01248/07/DE
WP 136

Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“

Angenommen am 20. Juni

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie sowie Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf Artikel 255 EG-Vertrag und auf die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission,

gestützt auf ihre Geschäftsordnung,

HAT DIESE STELLUNGNAHME ANGENOMMEN:

[1] ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. EINLEITUNG

Die Datenschutzgruppe ist sich der Notwendigkeit einer gründlichen Analyse des Begriffs „personenbezogene Daten“ bewusst. Die Informationen über die gegenwärtige Praxis in den EU-Mitgliedstaaten deuten auf gewisse Unsicherheiten und Unterschiede in Bezug auf wichtige Aspekte dieses Begriffs hin, die das bestimmungsgemäße Funktionieren des bestehenden Datenschutzrahmens in verschiedenen Zusammenhängen beeinträchtigen könnten. Das Ergebnis dieser Analyse, die sich auf ein zentrales Element für die Anwendung und Auslegung der Datenschutzbestimmungen konzentriert, hat unweigerlich tief greifende Auswirkungen auf eine Reihe wichtiger Aspekte und ist von besonderer Bedeutung für Themen wie Identitätsmanagement im Zusammenhang mit elektronischen Behördendiensten (E-Government), Online-Gesundheitsfürsorge (E-Health) und der RFID-Technik.

Mit ihrer Stellungnahme will die Datenschutzgruppe eine gemeinsame Verständnisgrundlage für den Begriff „personenbezogene Daten“, die Situationen, in denen nationale Datenschutzgesetze anzuwenden sind, und die Art ihrer Anwendung schaffen. Bei der Erarbeitung einer gemeinsamen Definition für den Begriff „personenbezogene Daten“ wird der Rahmen für den Geltungsbereich der Datenschutzbestimmungen abgesteckt. Außerdem werden Leitlinien für die Anwendung nationaler Datenschutzbestimmungen auf typische Situationen erarbeitet, wie sie in ganz Europa auftreten. Dadurch trägt die Artikel-29-Datenschutzgruppe entsprechend ihrem Mandat zur einheitlichen Anwendung dieser Regelwerke bei.

Zur Untermauerung und Veranschaulichung der Analyse werden Beispiele aus der innerstaatlichen Praxis europäischer Datenschutzbehörden herangezogen. Die meisten Beispiele wurden für diesen Verwendungszweck nur geringfügig bearbeitet.

II. ALLGEMEINE ÜBERLEGUNGEN UND KONZEPTIONELLE ASPEKTE

Die Richtlinie enthält eine weit gefasste Definition für personenbezogene Daten.

In der Richtlinie 95/46/EG (nachstehend „die Datenschutzrichtlinie" oder „die Richtlinie") werden personenbezogene Daten folgendermaßen definiert:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck a) „personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind".

An dieser Stelle ist anzumerken, dass diese Definition die Absicht des europäischen Gesetzgebers widerspiegelt, den Begriff „personenbezogene Daten" im gesamten Rechtsetzungsprozess möglichst weit zu fassen. Im ursprünglichen Vorschlag der Kommission wurde dargelegt, dass wie in der Übereinkunft 108 eine weit gefasste Definition angenommen wird, um alle Informationen mit einzubeziehen, die mit einer Person in Verbindung gebracht werden können.[2] Im geänderten Vorschlag der Kommission wurde angemerkt, dass der geänderte Vorschlag dem Wunsch des Parlaments entspricht, die Definition für „personenbezogene Daten" so allgemein wie möglich zu halten, damit alle Informationen über eine bestimmbare Person berücksichtigt werden.[3] Diesem Wunsch hat der Rat in seinem gemeinsamen Standpunkt entsprochen.[4]

Die Datenschutzbestimmungen in der Richtlinie dienen dem Schutz natürlicher Personen.

Artikel 1 der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG legen den Zweck der darin enthaltenen Datenschutzbestimmungen eindeutig dar: Schutz der Grundrechte und Grundfreiheiten und insbesondere Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Es ist sehr wichtig, dass dieser Aspekt bei der Auslegung und Anwendung der Vorschriften beider Rechtsinstrumente gebührend berücksichtigt wird. Er kann eine wesentliche Rolle bei der Beurteilung spielen, wie die Bestimmungen der Richtlinie auf verschiedene Situationen anzuwenden sind, in denen die Rechte natürlicher Personen nicht bedroht sind, und er kann vor einer Auslegung derselben Bestimmungen warnen, die natürlichen Personen den Schutz ihrer Rechte entziehen würde.

---

2 COM (90) 314 final, 13.9.1990, S. 19 (Erläuterung zu Artikel 2).
3 COM (92) 422 final, 28.10.1992, S. 10 (Erläuterung zu Artikel 2).
4 Gemeinsamer Standpunkt (EG) Nr. 1/95 vom Rat festgelegt am 20. Februar 1995, ABl. C 93 vom 13.4.1995, S. 20.

Die Richtlinie schließt in ihrem Anwendungsbereich eine Reihe von Tätigkeiten aus und sieht einen gewissen Handlungsspielraum vor, um eine den jeweiligen Umständen angemessene rechtliche Reaktion zu ermöglichen.

Trotz der in der Richtlinie weit gefassten Definition für „personenbezogene Daten“ und „Verarbeitung“ kann allein aus der Tatsache, dass eine bestimmte Situation die „Verarbeitung personenbezogener Daten“ im Sinne der Definition einschließt, nicht automatisch gefolgert werden, dass für diese Situation die Bestimmungen der Richtlinie, insbesondere Artikel 3, gelten. Abgesehen von den Ausnahmen aufgrund des Geltungsbereichs des Gemeinschaftsrechts berücksichtigen die Ausnahmen in Artikel 3 den technischen Aspekt der Verarbeitung (in nicht automatisierter und nicht strukturierter Form) und den vorgesehenen Verwendungszweck (von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten). Selbst wenn die Verarbeitung personenbezogener Daten in den Anwendungsbereich der Richtlinie fällt, sind nicht unbedingt alle darin enthaltenen Bestimmungen auf die konkrete Situation anzuwenden. Eine Reihe von Bestimmungen der Richtlinie bieten ein hohes Maß an Flexibilität, damit ein Mittelweg zwischen dem Schutz der Rechte betroffener Personen und den berechtigten Interessen der für die Verarbeitung Verantwortlichen, von Dritten und dem gegebenenfalls bestehenden öffentlichen Interesse gefunden werden kann. Solche Bestimmungen finden sich beispielsweise in Artikel 6 (Aufbewahrungsdauer abhängig vom Zweck der Daten), in Artikel 7 Buchstabe f (Abwägung der berechtigten Interessen bei der Verarbeitung), im letzten Absatz von Artikel 10 Buchstabe c und in Artikel 11 Absatz 1 Buchstabe c (Übermittlung von Informationen an die betroffene Person zur Gewährleistung einer Verarbeitung nach Treu und Glauben) oder in Artikel 18 (Ausnahmen von der Meldepflicht), um nur einige Beispiele zu nennen.

Der Anwendungsbereich der Datenschutzbestimmungen sollte nicht zu stark ausgeweitet werden.

Ein nicht erwünschtes Ergebnis wäre die Anwendung der Datenschutzbestimmungen auf Situationen, für die diese Bestimmungen nicht gelten sollten und die vom Gesetzgeber als mögliche Anwendungsbereiche auch nicht in Betracht gezogen wurden. Die wesentlichen Ausnahmen im oben genannten Artikel 3 und die Klarstellungen in den Erwägungsgründen 26 und 27 der Richtlinie zeigen, wie sich der Gesetzgeber den Datenschutz in der Praxis vorstellt.

Eine Einschränkung betrifft die Art der Datenverarbeitung. Vor diesem Hintergrund ist daran zu erinnern, dass die ersten Datenschutzgesetze in den 70er Jahren erlassen wurden, weil neue Techniken zur elektronischen Datenverarbeitung einen leichteren und umfassenderen Zugriff auf personenbezogene Daten als die konventionellen Verfahren der Datenverarbeitung ermöglichten. Folglich ist der Datenschutz im Rahmen der Richtlinie auf den Schutz vor Formen der Verarbeitung ausgerichtet, die für den „leichten Zugriff auf die Daten“ und die damit einhergehenden Risiken typisch sind (Erwägungsgrund 27). Die Richtlinie gilt nur dann für die nicht automatisierte Verarbeitung personenbezogener Daten, wenn die Daten in einer Datei gespeichert sind oder gespeichert werden sollen (Artikel 3).

Eine weitere allgemeine Einschränkung für die Anwendung des Datenschutzes im Rahmen der Richtlinie betrifft die Verarbeitung von Daten in Situationen in denen Mittel, die „vernünftigerweise […] eingesetzt werden könnten“ nicht zum Einsatz

kommen, um die betreffende Person zu bestimmen (Erwägungsgrund 26). Dieser Punkt wird weiter unten erörtert.

Die Definition für personenbezogene Daten sollte aber auch nicht zu restriktiv ausgelegt werden.

Wenn eine rein mechanistische Anwendung jeder einzelnen Bestimmung der Richtlinie auf den ersten Blick zu übermäßig bürokratischen oder gar absurden Konsequenzen führen würde, ist zunächst Folgendes zu prüfen: 1) Fällt die Situation in den Anwendungsbereich der Richtlinie, insbesondere im Hinblick auf Artikel 3? 2) Wenn ja, sieht die Richtlinie selbst bzw. sehen die zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Rechtsvorschriften Ausnahmen oder Vereinfachungen in bestimmten Situationen vor, um eine angemessene rechtliche Reaktion bei gleichzeitigem Schutz der Rechte natürlicher Personen sowie der berechtigten Interessen zu ermöglichen? Es gilt also, eine übermäßig restriktive Auslegung der Definition für personenbezogene Daten zu vermeiden und sich dafür zu vergegenwärtigen, dass ein beträchtlicher Handlungsspielraum für die Anwendung der Bestimmungen auf personenbezogene Daten vorhanden ist.

Die nationalen Kontrollstellen für den Datenschutz spielen bei der Überwachung der Anwendung der Datenschutzgesetze eine zentrale Rolle und sind im Rahmen ihres Mandats auch für die Auslegung der Rechtsvorschriften und die Ausarbeitung konkreter Leitlinien für die für die Verarbeitung Verantwortlichen und die betroffenen Personen zuständig. Sie sollten sich für eine Definition einsetzen, die so weit gefasst ist, dass sie künftige Entwicklungen antizipieren kann und alle „Grauzonen“ in ihrem Anwendungsbereich erfasst, und zugleich den in der Richtlinie vorgesehenen rechtlichen Spielraum voll ausschöpft. Der Richtlinientext ermutigt in der Tat zur Entwicklung eines Konzepts, das eine weit gefasste Auslegung des Begriffs „personenbezogene Daten“ mit einem angemessenen Mittelweg bei der Anwendung der Bestimmungen der Richtlinie verbindet.

III. ANALYSE DER DEFINITION FÜR PERSONENBEZOGENE DATEN IM SINNE DER DATENSCHUTZRICHTLINIE

Die Begriffsbestimmung in der Richtlinie enthält vier Hauptbausteine, die für die Zwecke des vorliegenden Arbeitspapiers einzeln analysiert werden. Hierbei handelt es sich um die folgenden Bausteine:

- „alle Informationen“
- „über“
- „eine bestimmte oder bestimmbare“
- „natürliche Person“

Diese vier Bausteine sind eng miteinander verknüpft und beeinflussen sich wechselseitig. Wegen der diesem Arbeitspapier zugrunde liegenden Methodik werden die einzelnen Bausteine jedoch getrennt analysiert.

1. ERSTES ELEMENT: „ALLE INFORMATIONEN“

Mit dem Ausdruck „alle Informationen“ in der Richtlinie setzt der Gesetzgeber ein klares Signal für seine Bereitschaft, den Begriff „personenbezogene Daten“ möglichst weit zu fassen. Dieser Wortlaut verlangt eine großzügige Auslegung.

Was die Art der Informationen anbetrifft, schließt der Begriff „personenbezogene Daten“ alle Arten von Aussagen über eine Person ein. Er umfasst „objektive“ Informationen, etwa das Vorhandensein einer bestimmten Substanz im Blut, aber auch „subjektive“ Informationen, Meinungen oder Beurteilungen. Auf diese zweite Art von Informationen entfällt ein erheblicher Anteil der personenbezogenen Daten, die in Wirtschaftszweigen wie dem Bankwesen zur Beurteilung der Kreditwürdigkeit von Bankkunden („Titius ist ein zuverlässiger Kreditnehmer“), im Versicherungswesen („Es ist nicht davon auszugehen, dass Titius bald sterben wird“) oder im Berufsleben („Titius ist ein guter Arbeitnehmer und hat eine Beförderung verdient“) verarbeitet werden.

Informationen brauchen nicht unbedingt wahr oder bewiesen zu sein, damit sie als „personenbezogene Daten“ eingestuft werden. Die Datenschutzbestimmungen ziehen bereits die Möglichkeit nicht korrekter Informationen in Betracht und räumen einer Person das Recht auf Auskunft über die sie betreffenden Informationen und Widerspruch durch Einlegen einschlägiger Rechtsmittel ein.[5]

Was den Inhalt der Informationen anbetrifft, schließt der Begriff „personenbezogene Daten“ Daten ein, die alle Arten von Informationen vermitteln. Dazu gehören zum einen personenbezogene Daten, die aufgrund spezifischer Risiken als „sensible“ Daten gemäß Artikel 8 der Richtlinie anzusehen sind, zum anderen aber auch allgemeinere Arten von Informationen. Der Begriff „personenbezogene Daten“ umfasst Informationen, die das Privat- und Familienleben der Person im strengen Sinn berühren, aber auch Informationen über alle Arten von Aktivitäten der Person, etwa im Zusammenhang mit Arbeitsbeziehungen oder ihrem ökonomischen oder sozialen Verhalten. Er umfasst folglich Informationen über Personen unabhängig von ihrer Position oder Funktion (als Verbraucher, Patient, Mitarbeiter, Kunde usw.).

Beispiel 1: Berufliche Gepflogenheiten und Praktiken

Informationen zu Arzneimittelrezepten (z. B. Kennnummer des Arzneimittels, Name, Wirkstoffgehalt, Hersteller, Verkaufspreis, neue Packung oder Nachfüllpackung, Gründe für die Verwendung, Gründe für den Verzicht auf Generika, Vor- und Nachname des verordnenden Arztes, Telefonnummer usw.), ob nun in Form eines Einzelrezepts oder in Form von Mustern, die aus mehreren Rezepten erkennbar sind, können auch dann als personenbezogene Daten über den das Rezept ausstellenden Arzt angesehen werden, wenn der Patient anonym ist. Somit ist die Bereitstellung von Informationen zu Rezepten, die von bestimmten oder bestimmbaren Ärzten für Hersteller rezeptpflichtiger Arzneimittel ausgestellt werden, als Übermittlung personenbezogener Daten an Dritte im Sinne der Richtlinie anzusehen.

Diese Auslegung wird durch den Wortlaut der Datenschutzrichtlinie untermauert. Einerseits ist zu berücksichtigen, dass der Begriff „Privat- und Familienleben“ weit

[5] Eine Berichtigung könnte in Form einer Stellungnahme zu den falschen Aussagen oder durch Einlegen einschlägiger Rechtsmittel wie Beschwerdeverfahren erwirkt werden.

gefasst ist, wie der Europäische Gerichtshof für Menschenrechte deutlich gemacht hat.[6] Andererseits gehen die Vorschriften für den Schutz personenbezogener Daten über den Schutz des weit gefassten Begriffs „Recht auf Achtung des Privat- und Familienlebens“ hinaus. Zu erwähnen ist auch, dass die Charta der Grundrechte der Europäischen Union den Schutz personenbezogener Daten in Artikel 8 als eigenständiges Recht verankert, das unabhängig vom Recht auf Achtung des Privatlebens gemäß Artikel 7 gilt, und Gleiches auf einzelstaatlicher Ebene in einigen Mitgliedstaaten gilt. Dies steht im Einklang mit Artikel 1 Absatz 1, der auf den Schutz „der Grundrechte und Grundfreiheiten und *insbesondere* [jedoch nicht ausschließlich] den Schutz der Privatsphäre natürlicher Personen“ ausgerichtet ist. Die Richtlinie bezieht sich also insbesondere auf die Verarbeitung personenbezogener Daten außerhalb des Privat- und Familienlebens, etwa auf dem Gebiet des Arbeitsrechts (Artikel 8 Absatz 2 Buchstabe b), strafrechtlicher Verurteilungen, verwaltungsrechtlicher Sanktionen oder Urteile in Zivilprozessen (Artikel 8 Absatz 5) oder der Direktwerbung (Artikel 14 Buchstabe b). Der Europäische Gerichtshof unterstützt diesen weit gefassten Ansatz.[7]

Was das Format oder den Träger der Informationen anbetrifft, schließt der Begriff „personenbezogene Daten“ in alphabetischer, numerischer, grafischer, fotografischer, akustischer oder in sonstiger Form vorliegende Informationen ein. Dies umfasst sowohl Informationen auf Papier als auch Informationen, die auf einem Computer in binärer Form oder beispielsweise auf einem Videoband gespeichert sind. Dies ergibt sich zwangsläufig aus der Aufnahme der automatisierten Verarbeitung personenbezogener Daten in den Geltungsbereich der Richtlinie. Unter diesem Aspekt sind vor allem Ton- und Bilddaten als personenbezogene Daten zu betrachten, weil sie Informationen über eine natürliche Person darstellen können. Insofern ist die ausdrückliche Erwähnung von Bild- und Tondaten in Artikel 33 der Richtlinie als Bestätigung und Klarstellung zu verstehen, dass diese Art von Daten definitiv in ihren Geltungsbereich fällt (sofern auch alle anderen Voraussetzungen erfüllt sind) und die Richtlinie folglich auf sie Anwendung findet. Dies ist auch eine folgerichtige Annahme für die in diesem Artikel enthaltene Bestimmung, die eine Beurteilung anstrebt, ob die Richtlinie eine angemessene rechtliche Reaktion in diesen Bereichen ermöglicht. Dieser Punkt wird im Erwägungsgrund 14 weiter ausgeführt, in dem es heißt: „*In Anbetracht der Bedeutung der gegenwärtigen Entwicklung im Zusammenhang mit der Informationsgesellschaft bezüglich Techniken der Erfassung, Übermittlung, Veränderung, Speicherung, Aufbewahrung oder Weitergabe von personenbezogenen Ton- und Bilddaten muss diese Richtlinie auch auf die Verarbeitung dieser Daten Anwendung finden.*“ Andererseits brauchen Informationen nicht unbedingt in einer strukturierten Datenbank oder Datei gespeichert zu sein, um als personenbezogene

---

[6] Im Urteil des Europäischen Gerichtshofs für Menschenrechte in der Rechtssache Amann gegen die Schweiz vom 16.2.2000, heißt es in § 65, dass [...] der Begriff Privatleben nicht eng ausgelegt werden darf. Vielmehr gehöre zum Recht auf Achtung des Privatlebens auch das Recht, Beziehungen zu anderen Menschen herzustellen und zu entfalten; daher könne man das Berufsleben nicht vom „Privatleben“ abgrenzen (siehe das Urteil Niemietz gegen Deutschland vom 16. Dezember 1992, Serie A Nr. 251-B, S. 33-34, § 29, und das oben zitierte Urteil in der Rechtssache Halford, S. 1015-16, § 42). Diese weit gefasste Auslegung entspricht der Auslegung des Europarats im Übereinkommen vom 28. Januar 1981.

[7] Urteil des Europäischen Gerichtshofs (Rechtssache C-101/01) vom 6.11.2003 (Lindqvist), Randnr. 24: *„Der in Artikel 3 Absatz 1 der Richtlinie 95/46 verwendete Begriff personenbezogene Daten bezieht sich nach der Definition ihres Artikel 2 Buchstabe a auf alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Dieser Ausdruck erfasst eindeutig die Nennung des Namens einer Person in Verbindung mit deren Telefonnummern oder mit Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen.“*

Daten betrachtet zu werden. Auch im Freitext eines elektronischen Dokuments enthaltene Informationen können als personenbezogene Daten gelten, sofern sie die übrigen Kriterien in der Definition für personenbezogene Daten erfüllen. Beispielsweise enthalten auch elektronische Nachrichten personenbezogene Daten.

Beispiel 2: Telefonbanking:

Beim Telefonbanking werden die Anweisungen, die der Kunde seiner Bank mündlich erteilt, auf Band aufgezeichnet. Diese aufgezeichneten Anweisungen sind als personenbezogene Daten anzusehen.

Beispiel 3: Videoüberwachung

Die Bilder von Personen, die von einem Videoüberwachungssystem erfasst werden, können als personenbezogene Daten angesehen werden, wenn die Personen zu erkennen sind.

Beispiel 4: Zeichnung eines Kindes

Bei einem Sorgerechtsverfahren wird eine Zeichnung vorgelegt, die ein Mädchen bei einem neuropsychiatrischen Test von seiner Familie angefertigt hat. Die Zeichnung enthält Informationen über die psychische Verfassung des Mädchens und über seine Einstellung zu verschiedenen Familienmitgliedern. Die Zeichnung könnte also der Kategorie „personenbezogene Daten“ zugerechnet werden, weil sie Informationen über das Kind (seine gesundheitliche Verfassung aus Sicht eines Psychiaters) sowie über das Verhalten seines Vaters oder seiner Mutter enthält. Daher können die Eltern in diesem Fall von ihrem Recht auf Zugang zu diesen spezifischen Informationen Gebrauch machen.

Besonderes Augenmerk ist hier auf biometrische Daten zu richten. Sie können als biologische Eigenschaften, physiologische Merkmale, Gesichtszüge oder reproduzierbare Handlungen definiert werden, wobei diese Merkmale und/oder Handlungen für die betreffende Person spezifisch und messbar sind, auch wenn die in der Praxis angewandten Modelle für ihre technische Messung in gewissem Umfang auf Wahrscheinlichkeiten beruhen. Typische Beispiele für biometrische Daten sind Fingerabdrücke, Augennetzhaut, Gesichtsform, Stimme, aber auch Handgeometrie, Venenstruktur oder auch spezielle Fähigkeiten oder sonstige Verhaltensmerkmale (z. B. handgeschriebene Unterschrift, Tastenanschlag, charakteristische Gangart oder Sprechweise usw.).

Eine Besonderheit biometrischer Daten besteht darin, dass sie sowohl als *inhaltliche* Information über eine bestimmte Person („Titius hat diesen Fingerabdruck“) als auch als ein Element zur Herstellung einer *Verbindung* zwischen einer Information und der Person angesehen werden können („Dieser Gegenstand wurde von einer Person mit diesem Fingerabdruck berührt. Dieser Fingerabdruck passt zu Titius; deswegen wurde dieser Gegenstand von Titius berührt.“). Insofern können sie als „Kennzeichen“ dienen. Aufgrund ihrer einzigartigen Verbindung mit einer bestimmten Person können biometrische Daten zur Identifizierung dieser Person verwendet werden. Diese Dualität

gilt auch für DNA-Daten, die Informationen über den menschlichen Körper enthalten und eine eindeutige und zweifelsfreie Identifizierung einer Person ermöglichen.

Auch Proben von menschlichem Gewebe (wie eine Blutprobe) dienen als Quelle für biometrische Daten, doch sie selbst sind keine biometrischen Daten (beispielsweise sind Fingerabdruckmuster biometrische Daten, jedoch nicht der Finger selbst). Daher ist das Extrahieren von Informationen aus Proben als Erhebung personenbezogener Daten einzustufen, die unter die Bestimmungen dieser Richtlinie fällt. Die Sammlung, Aufbewahrung und Verwendung von Gewebeproben kann gesonderten Regelwerken unterliegen.[8]

2. ZWEITES ELEMENT: „ÜBER“

Dieser Baustein in der Definition ist entscheidend, da es sehr wichtig ist, genau zu ermitteln, welche Beziehungen/Verbindungen eine Rolle spielen und wie diese voneinander zu unterscheiden sind.

Allgemein „beziehen“ sich Informationen auf eine Person, wenn es sich um Informationen *über* diese Person handelt.

In vielen Situationen lässt sich diese Beziehung auf einfache Weise herstellen. In der Personalabteilung beispielsweise „beziehen“ sich die in der Personalakte erfassten Daten eindeutig auf die Situation der Person in ihrer Eigenschaft als Mitarbeiter. Gleiches gilt für die Ergebnisdaten eines medizinischen Tests, die im Krankenblatt eines Patienten aufgezeichnet sind, oder für das Bild einer Person, die bei einem Videointerview gefilmt wurde.

Allerdings sind auch viele andere Situationen vorstellbar, in denen nicht so eindeutig wie in den oben genannten Fällen ermittelt werden kann, ob sich die Informationen auf eine Person „beziehen“.

Gelegentlich beziehen sich die von den Daten vermittelten Informationen in erster Linie auf Gegenstände, und nicht auf Personen. Diese Gegenstände gehören in der Regel einer Person, sie können einem bestimmten Einfluss durch oder auf Personen unterliegen oder irgendeine Art von physischer oder räumlicher Nähe zu Personen oder anderen Gegenständen haben. In diesem Fall kann lediglich eine indirekte Beziehung zwischen den Informationen und den Personen oder Gegenständen hergestellt werden.

Beispiel 5: Der Wert einer Immobilie

Der Wert einer Immobilie ist eine Information über einen Gegenstand. Hier finden Datenschutzbestimmungen eindeutig keine Anwendung, wenn die Information ausschließlich dazu verwendet wird, die Immobilienpreise in einem bestimmten Wohngebiet zu veranschaulichen. Unter bestimmten Umständen ist jedoch auch diese Information der Kategorie „personenbezogene Daten“ zuzurechnen. Die Immobilie ist nämlich ein Vermögenswert, der unter anderem zur Festsetzung der vom Eigentümer zu entrichtenden Steuern herangezogen wird. In diesem Kontext ist die Personenbezogenheit dieser Information nicht zu bestreiten.

[8] Siehe Empfehlung Rec (2006)4 des Europarats über Forschung mit humanbiologischem Material, angenommen vom Ministerkomitee am 15. März 2006.

Gleiches gilt für Situationen, in denen sich die Daten in erster Linie auf Prozesse oder Ereignisse beziehen, beispielsweise Informationen über das Funktionieren einer Anlage, die vom Menschen bedient werden muss. Unter bestimmten Umständen sind auch solche Informationen als „personenbezogen“ anzusehen.

Beispiel 6: Kundendienst-Scheckheft für ein Fahrzeug

In einem Kundendienst-Scheckheft werden von einem Automechaniker oder einer Werkstatt Fahrzeugdaten, Tachostand, Kundendiensttermine, technische Probleme und Materialzustand erfasst. Diese Daten werden zusammen mit dem Zulassungskennzeichen und der Motornummer aufgezeichnet, die wiederum mit dem Fahrzeugeigentümer in Verbindung gebracht werden kann. Wenn die Werkstatt bei der Ausstellung der Rechnung einen Bezug zwischen Fahrzeug und Eigentümer herstellt, „beziehen“ sich die Daten auf den Eigentümer oder den Fahrer. Wenn ein Bezug zu dem für die Kundendienstmaßnahmen zuständigen Mechaniker hergestellt wird, um seine Produktivität zu beurteilen, „beziehen“ sich diese Daten auch auf den Mechaniker.

Die Datenschutzgruppe hat sich mit der Frage, wann sich Daten auf eine Person „beziehen“, bereits befasst. Im Zusammenhang mit der Diskussion über Datenschutzfragen bei Verwendung von RFID-Etiketten wies die Datenschutzgruppe auf Folgendes hin: „*Daten beziehen sich auf eine Person, wenn sie die Identität, die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird.*“[9]

Bei den oben erwähnten Sachverhalten könnte mit der gleichen Begründung auch das Argument angeführt werden, dass ein „**Inhaltselement**“ ODER ein „**Zweckelement**“ ODER ein „**Ergebniselement**“ vorhanden sein sollte, damit die Daten als „personenbezogen“ angesehen Werden.

Das „**Inhaltselement**“ ist immer dann vorhanden, wenn – nach dem allgemein üblichen Verständnis des Wortes „beziehen“ – Informationen über eine bestimmte Person gegeben werden, und zwar unabhängig vom Zweck aufseiten des für die Verarbeitung Verantwortlichen oder eines Dritten oder von den Auswirkungen dieser Information auf die betroffene Person. Informationen „beziehen“ sich auf eine Person, wenn es sich um Informationen „über“ diese Person handelt, und dieser Punkt ist unter Berücksichtigung aller Begleitumstände zu beurteilen. Beispielsweise beziehen sich die Ergebnisse einer ärztlichen Untersuchung eindeutig auf den Patienten, und die in einem Firmenordner unter dem Namen eines bestimmten Kunden abgelegten Informationen beziehen sich eindeutig auf diesen Kunden. Ebenso beziehen sich die Informationen auf einem RFID-Etikett oder Strichcode im Personalausweis einer bestimmten Person auf diese Person, und Gleiches wird auch bei den künftigen Reisepässen mit einem RFID-Chip der Fall sein.

Auch ein „**Zweckelement**“ kann dazu führen, dass sich Informationen auf eine bestimmte Person „beziehen“. Ein solches „Zweckelement“ gilt als gegeben, wenn die Daten unter Berücksichtigung aller Begleitumstände mit dem Zweck verwendet

[9] Arbeitspapier WP 105 der Datenschutzgruppe: Datenschutzfragen im Zusammenhang mit der RFID-Technik, angenommen am 19.1.2005, S. 9.

werden bzw. verwendet werden könnten, eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen.

Beispiel 7: Anrufliste

Die Anrufliste in einem Firmenbüro enthält Informationen über die Anrufe von einem Telefonapparat, der mit einem bestimmten Teilnehmeranschluss verbunden ist. Anhand dieser Informationen kann eine Beziehung zu verschiedenen Personen hergestellt werden. Der Teilnehmeranschluss wurde für die Firma eingerichtet, und die Firma ist vertraglich dazu verpflichtet, für die Kosten der Gespräche aufzukommen. Der Telefonapparat steht während der Geschäftszeiten unter der Kontrolle eines bestimmten Mitarbeiters, und es ist davon auszugehen, dass die Gespräche von ihm geführt werden. Die Anrufliste kann auch Informationen über die angerufene Person enthalten. Außerdem kann das Telefon von jeder Person benutzt werden, die bei Abwesenheit des Mitarbeiters Zugang zum Gebäude erhält (z. B. Reinigungspersonal). Zwischen den Informationen über die Benutzung dieses Telefonapparats und dem Unternehmen, Mitarbeiter oder Reinigungspersonal kann für verschiedene Zwecke (beispielsweise zur Kontrolle der Uhrzeit, zu der das Reinigungspersonal das Bürogebäude verlässt, da es diese vor dem Abschließen des Gebäudes telefonisch durchgeben muss) ein Bezug hergestellt werden. In diesem Fall sind sowohl ankommende als auch abgehende Anrufe als „personenbezogene Daten“ anzusehen, weil alle Anrufe Informationen über das Privatleben, soziale Beziehungen und Mitteilungen enthalten.

Eine dritte Art von „Beziehung“ zu bestimmten Personen entsteht, wenn ein „**Ergebniselement**“ vorhanden ist. Auch wenn kein „Inhaltselement“ oder „Zweckelement“ vorhanden ist, können Daten als „personenbezogen“ angesehen werden, weil sich ihre Verwendung unter Berücksichtigung aller jeweiligen Begleitumstände auf die Rechte und Interessen einer bestimmten Person auswirken könnte. Dabei ist anzumerken, dass es sich bei dem möglichen Ergebnis nicht unbedingt um nachhaltige Auswirkungen handeln muss. Es reicht aus, wenn die Person aufgrund der Verarbeitung solcher Daten anders als andere Personen behandelt werden könnte.

Beispiel 8: Die Standortüberwachung von Taxis zur Verbesserung der Servicequalität hat Auswirkungen auf die Taxifahrer.

Ein Taxiunternehmen richtet ein Satellitenortungssystem ein, das den Standort der verfügbaren Taxis in Echtzeit ermitteln kann. Dabei wird jedem Kunden, der ein Taxi ruft, das in seiner Nähe befindliche Fahrzeug zugewiesen, wodurch der Service verbessert und Kraftstoff eingespart wird. Genau genommen geht es bei den für dieses System benötigten Daten um Daten über Fahrzeuge, und nicht um Daten über Taxifahrer. Der Zweck der Verarbeitung besteht nicht in der Beurteilung der Leistung von Taxifahrern, etwa durch Optimierung ihrer Fahrstrecken. Allerdings kann mit dem System auch die Leistung der Taxifahrer überwacht und kontrolliert werden, ob sie Geschwindigkeitsbegrenzungen einhalten, geeignete Fahrstrecken auswählen, hinter dem Lenkrad sitzen oder sich im Freien aufhalten usw. Somit kann das System erhebliche Auswirkungen auf diese Personen haben, und insofern können die Daten als Daten über natürliche Personen angesehen werden. Daher sollte die Verarbeitung Datenschutzbestimmungen unterliegen.

Die drei genannten Elemente (Inhalt, Zweck, Ergebnis) sind als alternative, nicht als kumulative Bedingungen anzusehen. Insbesondere bei Vorhandensein des inhaltlichen

Elements brauchen die anderen Elemente nicht vorhanden zu sein, damit die Daten als personenbezogen angesehen werden können. Daraus folgt, dass sich ein und dieselbe Information auf verschiedene Personen gleichzeitig beziehen kann, je nachdem, welches Element im Hinblick auf jede Person vorhanden ist. Eine bestimmte Information kann sich auf die Person Titius wegen des „Inhaltselements“ (es sind eindeutig Daten über Titius) UND auf Gaius wegen des „Zweckelements“ (sie wird benutzt, um Gaius in einer bestimmten Weise zu behandeln) UND auf Sempronius wegen des „Ergebniselements“ (sie kann sich auf die Rechte und Interessen von Sempronius auswirken) beziehen. Dies bedeutet auch, dass sich die Daten nicht unbedingt auf eine Person „konzentrieren“ müssen, damit sie als auf sie bezogen angesehen werden. Die obige Analyse zeigt, dass die Frage, ob sich Daten auf eine bestimmte Person beziehen, für jedes spezifische Datenelement gesondert beantwortet werden muss. Ebenso ist bei der Anwendung materiellrechtlicher Bestimmungen (beispielsweise in Bezug auf den Umfang des Auskunftsrechts) zu beachten, dass sich Informationen auf verschiedene Personen beziehen können.

Beispiel 9: In einem Sitzungsprotokoll enthaltene Informationen

Ein Beispiel für die Notwendigkeit, die obige Analyse für jede Information gesondert durchzuführen, zeigt der folgende Fall, in dem es um die in einem Sitzungsprotokoll enthaltenen Informationen geht. Der Schriftführer Sempronius protokolliert die Anwesenheit der Teilnehmer Titius, Gaius und Sempronius, die Aussagen von Titius und Gaius sowie das weitere Vorgehen bei bestimmten Themen. In Bezug auf Titius ist lediglich die Information, dass er an der Sitzung zu einer bestimmten Uhrzeit und an einem bestimmten Ort teilgenommen und bestimmte Aussagen gemacht hat, als „personenbezogen“ anzusehen. Die von Sempronius protokollierte Anwesenheit von Gaius auf der Sitzung, seine Aussagen und das weitere Vorgehen in einer bestimmten Sache sind KEINE personenbezogenen Daten über Titius. Dies gilt auch dann, wenn diese Information im selben Dokument enthalten ist und selbst wenn Titius das auf der Sitzung erörterte Thema aufgeworfen hat. Somit darf Titius, wenn er sein Auskunftsrecht für die ihn betreffenden personenbezogenen Daten in Anspruch nimmt, keine Auskunft über diese letztgenannten Informationen erhalten. Ob und in welchem Umfang die Informationen als personenbezogene Daten über Gaius und Sempronius anzusehen sind, muss gesondert anhand der oben beschriebenen Analyse ermittelt werden.

3. DRITTES ELEMENT: „EINE BESTIMMTE ODER BESTIMMBARE“ [NATÜRLICHE PERSON]

Laut der Richtlinie müssen sich die Informationen auf eine bereits „bestimmte oder bestimmbare“ natürliche Person beziehen. Dies wirft folgende Überlegungen auf.

Allgemein ist eine natürliche Person als „bestimmte Person“ anzusehen, wenn sie sich in einer Personengruppe von allen anderen Mitgliedern der Gruppe unterscheidet. Folglich ist die natürliche Person „bestimmbar“, wenn grundsätzlich die Möglichkeit besteht, ihre Identität festzustellen (dies ist die Bedeutung des Suffixes „-bar“), auch wenn dies noch nicht geschehen ist. Daher ist diese zweite Alternative in der Praxis die Grenzbedingung, die darüber entscheidet, ob die Information in den Anwendungsbereich des dritten Elements fällt.

Die Identifizierung erfolgt gewöhnlich anhand spezifischer Informationen, die als „Kennzeichen“ bezeichnet werden können und in einer besonderen und engen

Beziehung zu der betreffenden Person stehen. Beispiele dafür sind äußere Erscheinungsmerkmale der Person wie Körpergröße, Haarfarbe, Kleidung usw. oder eine Eigenschaft, die nicht auf Anhieb erkennbar ist, wie etwa ein Beruf, eine Funktion, ein Name usw. Die Richtlinie erwähnt diese „Kennzeichen" in der Definition für „personenbezogene Daten" in Artikel 2. Darin heißt es, dass eine natürliche Person *„direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind."*

„Direkt" oder „indirekt" bestimmbar

Nähere Ausführungen dazu finden sich in der Erläuterung zu den Artikeln im geänderten Vorschlag der Kommission, in der es heißt, dass eine Person direkt durch ihren Namen oder indirekt durch eine Telefonnummer, ein Autokennzeichen, eine Sozialversicherungsnummer, eine Reisepassnummer oder durch eine Kombination wesentlicher Kriterien identifiziert werden kann, die durch Eingrenzung der Gruppe (Alter, Beruf, Wohnort usw.), zu der die Person gehört, ihre Wiedererkennung ermöglichen. Diese Aussage zeigt klar, dass der Grad, der für die Identifizierung als ausreichend beurteilt wird, vom Kontext der jeweiligen Situation abhängt. Ein sehr häufig vorkommender Familienname reicht zur Identifizierung einer Person aus der Gesamtheit der Landesbevölkerung nicht aus, während ein Schüler einer Klasse vermutlich anhand seines Familiennamens identifiziert werden kann. Selbst Begleitinformationen, wie „der Mann im schwarzen Anzug" könnten auf einen bestimmten der an einer Fußgängerampel stehenden Passanten zutreffen. Daher hängt die Identifizierbarkeit der Person, auf die sich die Information bezieht, von den jeweiligen Umständen ab.

Bei „direkt" bestimmten oder bestimmbaren Personen ist der **Name** der Person in der Tat das häufigste Kennzeichen, und in der Praxis ist mit dem Begriff „bestimmte Person" meistens eine Bezugnahme auf den Namen der Person verbunden.

Zur Feststellung der Identität muss der Name der Person mitunter mit anderen Informationen (Geburtsdatum, Namen der Eltern, Adresse oder Fotografie des Gesichts) kombiniert werden, um Verwechslungen zwischen dieser Person und Personen mit gleichem Namen auszuschließen. Beispielsweise ist die Information, dass Titius einen bestimmten Geldbetrag schuldet, auf eine bestimmte Person bezogen anzusehen, weil sie mit dem Namen der Person verbunden ist. Der Name ist eine Information, die besagt, dass eine Person eine bestimmte Kombination von Buchstaben und Lauten verwendet, um sich von anderen Personen zu unterscheiden, zu denen sie Beziehungen unterhält. Der Name kann auch als Ausgangspunkt für Informationen über den Wohn- oder Aufenthaltsort, Familienangehörige (durch den Familiennamen) sowie verschiedene rechtliche und soziale Beziehungen verwendet werden, die mit dem Namen in Verbindung stehen (Bildungseinrichtungen, Krankenblätter, Bankkonten). Unter Umständen kann eine Person sogar wiedererkannt werden, wenn ihr Bild mit ihrem Namen in Verbindung gebracht wird. All diese neuen, mit dem Namen verbundenen Informationen könnten einen Rückschluss auf die lebende Person erlauben, und folglich ist die ursprüngliche Information anhand von Kennzeichen mit einer natürlichen Person verbunden, die von anderen Personen unterschieden werden kann.

Die Kategorie „indirekt bestimmte oder bestimmbare Personen“ bezieht sich typischerweise auf das Phänomen „einzigartiger Kombinationen“ gleich welcher Größe. Auch wenn der Umfang der vorhandenen Kennzeichen auf Anhieb keinen Rückschluss auf eine bestimmte Person erlaubt, könnte diese Person dennoch „bestimmbar“ sein, weil diese Information in Verbindung mit anderen Informationen (unabhängig davon, ob diese vom für die Verarbeitung Verantwortlichen gespeichert werden oder nicht) eine Unterscheidung dieser Person von anderen Personen ermöglicht. Genau an diesem Punkt setzt diese Richtlinie mit „einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“ an. Manche Eigenschaften sind so selten, dass eine Person mühelos bestimmt werden kann („derzeitiger spanischer Ministerpräsident“), doch auch eine Kombination von bestimmten Details (Altersgruppe, regionale Herkunft usw.) kann mitunter sehr aufschlussreich sein, besonders wenn eine Person Zugang zu irgendwelchen weiteren Informationen besitzt. Dieses Phänomen wurde von den Statistikern, die stets darauf bedacht sind, strengste Geheimhaltung zu wahren, umfassend untersucht.

Beispiel 10: Unvollständige Informationen in der Presse

In der Presse wird über einen zurückliegenden Kriminalfall berichtet, der in der Öffentlichkeit großes Aufsehen erregt hat. Der aktuelle Artikel erwähnt keines der üblichen Kennzeichen, die einen Rückschluss auf beteiligte Personen gestatten, insbesondere weder den Namen noch das Geburtsdatum der beteiligten Personen.

Es erscheint nicht sonderlich schwierig, sich Zugang zu weiteren Informationen zu verschaffen, um herauszufinden, welche Personen hauptsächlich an dem Fall beteiligt waren, z. B. durch Recherchieren in alten Zeitungen, in denen damals über den Fall berichtet wurde. Folglich ist nicht völlig auszuschließen, dass eine Person entsprechende Schritte unternimmt (Recherchieren in alten Zeitungen), die ihr mit großer Wahrscheinlichkeit Zugang zu den Namen und zu anderen Kennzeichen der Personen verschaffen, um die es in diesem Beispiel geht. Daher erscheint es gerechtfertigt, die Informationen in diesem Beispiel als „Daten über bestimmbare Personen“ und folglich als „personenbezogene Daten“ anzusehen.

An diesem Punkt ist anzumerken, dass Personen in der Praxis zwar überwiegend anhand ihres Namens identifiziert werden, ein Name zur Identifizierung einer Person jedoch keineswegs immer notwendig ist. Beispielsweise kann eine Person anhand anderer „Kennzeichen“ singularisiert werden. So ordnen rechnergestützte Dateien zur Erfassung personenbezogener Daten den erfassten Personen gewöhnlich ein eindeutiges Kennzeichen zu, um Verwechslungen zwischen zwei Personen in der Datei auszuschließen. Auch im Internet kann das Verhalten eines Geräts und somit des Gerätenutzers mit Hilfe von Überwachungswerkzeugen für den Internetverkehr problemlos identifiziert werden. Dadurch entsteht Stück für Stück ein Bild von der Persönlichkeit der Person, der bestimmte Entscheidungen zugeschrieben werden können. Die Person kann also ohne Kenntnis ihres Namens und ihrer Adresse anhand sozioökonomischer, psychologischer, philosophischer oder sonstiger Kriterien kategorisiert und mit bestimmten Entscheidungen in Zusammenhang gebracht werden, da der Kontaktpunkt der Person (Computer) die Offenlegung ihrer Identität im engeren Sinn nicht mehr zwingend erfordert. Mit anderen Worten setzt die Identifizierbarkeit

einer Person nicht mehr die Kenntnis ihres Namens voraus. In der Definition für personenbezogene Daten spiegelt sich dies wider.[10]

Der Europäische Gerichtshof hat sich in einem Urteil ebenfalls in dem Sinne geäußert, *„dass die Handlung, die darin besteht, auf einer Internetseite auf verschiedene Personen hinzuweisen und diese entweder durch ihren Namen oder auf andere Weise, etwa durch Angabe ihrer Telefonnummer oder durch Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen, erkennbar zu machen, eine […] Verarbeitung personenbezogener Daten im Sinne von […]Richtlinie 95/46/EG darstellt.“*[11]

Beispiel 11: Asylbewerber

Asylbewerber, die ihren tatsächlichen Namen in einem Asylantenwohnheim geheim halten, haben für administrative Zwecke eine Codenummer erhalten. Diese Nummer dient als „Kennzeichen“, damit ihnen verschiedene Informationen, die ihren Aufenthalt im Wohnheim betreffen, zugewiesen werden können. Anhand eines Fotos oder anderer biometrischer Indikatoren besitzt die Codenummer einen engen und unmittelbaren Bezug zur konkreten Person. Diese Person kann dadurch von anderen Asylbewerbern unterschieden und mit verschiedenen Informationen in Verbindung gebracht werden, die sich dann auf eine „identifizierte“ natürliche Person beziehen.

In Artikel 8 Absatz 7 heißt es ferner: „Die Mitgliedstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen.“ Diese Maßgabe enthält keine näheren Angaben, welche Art von Bedingungen die Mitgliedstaaten vorsehen sollten, sondern sie ist immer noch Teil des Artikels, der sich mit sensiblen Daten befasst. In Erwägungsgrund 33, der sich auf diese Art von Daten bezieht, heißt es: *„Daten, die aufgrund ihrer Art geeignet sind, die Grundfreiheiten oder die Privatsphäre zu beeinträchtigen“*. Dies legt den Gedanken nahe, dass der Gesetzgeber ähnliche Vorbehalte gegenüber nationalen Kennziffern hatte, weil sie ein so einfaches und eindeutiges Kombinieren verschiedener Informationen über eine bestimmte Person ermöglichen.

Mittel zur Identifizierung

Erwägungsgrund 26 der Richtlinie lenkt besondere Aufmerksamkeit auf das Wort „bestimmbar“: *„Bei der Entscheidung, ob eine Person bestimmbar ist, 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.“* Dies bedeutet, dass die rein hypothetische Möglichkeit zur Bestimmung der Person nicht ausreicht, um die Person als „bestimmbar“ anzusehen. Wenn *„alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten“* und diese Möglichkeit nicht besteht oder vernachlässigbar ist, ist die Person nicht als „bestimmbar“ anzusehen, und die Informationen würden nicht als „personenbezogene Daten“ betrachtet werden. Das Kriterium, nach dem *„alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die*

[10] Bericht über die Anwendung der Datenschutzgrundsätze auf die weltweiten Telekommunikationsnetze von Yves POULLET und seinem Team für den Beratenden Ausschuss (T-PD) des Europarats, Punkt 2.3.1, T-PD (2004) 04 final.

[11] Urteil des Europäischen Gerichtshofs (Rechtssache C-101/01) vom 6.11.2003 (Lindqvist), Randnr. 27.

Verarbeitung oder von einem Dritten eingesetzt werden könnten“, sollte insbesondere alle relevanten Kontextfaktoren berücksichtigen. Die Kosten der Identifizierung sind zwar ein Faktor, jedoch nicht der einzige Faktor. Der beabsichtigte Zweck, die Strukturierung der Verarbeitung, der von dem für die Verarbeitung Verantwortlichen erwartete Vorteil, die auf dem Spiel stehenden Interessen für die Personen sowie die Gefahr organisatorischer Dysfunktionen (z. B. Verletzung von Geheimhaltungspflichten) und technischer Fehler sollten ebenfalls Berücksichtigung finden. Gleichwohl handelt es sich um eine dynamische Prüfung, die den Stand der Technik zum Zeitpunkt der Verarbeitung und die Entwicklungsmöglichkeiten in dem Zeitraum berücksichtigen sollte, für den die Daten verarbeitet werden. Wenn alle Mittel berücksichtigt werden, die heute vernünftigerweise eingesetzt werden könnten, ist die Identifizierung heute unter Umständen nicht möglich. Wenn die Daten einen Monat lang aufbewahrt werden, ist eine Identifizierung während dieser „Lebensdauer“ so gut wie nicht zu erwarten, und folglich sind die Daten nicht als „personenbezogen“ anzusehen. Bei einer Aufbewahrungsdauer von zehn Jahren hingegen sollte der für die Verarbeitung Verantwortliche die Möglichkeit der Identifizierung berücksichtigen, die im neunten Jahr der Aufbewahrungsdauer der Daten entstehen könnte und die sie in diesem Moment zu personenbezogenen Daten machen würden. Das System sollte diesen Entwicklungen angepasst werden können und dann zum gegebenen Zeitpunkt die geeigneten technischen und organisatorischen Maßnahmen einbeziehen.

Beispiel 12: Veröffentlichung von Röntgenaufnahmen zusammen mit dem Vornamen einer Patientin

Eine Röntgenaufnahme wurde in einer wissenschaftlichen Fachzeitschrift zusammen mit dem sehr ungewöhnlichen Vornamen der Patientin veröffentlicht. Der Vorname der Patientin in Verbindung mit dem Wissen ihrer Verwandten und Bekannten, dass sie an einer bestimmten Krankheit litt, machte die Patientin für eine Reihe von Personen bestimmbar; in diesem Fall wäre die Röntgenaufnahme als Träger personenbezogener Daten anzusehen.

Beispiel 13: Pharmazeutische Forschungsdaten

Krankenhäuser oder einzelne Ärzte übertragen Daten aus Krankenblättern ihrer Patienten an ein Unternehmen zum Zwecke der medizinischen Forschung. Es werden keine Patientennamen verwendet, sondern nur Seriennummern, die jedem klinischen Fall nach dem Zufallsprinzip zugewiesen werden, um Verwechslungen bei Informationen über verschiedene Patienten auszuschließen. Die Namen der Patienten sind nur den zuständigen Ärzten bekannt, die der ärztlichen Schweigepflicht unterliegen. Die Daten enthalten keine zusätzlichen Informationen, die durch Kombinieren einen Rückschluss auf die Identität der Patienten erlauben. Außerdem wurden alle weiteren Maßnahmen – ob nun auf rechtlicher, technischer oder organisatorischer Ebene – ergriffen, um zu verhindern, dass die betreffenden Personen bestimmbar sind oder bestimmt werden könnten. Unter diesen Umständen könnte eine Datenschutzbehörde zu dem Ergebnis kommen, dass bei der Verarbeitung durch den Pharmakonzern keine Mittel vorhanden sind, die vernünftigerweise eingesetzt werden könnten, um die betreffenden Personen zu bestimmen.

Wie bereits weiter oben erwähnt, spielt der von dem für die Verarbeitung Verantwortlichen verfolgte Zweck eine wichtige Rolle bei der Beurteilung *„aller Mittel, die vernünftigerweise eingesetzt werden könnten“*, um die betreffenden Personen zu bestimmen. Die nationalen Datenschutzbehörden waren mit Fällen konfrontiert, in denen

einerseits der für die Verarbeitung Verantwortliche argumentierte, dass nur vereinzelte Informationen ohne Bezugnahme auf einen Namen oder sonstige direkte Kennzeichen verarbeitet werden, und dafür eintrat, die Daten nicht als personenbezogen anzusehen und keine Datenschutzbestimmungen auf sie anzuwenden. Andererseits ist die Verarbeitung derartiger Informationen nur dann sinnvoll, wenn sie die Identifizierung bestimmter Personen und eine bestimmte Behandlung ermöglichen. In diesen Fällen, in denen der Zweck der Verarbeitung die Identifizierung von Personen mit einschließt, kann davon ausgegangen werden, dass der für die Verarbeitung Verantwortliche oder eine andere beteiligte Person über die Mittel verfügt oder verfügen wird, die „vernünftigerweise eingesetzt werden könnten", um die betreffende Person zu bestimmen. Das Argument, dass Personen nicht bestimmbar sind, wenn der eigentliche Zweck der Verarbeitung in der Identifizierung von Personen besteht, wäre ein Widerspruch in sich. Daher sind die Informationen als Daten anzusehen, die sich auf bestimmbare Personen beziehen, und die Datenschutzbestimmungen sind auf die Verarbeitung anzuwenden.

Beispiel 14: Videoüberwachung

Im Zusammenhang mit Videoüberwachungssystemen führen die für die Verarbeitung Verantwortlichen häufig das Argument an, dass nur ein kleiner Prozentsatz des Videomaterials zur Identifizierung von Personen genutzt wird und somit keine personenbezogenen Daten verarbeitet werden, bevor eine Identifizierung von Personen in diesen seltenen Ausnahmefällen erfolgt. Da der Zweck eines Videoüberwachungssystems jedoch darin besteht, die Personen zu bestimmen, die auf den Videobildern zu sehen sind, wenn der für die Verarbeitung Verantwortliche ihre Identifizierung für notwendig hält, ist das gesamte System als Mittel zur Verarbeitung von Daten über bestimmbare Personen anzusehen, auch wenn einige aufgezeichnete Personen in der Praxis nicht bestimmbar sind.

Beispiel 15: Dynamische IP-Adressen

Die Datenschutzgruppe hat IP-Adressen als Daten, die sich auf eine bestimmbare Person beziehen, eingestuft. In ihrer Begründung heißt es: „[…] *können Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken ohne großen Aufwand Internet-Nutzer identifizieren, denen sie IP-Adressen zugewiesen haben, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internet-Nutzer zugeteilte dynamische IP-Adresse einfügen. Dasselbe lässt sich von den Internet-Diensteanbietern sagen, die in ihren HTTP-Servern Protokolle führen. In diesen Fällen besteht kein Zweifel, dass man von personenbezogenen Daten im Sinne von Artikel 2 Buchstabe a) der Richtlinie 95/46/EG reden kann.*"[12]

Vor allem in Fällen, in denen der Zweck der Verarbeitung von IP-Adressen in der Identifizierung der Computernutzer besteht (beispielsweise durch Inhaber von Urheberrechten zur strafrechtlichen Verfolgung von Computernutzern wegen Verletzung von Rechten an geistigem Eigentum), geht der für die Verarbeitung Verantwortliche vom Vorhandensein der Mittel aus, die zur Identifizierung der betreffenden Personen „vernünftigerweise eingesetzt werden könnten", z. B. von den

[12] Arbeitspapier WP 37: Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz – Angenommen am 21. November 2000.

Gerichten, bei denen Beschwerde eingelegt wurde (andernfalls wäre die Erhebung der Informationen nicht sinnvoll); aus diesem Grund sind die Informationen als personenbezogene Daten anzusehen.

Einen Sonderfall bilden IP-Adressen, die unter bestimmten Umständen aus verschiedenen technischen und organisatorischen Gründen keine Identifizierung des Nutzers gestatten. Ein Beispiel dafür sind IP-Adressen, die einem Computer in einem Internet-Café zugewiesen sind, in dem keine Identifizierung der Kunden gefordert wird. Es könnte argumentiert werden, dass die für die Nutzung von Computer X während eines bestimmten Zeitraums erfassten Daten keine Identifizierung des Nutzers unter Einsatz vernünftiger Mittel gestatten und daher nicht als personenbezogene Daten anzusehen sind. Hier ist jedoch anzumerken, dass die Internet-Diensteanbieter höchstwahrscheinlich nicht wissen, ob eine bestimmte IP-Adresse die Identifizierung ermöglicht oder nicht und daher die mit dieser IP-Adresse verknüpften Daten genauso verarbeiten wie Informationen, die mit IP-Adressen von ordnungsgemäß registrierten und bestimmbaren Benutzern verknüpft sind. Wenn der Internet-Diensteanbieter also nicht mit absoluter Sicherheit erkennen kann, dass die Daten zu nicht bestimmbaren Benutzern gehören, muss er sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln.

Beispiel 16: Durch Graffiti verursachte Schäden

Die Fahrzeuge eines Beförderungsunternehmens werden immer wieder mit Graffiti beschmiert. Zur Beurteilung der Schäden und einfacheren Geltendmachung seiner Rechtsansprüche legt das Unternehmen ein Verzeichnis mit Informationen über die Begleitumstände der Schäden, Bildern der beschädigten Gegenstände und „Identifizierungskennzeichen“ oder „Unterschriften“ der Schadensverursacher an. Bei der Eingabe der Informationen in das Verzeichnis ist nicht bekannt, wer den Schaden verursacht hat oder zu wem die „Unterschrift“ gehört. Es ist durchaus möglich, dass der Schadensverursacher niemals gefunden wird. Der Zweck der Verarbeitung besteht jedoch in der Identifizierung von Personen, auf die sich die Informationen beziehen, damit das Unternehmen Rechtsansprüche gegen den Schadensverursacher geltend machen kann. Eine derartige Verarbeitung ergibt einen Sinn, wenn der für die Verarbeitung Verantwortliche davon ausgeht, dass eines Tages Mittel vorhanden sein könnten, um die Personen zu bestimmen. Die in den Bildern enthaltenen Informationen sind als Daten, die sich auf „bestimmbare“ Personen beziehen, und die Informationen im Verzeichnis als „personenbezogene Daten“ anzusehen, und die Verarbeitung sollte den Datenschutzbestimmungen unterliegen, die eine derartige Verarbeitung unter bestimmten Umständen und mit bestimmten Garantien für rechtmäßig erklären.

Wenn der Zweck der Verarbeitung die Identifizierung der betroffenen Person nicht einschließt, kommt den technischen Maßnahmen zur Vermeidung der Identifizierung eine sehr wichtige Rolle zu. Sofern angemessene technische und organisatorische Maßnahmen auf dem Stand der Technik zum Schutz der Daten gegen Identifizierung getroffen werden, kann dies den Ausschlag bei den Überlegungen zur Nichtidentifizierbarkeit von Personen geben, wenn *alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten*, um die betreffenden Personen zu bestimmen. In diesem Fall ist die Umsetzung solcher Maßnahmen nicht die *Folge* einer rechtlichen Verpflichtung aufgrund von Artikel 17 der Richtlinie (der nur anzuwenden ist, wenn es sich von vornherein um personenbezogene Daten handelt), sondern eine

Voraussetzung dafür, dass die Informationen nicht als personenbezogen anzusehen sind und ihre Verarbeitung nicht der Richtlinie unterliegt.

Pseudonymisierte Daten

Bei der Pseudonymisierung geht es um Identitätsverschleierung. Dabei wird das Ziel verfolgt, weitere Daten über eine Person zu sammeln, ohne die Identität der Person zu kennen. Dies ist in den Bereichen Forschung und Statistik von besonderer Relevanz.

Die Pseudonymisierung kann auf rücknehmbare Weise anhand von Referenzlisten für Identitäten und ihren Pseudonymen oder anhand von Zweiwege-Verschlüsselungsalgorithmen für die Pseudonymisierung erfolgen. Identitäten können auch so verschleiert werden, dass eine Reidentifizierung nicht mehr möglich ist, d. h. durch Einweg-Verschlüsselung, wodurch gewöhnlich anonymisierte Daten entstehen.

Die Wirksamkeit der Pseudonymisierung hängt von verschiedenen Einflussfaktoren ab (vom Zeitpunkt der Pseudonymisierung, von der Rücknahmefestigkeit der Pseudonymisierungsprozedur, von der Größe der Population, in der sich der Betroffene verbirgt, von der Verkettungsmöglichkeit von einzelnen Transaktionen oder Datensätzen desselben Betroffenen usw.). Pseudonyme sollten zufällig und nicht vorhersagbar gewählt werden. Die Menge der möglichen Pseudonyme sollte so groß sein, dass bei zufälliger Auswahl nicht zweimal das gleiche Pseudonym gewählt wird. Ist eine hohe Sicherheit erforderlich ist, muss die Menge der Pseudonymkandidaten mindestens so groß sein wie der Wertebereich sicherer kryptografischer Hash-Funktionen.[13]

Rücknehmbar pseudonymisierte Daten sind als *indirekt bestimmbare* Informationen über Personen anzusehen. Bei Verwendung eines Pseudonyms besteht also die Möglichkeit der Rückverfolgung zur Person und Aufdeckung ihrer Identität, wenn auch nur unter zuvor festgelegten Bedingungen. Bei der Verarbeitung indirekt bestimmbarer Informationen sind die Risiken für die Personen zumeist sehr gering, so dass die Datenschutzbestimmungen zu Recht flexibler als bei der Verarbeitung von Informationen über direkt bestimmbare Personen angewandt werden.

Verschlüsselte Daten

Verschlüsselte Daten sind ein klassisches Beispiel für Pseudonymisierung. Informationen beziehen sich auf Personen, die durch einen Code gekennzeichnet sind, während der Schlüssel für die Zuordnung des Codes zu den Kennzeichen der Personen (z. B. Name, Geburtsdatum, Adresse) gesondert aufbewahrt wird.

Beispiel 17: Nicht aggregierte Daten für Statistiken

Wie wichtig die Berücksichtigung aller Begleitumstände bei der Beurteilung der Mittel ist, die zur Identifizierung „vernünftigerweise eingesetzt werden könnten“, zeigt das folgende Beispiel, in dem es um die Verarbeitung personenbezogener Daten durch das nationale statistische Amt geht. Dabei werden die Informationen zu einem bestimmten Zeitpunkt in nicht aggregierter Form gespeichert und beziehen sich auf spezifische Personen, denen jedoch ein Code anstelle eines Namens zugewiesen ist (z. B. die

[13] Siehe das Arbeitspapier „Datenschutzfreundliche Technologien“ der Arbeitsgruppe „Datenschutzfreundliche Technologien“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder (Oktober 1997), veröffentlicht unter http://ec.europa.eu/justice_home/fsj/privacy/studies/index_de.htm

Person mit dem Code X1234 trinkt öfter als dreimal pro Woche ein Glas Wein). Das statistische Amt bewahrt den Schlüssel für diese Codes gesondert auf (d. h. die Liste für die Zuordnung der Codes zu den Namen der Personen). Dieser Schlüssel kann als ein vom statistischen Amt „vernünftigerweise eingesetztes Mittel" angesehen werden. Folglich sind die Informationen über die Person als personenbezogene Daten anzusehen, auf die die Datenschutzbestimmungen anzuwenden sind. Nun wäre vorstellbar, dass eine Liste mit Daten über die Konsumgewohnheiten von Weintrinkern an den nationalen Weinerzeugerverband übermittelt wird, der seinen öffentlichen Standpunkt mit Statistiken untermauern will. Bei der Frage, ob es sich bei dieser Liste mit Informationen immer noch um personenbezogene Daten handelt, ist zu beurteilen, ob einzelne Weinkonsumenten identifiziert werden können, wenn *„alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden."*

Bei Verwendung eindeutiger Codes für jede Person entsteht ein gewisses Identifizierungsrisiko, wenn es möglich ist, Zugang zu dem für die Verschlüsselung verwendeten Schlüssel zu erhalten. Daher sind die Risiken externer Hacking-Angriffe, die Wahrscheinlichkeit, dass eine Person in der übermittelnden Organisation – ungeachtet ihrer beruflichen Schweigepflicht – den Schlüssel preisgibt *und* die Machbarkeit einer indirekten Identifizierung bei der Frage einzubeziehen, ob die Personen bestimmbar sind, *wenn alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden*, und ob die Informationen folglich als „personenbezogene Daten" anzusehen sind. Falls ja, finden die Datenschutzbestimmungen Anwendung. Eine andere Frage ist, ob diese Datenschutzbestimmungen berücksichtigen könnten, ob die Risiken für die Personen gemindert werden, und mehr oder weniger strenge Bedingungen für die Verarbeitung unter Ausnutzung des in der Richtlinie zulässigen Handlungsspielraums auferlegen.

Wenn die Codes hingegen nicht eindeutig sind, sondern ein und dieselbe Codenummer (z. B. „123") für Personen in verschiedenen Städten und für Daten aus verschiedenen Jahren (nur zur Unterscheidung einer bestimmten Person in einem Jahr und in der Stichprobe in derselben Stadt) verwendet wird, könnte der für die Verarbeitung Verantwortliche oder ein Dritter eine spezifische Person nur dann bestimmen, wenn er weiß, auf welches Jahr und auf welche Stadt sich die Daten beziehen. Wenn diese Zusatzinformationen nicht mehr vorhanden und mit vertretbarem Aufwand auch nicht mehr wiederherzustellen sind, könnten die Informationen als nicht auf bestimmbare Personen bezogen angesehen werden, und die Datenschutzbestimmungen würden folglich keine Anwendung finden.

Diese Art von Daten wird häufig bei klinischen Prüfungen von Arzneimitteln verwendet. Die Richtlinie Nr. 2001/20/EG vom 4. April 2001 über die Anwendung der guten klinischen Praxis bei der Durchführung von klinischen Prüfungen[14] legt einen Rechtsrahmen für die Ausübung dieser Tätigkeit fest. Der für die klinischen Prüfungen zuständige Arzt/Forschungsleiter („Prüfer") erfasst die Daten zu den klinischen Ergebnissen für jeden Patienten und ordnet jedem Patienten einen Code zu. Der Prüfer leitet die Daten an den Pharmakonzern oder Dritte („Geldgeber") ausschließlich in dieser codierten Form weiter, da diese nur an biostatistischen Daten interessiert sind. Der Prüfer führt jedoch einen separaten Schlüssel, der diesen Code mit allgemeinen Informationen verknüpft, um die Patienten einzeln identifizieren zu können. Der Prüfer

[14] ABl. L 121 vom 1.5.2001, S. 34.

ist zur Führung dieses Schlüssels verpflichtet, damit einzelne Patienten identifiziert und entsprechend behandelt werden können, falls sich das Arzneimittel als Gefahr für die Gesundheit der Patienten erweist.

Hier stellt sich die Frage, ob die für die klinischen Prüfungen verwendeten Daten als Daten anzusehen sind, die sich auf „bestimmbare" natürliche Personen beziehen und somit den Datenschutzbestimmungen unterliegen. Wie in der obigen Analyse beschrieben, sind bei der Ermittlung, ob eine Person bestimmbar ist, alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. In diesem Fall ist die Identifizierung von Personen (damit sie im Bedarfsfall angemessen behandelt werden können) einer der Zwecke bei der Verarbeitung der verschlüsselten Daten. Der Pharmakonzern hat die Mittel für die Verarbeitung bereitgestellt und die organisatorischen Maßnahmen und seine Beziehungen zum Prüfer (der im Besitz des Schlüssels ist) so gestaltet, dass die Identifizierung von Personen nicht nur erfolgen *kann*, sondern unter bestimmten Umständen erfolgen *muss*. Die Identifizierung von Patienten ist somit in den Zwecken und Mitteln für die Verarbeitung fest verankert. In diesem Fall kann gefolgert werden, dass derartig verschlüsselte Daten Informationen über natürliche Personen darstellen, die von allen an einer möglichen Identifizierung beteiligten Dritten bestimmbar sind, und den Datenschutzbestimmungen unterliegen sollten. Dies bedeutet jedoch nicht, dass ein anderer für die Verarbeitung Verantwortlicher, der denselben Satz codierter Daten verarbeitet, personenbezogene Daten verarbeiten würde, wenn in dem speziellen Rahmen, in dem andere für die Verarbeitung Verantwortliche ihre Tätigkeit ausüben, die Reidentifizierung explizit ausgeschlossen ist und diesbezüglich geeignete technische Maßnahmen getroffen wurden.

Auf anderen Forschungsgebieten oder im gleichen Projekt könnte die Reidentifizierung in Übermittlungs- und Verfahrensvorschriften ausgeschlossen worden sein, etwa weil therapeutische Aspekte keine Rolle spielen. Aus technischen oder anderen Gründen kann es immer noch einen Weg geben, herauszufinden, welche klinischen Daten zu welchen Personen gehören, doch die Identifizierung ist keinesfalls beabsichtigt oder zu erwarten, weswegen geeignete technische Maßnahmen (z. B. Verschlüsselung, nicht rücknehmbares Hashing) getroffen wurden, die genau dies verhindern sollen. Selbst wenn ungeachtet aller Übermittlungsvorschriften und Maßnahmen (aufgrund unvorhersehbarer Umstände wie die zufällige Zuordnung von Eigenschaften, die die Identität einzelner Personen offenbaren) einzelne Personen identifiziert werden, sind die vom ursprünglichen Verantwortlichen verarbeiteten Informationen nicht als Daten anzusehen, die sich auf bestimmte oder bestimmbare Personen beziehen, wenn *alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden.* Die Bestimmungen der Richtlinie finden somit auf ihre Verarbeitung keine Anwendung. Anders verhält es sich, wenn ein neuer für die Verarbeitung Verantwortlicher Zugang zu den bestimmbaren Informationen erhalten hat; in diesem Fall sind sie ohne jeden Zweifel als „personenbezogene Daten" anzusehen.

Häufig gestellte Fragen (FAQ 14-7) zu den Grundsätzen des „sicheren Hafens"

Die Verwendung verschlüsselter Daten in der pharmazeutischen Forschung wurde auch in den Grundsätzen des „sicheren Hafens“ erörtert.[15] FAQ 14-7 lautet:

FAQ 14 – Arzneimittel und Medizinprodukte

7. F: Forschungsdaten werden stets an der Quelle verschlüsselt, damit aus ihnen nicht die Identität einzelner Personen zu ersehen ist. Den Pharmaorganisationen, also den Projektträgern, wird der Schlüssel nicht ausgehändigt, er verbleibt beim Forscher, so dass er unter bestimmten Umständen (z. B. wenn eine nachträgliche Überwachung notwendig ist) einzelne Versuchspersonen identifizieren kann. Ist die Übermittlung derart verschlüsselter Daten von der EU in die USA als Übermittlung personenbezogener Daten anzusehen, die den Grundsätzen des sicheren Hafens unterliegt?

7. A: Nein, das gilt nicht als Übermittlung personenbezogener Daten, die den Grundsätzen des „sicheren Hafens“ unterliegt.

Nach Auffassung der Datenschutzgruppe steht diese Erklärung in den Grundsätzen des „sicheren Hafens“ nicht im Widerspruch zu den obigen Ausführungen, die derartige Informationen als personenbezogene Daten gemäß der Richtlinie ansehen. Tatsächlich ist diese Frage nicht präzise genug formuliert, da sie keine Angaben darüber enthält, an wen und unter welchen Bedingungen die Daten übermittelt werden. Die Datenschutzgruppe geht davon aus, dass sich die Frage lediglich auf die Übermittlung verschlüsselter Daten an einen Empfänger in den USA (beispielsweise das Pharmaunternehmen) bezieht, der nur die verschlüsselten Daten erhält und zu keinem Zeitpunkt von der Identität der Patienten erfährt, die bekannt ist und nur dem Arzt/Forschungsleiter in der EU – zu keinem Zeitpunkt jedoch dem Unternehmen in den USA – mitgeteilt wird, falls eine medizinische Behandlung notwendig ist.

Anonyme Daten

„Anonyme Daten“ sind im Sinne der Richtlinie Informationen, die sich auf eine natürliche Person beziehen, wobei die Person von dem für die Verarbeitung Verantwortlichen oder einem Dritten nicht bestimmt werden kann, *wenn alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden*, um die betreffende Person zu bestimmen. „Anonymisierte Daten“ sind somit anonyme Daten, die sich zuvor auf eine bestimmbare Person bezogen, die jedoch nicht mehr identifizierbar ist. Erwägungsgrund 26 bezieht sich ebenfalls auf diesen Begriff: „*Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist.*“ Auch hier hängt die Beurteilung, ob die Daten die Identifizierung einer Person ermöglichen und ob die Informationen als anonym betrachtet werden können oder nicht, von den jeweiligen Umständen ab, und es sollte wie in Erwägungsgrund 26 beschrieben eine Einzelfallanalyse insbesondere im Hinblick darauf durchgeführt werden, inwieweit Mittel in vertretbarem Umfang eingesetzt werden könnten, um die betreffende Person zu bestimmen. Dies ist von besonderer Bedeutung bei statistischen Informationen, bei denen die Originalstichprobe nicht ausreichend groß ist und andere vereinzelte Informationen die Identifizierung von Personen ermöglichen, obwohl die Informationen in aggregierter Form präsentiert werden.

[15] Entscheidung der Kommission 2000/520/EG vom 26.7.2000, ABl. L 215/7 vom 25.8.2000.

Beispiel 18: Statistische Erhebungen und Kombination vereinzelter Informationen

Abgesehen von ihrer allgemeinen Pflicht im Hinblick auf die Einhaltung der Datenschutzbestimmungen zur Sicherstellung der Anonymität statistischer Erhebungen sind Statistiker an eine spezielle Geheimhaltungspflicht gebunden, die ihnen die Veröffentlichung nicht anonymer Daten verbietet. Demnach dürfen sie statistische Daten nur in aggregierter Form veröffentlichen, bei denen die Zuordnung zu bestimmten Personen nicht möglich ist. Diese Regelung ist von besonderer Bedeutung für die Veröffentlichung von Erhebungsdaten. In jeder Situation sollte ein Grenzwert festgelegt werden, unter dem die Identifizierung einzelner Personen als möglich angesehen wird. Wenn ein Kriterium die Identifizierung in einer bestimmten Personengruppe gleich welcher Größe (z. B. nur ein Arzt in einer Stadt mit 6000 Einwohnern) zu ermöglichen scheint, sollte dieses Unterscheidungskriterium weggelassen oder andere Kriterien zur „Verschleierung" der Ergebnisse über eine bestimmte Person aufgenommen werden, um die statistische Geheimhaltungspflicht zu erfüllen.

Beispiel 19: Veröffentlichung von Videoaufzeichnungen

Ein Ladenbesitzer installiert in seinem Geschäft ein Videoüberwachungssystem. Er veröffentlicht in seinem Geschäft Bilder von Ladendieben, die mit Hilfe des Kameraüberwachungssystems überführt wurden. Nach dem Einschreiten der Polizei macht er das Gesicht der Diebe unkenntlich. Dennoch besteht weiterhin die Möglichkeit, dass die Personen auf den Fotos von ihren Freunden, Verwandten oder Nachbarn erkannt werden, weil ihre Figur, Frisur und Kleidung ihre Identität offenbaren können.

4. VIERTES ELEMENT: „NATÜRLICHE PERSON"

Der durch die Bestimmungen der Richtlinie gebotene Schutz gilt für natürliche Personen, d. h. Menschen. Insofern ist das Recht auf den Schutz personenbezogener Daten ein allgemeines Recht, das nicht auf Staatsangehörige oder Bewohner eines bestimmten Landes beschränkt ist. Dieser Aspekt wird in Erwägungsgrund 2 der Richtlinie ausdrücklich betont: „*Die Datenverarbeitungssysteme stehen im Dienste des Menschen*" und „*sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und Freiheiten […] zu achten*".

Um den Begriff der natürlichen Person geht es auch in Artikel 6 der Allgemeinen Erklärung der Menschenrechte: „*Jeder hat das Recht, überall als rechtsfähig anerkannt zu werden.*" Das Zivilrecht der Mitgliedstaaten setzt sich genauer mit dem Begriff der Rechtspersönlichkeit auseinander, die als mit der Geburt der Person beginnende und mit ihrem Tod endende Fähigkeit verstanden wird, ein Rechtsverhältnis einzugehen. Personenbezogene Daten sind folglich Daten, die sich grundsätzlich auf bestimmte oder bestimmbare *lebende Personen* beziehen. Dies wirft für die Zwecke dieser Analyse eine Reihe von Fragen auf.

Daten über verstorbene Personen

Gemäß den Bestimmungen der Richtlinie sind Informationen über verstorbene Personen grundsätzlich nicht als personenbezogene Daten anzusehen, da verstorbene Personen im Zivilrecht keine natürliche Personen mehr sind. In bestimmten Fällen können die Daten verstorbener Personen dennoch indirekten Schutz genießen.

Erstens kann der für die Verarbeitung Verantwortliche eventuell nicht feststellen, ob die Person, auf die sich die Daten beziehen, noch lebt oder bereits verstorben ist. Selbst wenn er dazu in der Lage ist, werden die Informationen über verstorbene Personen unter Umständen ohne Unterscheidung nach den gleichen Regeln wie für lebende Personen verarbeitet. Da der für die Verarbeitung Verantwortliche bei der Verarbeitung von Daten über lebende Personen zur Einhaltung der Datenschutzbestimmungen der Richtlinie verpflichtet ist, dürfte es für ihn in der Praxis einfacher sein, Daten über verstorbene Personen ebenfalls im Sinne der Datenschutzbestimmungen zu verarbeiten, als die beiden Gruppen von Daten voneinander getrennt zu verarbeiten.

Zweitens könnten sich Informationen über verstorbene Personen auch auf lebende Personen beziehen. Beispielsweise deutet die Information, dass die verstorbene Gaia an der Bluterkrankheit litt, darauf hin, dass ihr Sohn Titius ebenfalls an dieser Krankheit leidet, da sie mit einem Gen auf dem X-Chromosom verknüpft ist. Wenn sich die Information, die Daten über verstorbene Personen enthält, gleichzeitig auf lebende Personen bezieht und es sich um personenbezogene Daten im Sinne der Richtlinie handelt, können personenbezogene Daten über verstorbene Personen indirekt den Schutz der Datenschutzbestimmungen genießen.

Drittens können Informationen über verstorbene Personen einem speziellen Schutz unterliegen, der durch andere Regelwerke als Datenschutzbestimmungen gewährt wird und der die Grenze bei *„personalitas praeterita“* zieht. Die Schweigepflicht von Ärzten endet nicht mit dem Tod des Patienten. Die einzelstaatlichen Rechtsvorschriften für die Rechte am eigenen Bild und an der Bewahrung der Ehre können auch Schutz für das Andenken an verstorbene Personen bieten.

Viertens wird ein Mitgliedstaat durch nichts daran gehindert, den Geltungsbereich der die Richtlinie 95/46/EG umsetzenden innerstaatlichen Rechtsvorschriften auf vom Anwendungsbereich dieser Richtlinie nicht erfasste Bereiche auszudehnen, soweit dem keine andere Bestimmung des Gemeinschaftsrechts entgegensteht, wie der Europäische Gerichtshof in Erinnerung rief.[16] Ein nationaler Gesetzgeber könnte also die Bestimmungen der nationalen Datenschutzgesetze auf Aspekte ausweiten, die sich auf die Verarbeitung von Daten über verstorbene Personen beziehen, wenn ein legitimes Interesse dies rechtfertigt.[17]

Ungeborene Kinder

In welchem Umfang Datenschutzbestimmungen vor der Geburt Anwendung finden, richtet sich nach dem allgemeinen Standpunkt der nationalen Rechtssysteme in Bezug auf den Schutz ungeborener Kinder. Insbesondere für die Berücksichtigung von

---

16 Urteil des Europäischen Gerichtshofs (Rechtssache C-101/01) vom 6.11.2003 (Lindqvist), Randnr. 98.

17 Protokoll des Rates der Europäischen Union vom 8.2.1995, Dokument 4730/95: „Re Article 2(a): *The Council and the Commission confirm that it is for the Member States to lay down whether and to what extent this Directive shall be applied to deceased persons.*“ (Zu Artikel 2 Buchstabe a: Der Rat und die Kommission bestätigen, dass es den Mitgliedstaaten überlassen bleibt festzulegen, ob und in welchem Umfang diese Richtlinie auf verstorbene Personen anzuwenden ist.)

Erbschaftsansprüchen erkennen einige Mitgliedstaaten den Grundsatz an, dass gezeugte, aber noch nicht geborene Kinder hinsichtlich zu erwartender Leistungen als geborene Kinder anzusehen sind (und somit ein Erbe antreten oder eine Schenkung annehmen können), vorausgesetzt, dass sie auch geboren werden. In anderen Mitgliedstaaten gewähren spezielle Rechtsvorschriften besonderen Schutz, der jedoch an dieselbe Bedingung geknüpft ist. Um zu ermitteln, ob die nationalen Datenschutzbestimmungen auch für Informationen über ungeborene Kinder gelten, sollte der allgemeine Ansatz des nationalen Rechtssystems in Verbindung mit der Überlegung betrachtet werden, dass mit den Datenschutzbestimmungen der Schutz von Personen bezweckt wird.

Eine zweite Frage wird durch die Überlegung aufgeworfen, dass die allgemeine Reaktion des Rechtssystems auf der Erwartung beruht, dass die Situation ungeborener Kinder auf die Schwangerschaftsmonate befristet ist. Sie berücksichtigt nicht, dass diese Situation tatsächlich wesentlich länger andauern kann, etwa im Falle eingefrorener Embryonen. Schließlich sind auch spezifische Reaktionen des Rechtssystems in bestimmten Vorschriften zu Reproduktionsverfahren zu finden, in denen es um die Verwendung medizinischer oder genetischer Informationen über Embryonen geht.

Juristische Personen

Da sich die Definition für personenbezogene Daten auf Personen bezieht, d. h. natürliche Personen, fallen Informationen über juristische Personen grundsätzlich nicht in den Anwendungsbereich der Richtlinie, und der durch die Richtlinie gewährte Schutz findet keine Anwendung.[18] Unter verschiedenen Umständen finden bestimmte Datenschutzbestimmungen jedoch indirekt Anwendung auf Informationen, die sich auf Unternehmen oder juristische Personen beziehen.

Einige Bestimmungen der Datenschutzrichtlinie 2002/58/EG für die elektronische Kommunikation gelten auch für juristische Personen. In Artikel 1 dieser Richtlinie heißt es: *„(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.*“ Entsprechend wird in Artikel 12 und 13 die Anwendung einiger Bestimmungen für Teilnehmerverzeichnisse und unerbetene Nachrichten auch auf juristische Personen ausgeweitet.

Nach den im vorliegenden Arbeitspapier genannten Kriterien könnten sich Informationen über juristische Personen ihrem wesentlichen Inhalt nach auch auf natürliche Personen „beziehen“, etwa wenn sich der Name der juristischen Person vom Namen einer natürlichen Person ableitet. Ein weiteres Beispiel ist die elektronische Post in Unternehmen, die gewöhnlich von einem bestimmten Mitarbeiter genutzt wird oder Informationen über einen Kleinbetrieb (vom rechtlichen Standpunkt aus betrachtet ein „Gegenstand“ und keine juristische Person), die das Verhalten ihres Eigentümers beschreibet. In allen diesen Fällen, in denen die Kriterien „Inhalt“, „Zweck“ oder „Ergebnis“ bei Informationen über die juristische Person oder das Unternehmen einen Bezug zu einer natürlichen Person herstellen, sind die Daten als personenbezogen anzusehen und die Datenschutzbestimmungen auf sie anzuwenden.

[18] Erwägungsgrund 24 der Richtlinie: „Diese Richtlinie berührt nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen.“

Der Europäische Gerichtshof hat klargestellt, dass die Mitgliedstaaten durch nichts daran gehindert werden, den Geltungsbereich der die Richtlinie umsetzenden innerstaatlichen Rechtsvorschriften auf vom Anwendungsbereich dieser Richtlinie nicht erfasste Bereiche auszudehnen, soweit dem keine andere Bestimmung des Gemeinschaftsrechts entgegensteht.[19] Entsprechend haben einige Mitgliedstaaten wie Italien, Österreich oder Luxemburg den Geltungsbereich ihrer die Richtlinie umsetzenden Rechtsvorschriften (beispielsweise für Sicherheitsvorkehrungen) auf die Verarbeitung von Daten über juristische Personen ausgeweitet.

Ebenso wie bei Informationen über verstorbene Personen können die vom für die Verarbeitung Verantwortlichen getroffenen, praktischen Vorkehrungen zur Folge haben, dass die Datenschutzbestimmungen auch auf Daten über juristische Personen Anwendung finden. Wenn der für die Verarbeitung Verantwortliche Daten über natürliche und juristische Personen unscharf erhebt und in die gleichen Datensätze aufnimmt, können die Datenverarbeitungsmechanismen und das Kontrollsystem so eingerichtet werden, dass sie den Datenschutzbestimmungen entsprechen. Unter Umständen ist es für den für die Verarbeitung Verantwortlichen jedoch einfacher, die Datenschutzbestimmungen auf alle Arten von Informationen anzuwenden, als bei der Verarbeitung der Daten einzeln zu prüfen, ob sie sich auf natürliche oder juristische Personen beziehen.

IV. WIE IST ZU VERFAHREN, WENN DIE DATEN NICHT UNTER DIE DEFINITION FALLEN?

Wie in diesem Arbeitspapier aufgezeigt wurde, sind Informationen in verschiedenen Situationen nicht als personenbezogene Daten anzusehen. Dies ist der Fall, wenn die Daten keinen Bezug zu einer Person herstellen oder die Person nicht als bestimmt oder bestimmbar anzusehen ist. Wenn die verarbeitete Information nicht unter den Begriff „personenbezogene Daten“ fällt, findet die Richtlinie gemäß Artikel 3 folglich keine Anwendung. Dies bedeutet aber nicht, dass die Personen in der jeweiligen Situation keinen Schutz genießen. Hier sind folgende Überlegungen zu berücksichtigen.

Wenn die Richtlinie nicht anwendbar ist, kommen unter Umständen innerstaatliche Datenschutzgesetze zur Anwendung. Laut Artikel 34 ist die Richtlinie an die Mitgliedstaaten gerichtet. Außerhalb des Anwendungsbereichs der Richtlinie sind die Mitgliedstaaten nicht an die von ihr auferlegten Verpflichtungen gebunden, die hauptsächlich in der Inkraftsetzung der einschlägigen Rechts- und Verwaltungsvorschriften bestehen. Wie der Europäische Gerichtshof klargestellt hat, werden die Mitgliedstaaten jedoch durch nichts daran gehindert, den Geltungsbereich der die Richtlinie umsetzenden innerstaatlichen Rechtsvorschriften auf vom Anwendungsbereich dieser Richtlinie nicht erfasste Bereiche auszudehnen, soweit dem keine andere Bestimmung des Gemeinschaftsrechts entgegensteht. Somit wäre es vorstellbar, dass auf bestimmte Situationen, in denen keine personenbezogenen Daten im Sinne dieser Richtlinie verarbeitet werden, dennoch Schutzmaßnahmen nach einzelstaatlichem Recht Anwendung finden. Ein Beispiel dafür sind verschlüsselte Daten, und zwar unabhängig davon, ob es sich um personenbezogene Daten handelt oder nicht.

Wenn Datenschutzbestimmungen keine Anwendung finden, können bestimmte Aktivitäten dennoch einen Eingriff in die Persönlichkeitsrechte gemäß Artikel 8 der

[19] Urteil des Europäischen Gerichtshofs (Rechtssache C-101/01) vom 6.11.2003 (Lindqvist), Randnr. 98.

Europäischen Menschenrechtskonvention darstellen, der das Recht auf Achtung des Privat- und Familienlebens im Lichte der weit reichenden Rechtsprechung der Menschenrechtskonvention schützt. Andere Regelwerke, z. B. das Schadenersatzrecht, Strafrecht oder Antidiskriminierungsrecht, können ebenfalls zum Schutz von Persönlichkeitsrechten herangezogen werden, wenn Datenschutzbestimmungen keine Anwendung finden und verschiedene berechtigte Interessen auf dem Spiel stehen.

V. SCHLUSSFOLGERUNGEN

Die Datenschutzgruppe hat in dieser Stellungnahme Orientierungshilfen gegeben, wie der Begriff „personenbezogene Daten“ in der Richtlinie 95/46/EG und die einschlägigen Rechtsvorschriften der Gemeinschaft zu verstehen und in verschiedenen Situationen anzuwenden sind.

In den allgemeinen Überlegungen wurde darauf hingewiesen, dass zwar der europäische Gesetzgeber die Absicht verfolgte, den Begriff „personenbezogene Daten“ möglichst weit zu fassen, jedoch gewisse Grenzen zu beachten sind. Es sollte stets bedacht werden, dass die Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre von Personen bei der Verarbeitung personenbezogener Daten zum Ziel haben. Diese Bestimmungen wurden daher für Situationen vorgesehen, in denen die Rechte von Personen bedroht sein könnten und folglich geschützt werden müssen. Der Anwendungsbereich der Datenschutzbestimmungen sollte einerseits zwar nicht zu stark ausgeweitet werden, doch andererseits sollte auch eine übermäßige Einschränkung des Begriffs „personenbezogene Daten“ vermieden werden. Die Richtlinie hat den Anwendungsbereich des Begriffs unter Ausschluss verschiedener Tätigkeiten definiert und lässt eine gewisse Flexibilität bei der Anwendung der Bestimmungen auf Tätigkeiten zu, die außerhalb ihres Anwendungsbereichs liegen. Den Datenschutzbehörden kommt eine wichtige Rolle bei der Suche nach einem angemessenen Mittelweg bei der Anwendung dieser Richtlinie zu (siehe Abschnitt II).

Die Analyse der Datenschutzgruppe konzentrierte sich auf die vier Hauptbausteine, aus denen sich die Definition für „personenbezogene Daten“ zusammensetzt: „alle Informationen“, „über“, „eine bestimmte oder bestimmbare“, „natürliche Person“. Diese Bausteine sind eng miteinander verbunden und beeinflussen sich wechselseitig, zusammen entscheiden sie jedoch darüber, ob eine Information als „personenbezogen“ anzusehen ist. Die Analyse wird durch Beispiele aus der einzelstaatlichen Praxis europäischer Datenschutzbehörden untermauert.

- Das erste Element – „alle Informationen“ – erfordert eine weit gefasste Auslegung des Begriffs unabhängig von der Art oder vom Inhalt der Information und der technischen Form, in der sie präsentiert wird. Dies bedeutet, dass sowohl objektive als auch subjektive Informationen über eine Person – in welcher Funktion auch immer – als „personenbezogene Daten“ angesehen werden können, und zwar unabhängig vom technischen Medium, auf dem sie aufgezeichnet sind. Die Stellungnahme befasst sich auch mit biometrischen Daten und den rechtlichen Unterscheidungsmerkmalen bei menschlichen Proben, aus denen sie extrahiert werden können (siehe Abschnitt III.1).

- Das zweite Element – „über“ – wurde bisher oftmals übersehen, spielt jedoch eine wichtige Rolle bei der Beurteilung der inhaltlichen Dimension des Begriffs, insbesondere im Zusammenhang mit Gegenständen und neuen Technologien. In der

Stellungnahme werden drei alternative Elemente – d. h. Inhalt, Zweck oder Ergebnis – angesprochen, um zu ermitteln, ob sich eine Information auf eine Person „bezieht". Dies gilt auch für Informationen, die offenkundige Auswirkungen auf die Art der Behandlung oder Beurteilung einer Person haben können (siehe Abschnitt III.2).

- Das dritte Element – „bestimmte oder bestimmbare" – konzentriert sich auf die Bedingungen, unter denen eine Person als „bestimmbar" anzusehen ist, und insbesondere auf die Mittel, die „vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden", um die betreffende Person zu bestimmen. Die Kontextfaktoren und Begleitumstände in einem konkreten Fall spielen bei dieser Analyse eine wichtige Rolle. Die Stellungnahme befasst sich auch mit „pseudonymisierten Daten" und der Verwendung „verschlüsselter Daten" in der statistischen oder pharmazeutischen Forschung (siehe Abschnitt III.3).

- Im vierten Element – „natürliche Person" – geht es um die Forderung, dass sich „personenbezogene Daten" auf „lebende Personen" beziehen müssen. Die Stellungnahme geht auch auf die Grauzonen ein, die bei Daten über verstorbene Personen, ungeborene Kinder und juristische Personen entstehen (siehe Abschnitt III.4).

In der Stellungnahme wird abschließend erörtert, wie zu verfahren ist, wenn Daten nicht unter die Definition für „personenbezogene Daten" fallen. In diesen Fällen bieten sich verschiedene Lösungen an, etwa die Anwendung nicht unter diese Richtlinie fallender, innerstaatlicher Rechtsvorschriften, sofern diese nicht gegen das Gemeinschaftsrecht verstoßen (siehe Abschnitt IV).

Die Datenschutzgruppe ersucht alle interessierten Kreise, die in dieser Stellungnahme dargelegten Leitlinien sorgfältig zu prüfen und diese bei der Auslegung und Anwendung des einzelstaatlichen Rechts im Sinne der Richtlinie 95/46/EG zu berücksichtigen.

Die Mitglieder der Datenschutzgruppe, die überwiegend aus Vertretern der nationalen Kontrollstellen für den Datenschutz besteht, setzen sich für die Weiterentwicklung der Leitlinien in dieser Stellungnahme in ihren eigenen Zuständigkeitsbereichen und für die ordnungsgemäße Anwendung ihres einzelstaatlichen Rechts gemäß Richtlinie 95/46/EG ein.

Die Datenschutzgruppe beabsichtigt, die in dieser Stellungnahme formulierten Leitlinien anzuwenden und gegebenenfalls weiterzuentwickeln und bei ihrer künftigen Arbeit, insbesondere bei der Erörterung von Themen wie dem Identitätsmanagement im Zusammenhang mit E-Government und E-Health und der RFID-Technik, entsprechend zu berücksichtigen. Zum Thema RFID-Technik plant die Datenschutzgruppe, sich an einer weiteren Analyse zu beteiligen, die sich mit der Frage befasst, wie sich die Datenschutzbestimmungen auf die Verwendung von RFID-Etiketten auswirken und ob weitere Maßnahmen notwendig sind, um die Achtung der Datenschutzrechte und Interessen auf diesem Gebiet sicherzustellen.

Die Datenschutzgruppe ist für Rückmeldungen interessierter Kreise und der Kontrollstellen hinsichtlich ihrer praktischen Erfahrungen mit den in dieser Stellungnahme gegebenen Leitlinien, eventuell unter Angabe weiterer Beispiele, dankbar. Sie plant, das Thema zu einem späteren Zeitpunkt erneut aufzugreifen, um das gemeinsame Verständnis des Schlüsselbegriffs „personenbezogene Daten" weiter zu

verbessern und eine harmonisierte Anwendung und bessere Umsetzung der Richtlinie 95/46/EG und des einschlägigen Gemeinschaftsrechts auf dieser Grundlage sicherzustellen.

Für die Datenschutzgruppe

Der Vorsitzende
Peter SCHAAR