; Nichtabstreitbarkeit: Gewährleistung, dass die Daten von den Seiten gesendet und empfangen wurden, die dies für sich beanspruchen; Gewährleistung, dass eine Seite in einem Streitfall die Gültigkeit einer Aussage nicht abstreiten oder anfechten kann (Quelle: <http://www.wikipedia.org>).

(3) Der Umfang, in dem unverzüglich auf Daten zugegriffen werden kann (Quelle: <http://www.pcmag.com>).

(4) Es ist anzumerken, dass allein die Tatsache, dass einem Empfänger ein Organ transplantiert wird, bereits eine sensible personenbezogene Information über die Gesundheit dieser Person darstellt.

(5) Potenzielle Spender, die nicht als Idealspender gelten, die aber unter gewissen Umständen, z. B. für ältere Menschen, in Frage kommen. Siehe: Arbeitspapier der Kommissionsdienststellen als Begleitpapier zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Qualitäts- und Sicherheitsstandards für zur Transplantation bestimmte menschliche Organe und zur Mitteilung der Kommission „Aktionsplan im Bereich Organspende und -transplantation (2009—2015): Verstärkte Zusammenarbeit zwischen den Mitgliedstaaten“ — Zusammenfassung der Folgenabschätzung vom 8.12.2008.

- Einrichtungen an dem gesamten Spenden- und Transplantationssystem beteiligt sind, ein Weg gefunden werden, damit alle beteiligten Einrichtungen sich ihrer Verantwortung bewusst sind und die Verantwortung für ihr Handeln übernehmen können, z. B. wenn Angaben über die Spenderidentität in unbefugte Hände gelangen oder die medizinischen Daten eines Organs nicht exakt sind. Da das gesamte System auf der Übermittlung von organbezogenen Daten und dem Mechanismus der Rückverfolgbarkeit vom Spender zum Empfänger beruht, sollten diese Daten befugten Personen bei Bedarf unverzüglich zur Verfügung stehen (andernfalls würde die Nichtverfügbarkeit das reibungslose Funktionieren des Systems gefährden).
32. In diesem Zusammenhang sollten geeignete *Autorisierungsmechanismen* nach speziellen Grundsätzen für die Zugriffskontrolle sowohl für die nationalen Datenbanken als auch für den grenzüberschreitenden Organ austausch vorhanden sein. Diese Grundsätze sollten zunächst auf Ebene der Einrichtungen festgelegt werden, insbesondere für die Verfahren zur Identifizierung von Spendern und Empfängern (z. B. wer hat unter welchen Bedingungen Zugriff auf welche Informationen). Auf diese Weise werden *Zugriffsrechte* sowie *Zugriffsszenarios* für die Ausübung dieser Rechte festgelegt (z. B. die Umstände und Verfahren für die Offenlegung von Daten durch die Beschaffungseinrichtung gegenüber der zuständigen Behörde, gegebenenfalls einige Fälle, in denen dem Empfänger die Identität des Spenders bekanntgegeben werden muss und die hierfür geltenden Verfahren). Um die Wirksamkeit der Grundsätze zu gewährleisten, sollten für die an der Verarbeitung beteiligten Personen spezielle *Vertraulichkeitsvorschriften* gelten.
33. Sobald diese Grundsätze feststehen, können sie auf technischer Ebene umgesetzt werden, d. h. im Hinblick auf die Kontrolle des Benutzerzugriffs auf die Systeme und Anwendungen entsprechend den vordefinierten Zugriffsrechten. Hierfür können bewährte Technologien wie *Verschlüsselung* und *digitale Zertifikate* ⁽¹⁾ (z. B. auf der Grundlage einer *Public-Key-Infrastruktur* ⁽²⁾) genutzt werden. *Rollenbasierte Authentisierungsmechanismen* können zudem verwendet werden, um die Zugriffsrechte der Benutzer ausgehend von ihrer Rolle einzuschränken (z. B. sollten nur Ärzte befugt sein, die medizinischen Daten von Empfängern und Spendern in den nationalen Datenbanken zu ändern).
34. Die Zugriffskontrolle sollte durch Möglichkeiten zur *Erfassung* von Benutzeraktionen ergänzt werden (z. B. Lese- und Schreibzugriff auf medizinische Daten), insbesondere wenn elektronische Systeme genutzt werden. Durch physische und logische Sicherheitsmaßnahmen sollte auch sichergestellt werden, dass die Spender- und Organdatenbanken als ein zentrales Element des vorgeschlagenen Spenden- und Transplantationssystems *voll funktionsfähig* sind. Die Verfügbarkeit der Daten sollte als ein Eckstein des Systems betrachtet werden. Hier sollte die Informationssicherheitspolitik auf einer soliden *Risikoanalyse und -bewertung* beruhen und auch Elemente wie Incident Management und Business Continuity Management (BCM) umfassen. Alle diese Elemente sollten im Rahmen regelmäßiger Kontrollen und Überprüfungen erhalten und verbessert werden. *Unabhängige Audits* können ebenfalls die Wirksamkeit des Systems steigern und dieses weiter verbessern, wobei besonderes Augenmerk auf die Pseudonymisierung, Rückverfolgbarkeit und Datenübertragung zu richten ist.
35. Der EDSB spricht sich dafür aus, dass die Notwendigkeit derartiger Maßnahmen im Rahmen der vorgeschlagenen Richtlinie stärker herausgestellt wird.
- Verstärkung der Sicherheitsbestimmungen des Vorschlags*
36. In dem Vorschlag heißt es in Artikel 16 betreffend den Schutz personenbezogener Daten, Vertraulichkeit und Sicherheit der Verarbeitung: „Die Mitgliedstaaten stellen sicher, dass bei allen Tätigkeiten im Zusammenhang mit der Organtransplantation das Grundrecht auf Schutz personenbezogener Daten im Einklang mit den Gemeinschaftsvorschriften über den Schutz personenbezogener Daten, insbesondere Artikel 8 Absatz 3, Artikel 16, 17 und Artikel 28 Absatz 2 der Richtlinie 95/46/EG, vollständig und wirksam gewährleistet wird.“ Der EDSB empfiehlt, in diesen Artikel einen *zweiten Absatz* aufzunehmen, in dem die Grundprinzipien für die Gewährleistung der Sicherheit auf Ebene der Mitgliedstaaten beschrieben werden und mindestens auf die folgenden Punkte Bezug genommen wird:
- Es sollte eine Informationssicherheitspolitik zur Umsetzung der technischen und organisatorischen Maßnahmen geben, um in Bezug auf die personenbezogenen Daten von Spendern und Empfängern Vertraulichkeit, Integrität, Rechenschaftspflicht und Verfügbarkeit zu gewährleisten.
 - Es sollte eine spezielle Strategie für die Vertraulichkeit und die Zugriffskontrolle zur Anwendung in allen Mitgliedstaaten erarbeitet werden, in der die Zugriffsrechte, Rollen und Verantwortlichkeiten aller Beteiligten (Spender, Beschaffungseinrichtung, Transplantationszentrum, Empfänger, zuständige nationale Behörde, für den grenzüberschreitenden Organaustausch zuständige Behörden) festgelegt sind. Es sollte konkrete Garantien für die Vertraulichkeit der Daten für die an der Verarbeitung beteiligten Personen geben, insbesondere wenn diese nicht der ärztlichen Schweigepflicht unterliegen (z. B. Verhaltenskodizes zur Vertraulichkeit und Sensibilisierungsmaßnahmen).
 - Es sollte herausgestellt werden, dass Sicherheitsmechanismen (wie Verschlüsselung und digitale Zertifikate) in den nationalen Datenbanken zum Tragen kommen müssen. Insbesondere für die Spenderregister sollte der Grundsatz des „eingebauten Datenschutzes“ (privacy by design) gelten, damit alle notwendigen Sicherheitsanforderungen in den ersten Durchführungsphasen solcher Entwicklungen berücksichtigt werden.
 - Es sollten ferner Verfahren zur Sicherung der Datenschutzrechte der Spender und Empfänger, insbesondere des Zugriffs- und Berichtigungsrechts sowie des Rechts auf Information, festgelegt werden. Besonders sorgfältig sollte auch vorgegangen werden, wenn Spender ihre Zustimmung widerrufen wollen oder nicht als Spender akzeptiert werden (nach der Spender- und Organcharakterisierung). Für diesen Fall sollten ein spezielles Verfahren und eine Frist für die Aufbewahrung ihrer Daten festgelegt werden.

(1) Das elektronische Äquivalent eines Personalausweises, das den Urheber einer digitalen Signatur authentisiert (Quelle: http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html).

(2) Eine Public-Key-Infrastruktur (PKI) ist ein System von Hardware, Software, Menschen, Konzepten und Verfahren, das zur Erzeugung, Verwaltung, Speicherung und Verteilung sowie zum Widerruf digitaler Zertifikate dient (Quelle: <http://www.wikipedia.org>).

- Außerdem sollten im Rahmen der Informationssicherheitspolitik Maßnahmen vorgesehen werden, um die Integrität und ununterbrochene Verfügbarkeit der Daten zu garantieren. Die Rolle der Bewertung der Informationssicherheitsrisiken sollte durch die Übernahme von Elementen des Incident Managements und des Business Continuity Managements ergänzt werden.
- Die Informationssicherheitspolitik sollte einer regelmäßigen Kontrolle und Überprüfung, einschließlich unabhängiger Audits, unterliegen.

37. Der EDSB empfiehlt, die obengenannten Elemente in Artikel 16 aufzunehmen und dann als Teil der Durchführungsmaßnahmen des Artikels 25, insbesondere des Absatzes 1 Buchstaben a, b und c, weiter auszuführen.

IV. GARANTIE IN BEZUG AUF DEN GRENZÜBERSCHREITENDEN ORGANAUSTAUSCH

Harmonisierung der Sicherheitspolitik in den Mitgliedstaaten

38. Der grenzüberschreitende Organaustausch wird in der Praxis immer die Verarbeitung personenbezogener Daten einschließen, insofern als selbst im Falle einer Codierung die Organe nach wie vor (indirekt) durch die zuständigen nationalen Behörden identifiziert werden können.
39. Der EDSB hat bereits zu den Sicherheitserfordernissen für den Schutz personenbezogener Daten bei der grenzüberschreitenden Gesundheitsversorgung in Europa Stellung genommen und dabei unter anderem betont, dass die Informationssicherheitspolitik der Mitgliedstaaten harmonisiert werden muss, um ein solides Datenschutzniveau zu erreichen⁽¹⁾. Er empfiehlt, dass dieser Aspekt auch in dem vorliegenden Vorschlag erwähnt wird, konkret in Erwägungsgrund 17, in dem auf die Bestimmung über die Sicherheit der Verarbeitung in der Richtlinie 95/46/EG hingewiesen wird.

Schaffung des Rückverfolgungssystems

40. In diesem konkreten Fall ist der zu schaffende Rückverfolgungsmechanismus ein wichtiger Parameter für die grenzüberschreitende Datensicherheit. Daher sollte neben den auf Ebene der Mitgliedstaaten geltenden Sicherheitsmaßnahmen besonderes Augenmerk darauf gerichtet werden, welche Pseudonymisierungsmöglichkeiten zur Identifizierung der Spender und Empfänger genutzt werden (z. B. Art der Verschlüsselung, Möglichkeit der Doppelverschlüsselung usw.) und wie die Interoperabilität mit dem Gewebe- und Zellenidentifikationssystem gewahrt wird.
41. Der EDSB empfiehlt, dass in den die Durchführungsmaßnahmen betreffenden Artikel 25 der vorgeschlagenen Richtlinie ein spezieller Verweis auf dieses Problem erfolgt, indem Absatz 1 Buchstabe b folgende Fassung erhält: „Verfahren zur Sicherstellung der lückenlosen Rückverfolgbarkeit der Organe, einschließlich Kennzeichnungsvorschriften, das die Vertraulichkeit in Bezug auf Spender und Empfänger während des gesamten Rückverfolgungsprozesses garantiert und die Interoperabilität mit dem Gewebe- und Zellenidentifikationssystem wahrt;“

Organaustausch mit Drittländern

42. Sicherheitserfordernisse gewinnen noch an Bedeutung, wenn Daten mit Drittländern ausgetauscht werden, in denen ein angemessenes Datenschutzniveau nicht immer garantiert werden kann. Eine besondere Regelung für die Übermittlung personenbezogener Daten an Drittländer ist in den Artikeln 25 und 26 der Richtlinie 95/46/EG enthalten. Der EDSB ist sich der Tatsache bewusst, dass Datenschutzanforderungen nicht den schnellen und effizienten Organtransfer behindern sollten, der ein Erfordernis des Organspendesystems darstellt und oft sogar zu einer Frage von Leben oder Tod werden kann. Daher sollten die Möglichkeiten geprüft werden, Transfers zu erlauben, auch wenn in dem betreffenden Drittland ein angemessenes Datenschutzniveau im Allgemeinen nicht gegeben ist. Dabei sollte berücksichtigt werden, dass aufgrund der Tatsache, dass auf grenzüberschreitender Ebene die Identifizierung der betreffenden Personen nur indirekt möglich ist und dass die zuständigen nationalen Behörden die Oberaufsicht über das System haben, die entsprechenden Risiken höchstwahrscheinlich geringer sind als auf nationaler Ebene⁽²⁾.
43. Nach Auffassung des EDSB sollte zu diesem Zweck die zuständige Behörde, die für die Genehmigung solcher Transfers verantwortlich ist, sich mit der nationalen Datenschutzbehörde abstimmen, um unter Berücksichtigung der in Artikel 26 der Richtlinie 95/46/EG genannten möglichen Ausnahmen den notwendigen Rahmen für die sichere, aber auch schnelle und effiziente Übermittlung von organbezogenen Daten an Drittländer und aus Drittländern zu entwickeln. Der EDSB empfiehlt, dass in Artikel 21 über den Organaustausch mit Drittländern oder in dem entsprechenden Erwägungsgrund 15 ein Verweis auf dieses Thema erfolgt.

Durchführungsmaßnahmen

44. Abschließend ersucht der EDSB den Gesetzgeber dringend, zu gewährleisten, dass in Bezug auf Artikel 25 immer dann, wenn den Datenschutz und die Datensicherheit betreffende Durchführungsmaßnahmen geprüft werden, eine Konsultation aller relevanten Akteure, einschließlich des EDSB und der Artikel-29-Datenschutzgruppe, erfolgt.

V. SCHLUSSFOLGERUNGEN

45. Der EDSB hat Kenntnis von der Initiative genommen, hohe Qualitäts- und Sicherheitsstandards für zur Transplantation bestimmte menschliche Organe zu gewährleisten, die als Teil des Gesamtkonzepts der EG für die Festlegung gemeinsamer Standards zur Förderung der grenzüberschreitenden Verfügbarkeit von Gesundheitsdienstleistungen in ganz Europa angesehen werden kann.
46. In dem Vorschlag wurden die Datenschutzbedürfnisse von Organspendern und -empfängern, insbesondere das Erfordernis, ihre Anonymität zu wahren, bereits berücksichtigt. Der EDSB bedauert jedoch, dass einige dieser Bestimmungen ungenau, mehrdeutig oder allgemein sind, und empfiehlt daher eine Reihe von Änderungen, um den datenschutzbezogenen Inhalt des Vorschlags zu verbessern.

⁽¹⁾ Stellungnahme des EDSB vom 2. Dezember 2008 zum Vorschlag für eine Richtlinie über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung.

⁽²⁾ Zu pseudonymisierten und verschlüsselten Daten siehe Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe, S. 21.

47. Zunächst stellt der EDSB fest, dass die in dem Vorschlag verwendeten Begriffe „Rückverfolgbarkeit“ und „Anonymität“ im Widerspruch zueinander stehen. Hier empfiehlt er konkrete Änderungen der Formulierungen in einigen Teilen des Vorschlags (speziell in Erwägungsgrund 16, Artikel 10 Absatz 2 und Artikel 17), um Mehrdeutigkeit zu vermeiden und deutlich zum Ausdruck zu bringen, dass die Daten nicht anonym sind, sondern nach strengen Vertraulichkeits- und Sicherheitsvorschriften verarbeitet werden sollten.
48. Außerdem empfiehlt er, die Notwendigkeit, strenge Sicherheitsmaßnahmen auf nationaler Ebene anzunehmen, stärker herauszustellen. Dies könnte durch die Aufnahme eines zweiten Absatzes in Artikel 16, in dem die Grundprinzipien für die Gewährleistung der Sicherheit auf Ebene der Mitgliedstaaten beschrieben werden, und durch eine detailliertere Auflistung dieser Prinzipien als Teil der Durchführungsmaßnahmen von Artikel 25 Absatz 1 geschehen. Es werden folgende Sicherheitsprinzipien vorgeschlagen:
- a) Annahme einer Informationssicherheitspolitik, um in Bezug auf personenbezogene Daten von Spendern und Empfängern Vertraulichkeit, Integrität, Rechenschaftspflicht und Verfügbarkeit zu gewährleisten;
 - b) Festlegung einer speziellen Strategie für die Vertraulichkeit und die Zugriffskontrolle, begleitet von Garantien für die Vertraulichkeit der Daten für die an der Verarbeitung beteiligten Personen;
 - c) Berücksichtigung von Sicherheitsmechanismen in den nationalen Datenbanken nach dem Grundsatz des „eingebauten Datenschutzes“ (privacy by design);
 - d) Festlegung von Verfahren, um die Datenschutzrechte von Spendern und Empfängern, insbesondere das Zugriffs- und Berichtigungsrecht und das Recht auf Information, zu garantieren, wobei besonderes Augenmerk auf Fälle zu richten ist, in denen Spender ihre Zustimmung widerrufen wollen oder nicht als Spender akzeptiert werden;
 - e) Erlass von Maßnahmen, um die Integrität und ununterbrochene Verfügbarkeit der Daten zu gewährleisten;
 - f) Gewährleistung regelmäßiger Kontrollen und unabhängiger Audits der bestehenden Sicherheitsstrategien.
49. In Bezug auf den grenzüberschreitenden Organaustausch empfiehlt der EDSB, dass die Notwendigkeit einer Harmonisierung der Informationssicherheitspolitik der Mitgliedstaaten in Erwägungsgrund 17 des Vorschlags erwähnt wird. Außerdem sollte besonderes Augenmerk darauf gerichtet werden, welche Pseudonymisierungsmöglichkeiten zur Identifizierung der Spender und Empfänger genutzt werden und dass die Interoperabilität mit dem Identifikationssystem für Gewebe und Zellen gewahrt bleibt. Der EDSB empfiehlt, dass in Artikel 25 Absatz 1 Buchstabe b ein spezieller Verweis auf dieses Thema erfolgt.
50. Was den Organaustausch mit Drittländern anbelangt, so empfiehlt der EDSB, in Artikel 21 oder in dem entsprechenden Erwägungsgrund 15 des Vorschlags zu erwähnen, dass die zuständige Behörde sich mit der nationalen Datenschutzbehörde abstimmen wird, um den notwendigen Rahmen für die sichere, aber auch schnelle und effiziente Übermittlung von organbezogenen Daten an Drittländer und aus Drittländern zu entwickeln.
51. Abschließend empfiehlt der EDSB, dass immer dann, wenn den Datenschutz und die Datensicherheit betreffende Durchführungsmaßnahmen geprüft werden, alle relevanten Akteure, einschließlich des EDSB und der Artikel-29-Datenschutzgruppe, konsultiert werden.

Geschehen zu Brüssel am 5. März 2009.

Peter HUSTINX

Europäischer Datenschutzbeauftragter