Dokumente
zu Datenschutz
und Informationsfreiheit
2012

Impressum

Herausgeber: **Berliner Beauftragter für Datenschutz und Informationsfreiheit**
An der Urania 4 – 10, 10787 Berlin
Telefon: 0 30/1 38 89-0
Telefax: 0 30/2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft mbH

Stand: Februar 2013

Inhaltsverzeichnis

Vorwort

Die Dokumente dieses Bandes behandeln neben einer Vielzahl von aktuellen Entwicklungen drei Schwerpunkte:

Im Vordergrund steht die Reform des Europäischen Rechtsrahmens für den Datenschutz, wie sie die Kommission im Januar 2012 vorgeschlagen hat. Hierzu haben sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder als auch die Gruppe der europäischen Datenschutzbehörden nach Art. 29 der Datenschutzrichtlinie von 1995 Stellung genommen. Die Vorschläge der Kommission und die Stellungnahmen der Art. 29-Gruppe würden den Rahmen dieses Bandes sprengen, sie sind aber online verfügbar.[1]

Angesichts der zunehmenden praktischen Bedeutung, die das Cloud Computing gewinnt, ist es nicht verwunderlich, dass mehrere europäische und internationale Gremien hierzu Forderungskataloge aufgestellt haben. Den Anfang machte die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. „Berlin Group“) mit dem Sopot-Memorandum, ihr folgten die Art. 29-Gruppe und die Internationale Konferenz der Datenschutzbeauftragten. Den Anstoß für diese Diskussion auf internationaler Ebene haben die deutschen Datenschutzbeauftragten mit ihrer Entschließung vom September 2011 zur datenschutzkonformen Gestaltung und Nutzung von Cloud Computing gegeben.[2]

Schließlich enthält dieser Band die vom Gesamtverband der Deutschen Versicherungswirtschaft entwickelten Verhaltensregeln für den Umgang mit personenbezogenen Daten, die 2012 vom Berliner Beauftragten für Datenschutz und Informationsfreiheit nach § 38 a des Bundesdatenschutzgesetzes anerkannt wurden. Damit hat erstmals ein Verband in Deutschland die Möglichkeiten zur regulierten Selbstregulierung genutzt, die das Bundesdatenschutzgesetz eröffnet.

---

[1] Vorschläge der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(2012) 11 endg. (Datenschutz-Grundverordnung), und für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endg. (Polizei- und Justiz-Richtlinie), beide v. 25.1.2012; Stellungnahmen der Art. 29-Gruppe 1/2012 zu den Reformvorschlägen im Bereich des Datenschutzes v. 23.3.2012 (WP 191) und 8/2012 mit weiteren Beiträgen zur Diskussion der Datenschutzreform v. 5.10.2012 (WP 199)

[2] Vgl. Dokumente zu Datenschutz und Informationsfreiheit 2011, S. 22

Auch die Konferenz der Informationsfreiheitsbeauftragten in Deutschland hat erneut Entschließungen zu aktuellen Fragen der Transparenz gefasst, die hier abgedruckt sind.

Diese Dokumentensammlung kann auch über unsere Webseite abgerufen werden.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließung zwischen der 82. und 83. Konferenz (vom 7. Februar 2012)

Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte

jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen.

2. Entschließungen der 83. Konferenz am 21./22. März 2012 in Potsdam

Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer **Datenschutz-Grundverordnung** enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,

- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,

- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,
- die Förderung des Selbstdatenschutzes,
- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,
- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und
- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im **Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Da-

tenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik – insbesondere der Videoüberwachung und dem Instrument der Mustererkennung – menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder" frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT" (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

3. Entschließungen zwischen der 83. und 84. Konferenz

„Patientenrechte müssen umfassend gestärkt werden“
Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!
(vom 23. Mai 2012)

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken.

Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

– Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.

– Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.

– Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.

– Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.

– Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.

– Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z. B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

Orientierungshilfe zum datenschutzgerechten Smart Metering (vom 27. Juni 2012)

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d. h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

– Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.

– Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.

– Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.

– Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.

– Die Daten sollen an möglichst wenige Stellen übermittelt werden.

– Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.

– Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss

Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.

– Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.

– Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.

– Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.

– Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

Melderecht datenschutzkonform gestalten!
(vom 22. August 2012)

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenomme-

nen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

– Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage. Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.

– Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.

– Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.

– Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.

– Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.

– Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.

– Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

4. Entschließungen der 84. Konferenz am 7./8. November 2012 in Frankfurt (Oder)

Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der **Datenschutz-Grundverordnung** an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

  Jede Verarbeitung scheinbar, „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits

1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

- Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.

- Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.

- Mit Blick auf die **Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene“ Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfas-

sungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u. a. Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektroni-

scher Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe

fixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.

- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.

- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.

- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.

- Interface Identifier und Präfix sollten synchron gewechselt werden.

- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.

- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.

- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.

- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Diens-

tes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfix.

- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.

- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

II. Düsseldorfer Kreis – Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

1. Umlaufbeschluss (vom 17. Januar 2012)

Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung[a]

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY[1] daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z. B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung *(Krankenversicherung)*[2] benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache, dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. …[3] weiterleiten zu dürfen.

---

[a] Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.

[1] Hier und im Folgenden kann anstelle von „die Versicherung XY" der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY") jeweils „wir" eingefügt werden.

[2] Hier kann die konkrete Sparte genannt werden.

[3] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[4] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.[5]

Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY *[Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird]* selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[6]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

---

4 Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

5 Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4a Abs. 1 Satz 2 BDSG

6 Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen (siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

7 Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht[7]

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesundheitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

- Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist – meine Gesundheitsdaten bei Ärzten, Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden[8] erhebt und für diese Zwecke verwendet.

  Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen sowie Versicherungsanträgen und -verträgen aus einem Zeitraum von bis zu zehn Jahren[9] vor Antragstellung an die Versicherung XY übermittelt werden.

---

[7] Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

[8] Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35–40.

[9] Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang – soweit erforderlich – meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von ihrer Schweigepflicht.

Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.[10]

Möglichkeit II:

- Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich
  - in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
  - oder die erforderlichen Unterlagen selbst beibringe.

  Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren[11] nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte[12] dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärungen bis zu zehn Jahre nach Vertragsschluss.

2.2. Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY kon-

10 Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 S. 2 i.V.m. Abs. 4 VVG

11 Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.

12 Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

krete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:[13]

Möglichkeit I:

- Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I).

Möglichkeit II:

- Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn diese abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.[14]

3.1. Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in

[13] Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z. B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

[14] Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet.[15]

> Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XY-Gruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[16] soweit erforderlich für die anderen Stellen.[17]

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[18] über die Stellen[19] und Kategorien von Stellen[20], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertrage-

---

15 Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.

16 Der Satzteil „für sich und“ ist nur für die Kranken, Leben- und Unfallversicherung zu verwenden.

17 Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.

18 In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.

19 Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.

20 Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z. B. Krankentransporte.

nen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.[21] Eine aktuelle Liste kann auch im Internet unter *(Internetadresse)* eingesehen oder bei *(Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse)* angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,[22] dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen[23] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[24] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt.

Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrundihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt.

Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.

---

21 Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.

22 Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.

23 „und sonstige Stellen" – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.

24 Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.

Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.[25] Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.

Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet.

Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet[26].

> Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheitsdaten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[27]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.[28] Zwar werden dabei keine Ge-

---

[25] Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.

[26] Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.

[27] Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht.
Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

[28] Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.

sundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweigepflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen ist oder nicht.

> Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[29] melden.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Informationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

---

[29] Durch die Formulierung „an den jeweiligen Betreiber“ sowie die Aufnahme von „derzeit“ im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten, wenn der Vertrag nicht zustande kommt[30]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragen weiterer Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[31] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.[32]

Ort, Datum	Unterschrift Antragsteller/in oder mitzuversichernde Person
Ort, Datum	Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres)
Ort, Datum	Unterschrift des gesetzlichen Vertreters

30 Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt.
Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.

31 Es zählt das Datum der Unterschrift im Antrag.

32 Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung / Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel – BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z. B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen

vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung *dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist*.

Anlage:

Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft

I. EINLEITUNG

Der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) mit Sitz in Berlin ist die Dachorganisation der privaten Versicherer in Deutschland. Ihm gehören über 450 Mitgliedsunternehmen an. Diese bieten als Risikoträger Risikoschutz und Unterstützung sowohl für private Haushalte als auch für Industrie, Gewerbe und öffentliche Einrichtungen. Der Verband setzt sich für alle die Versicherungswirtschaft betreffenden Fachfragen und für ordnungspolitische Rahmenbedingungen ein, die den Versicherern die optimale Erfüllung ihrer Aufgaben ermöglichen.

Die Versicherungswirtschaft ist von jeher darauf angewiesen, in großem Umfang personenbezogene Daten der Versicherten zu verwenden. Sie werden zur Antrags-, Vertrags- und Leistungsabwicklung erhoben, verarbeitet und genutzt um Versicherte zu beraten und zu betreuen sowie um das zu versichernde Risiko einzuschätzen, die Leistungspflicht zu prüfen und Versicherungsmissbrauch im Interesse der Versichertengemeinschaft zu verhindern. Versicherungen können dabei heute ihre Aufgaben nur noch mit Hilfe der elektronischen Datenverarbeitung erfüllen.

Die Wahrung der informationellen Selbstbestimmung und der Schutz der Privatsphäre sowie die Sicherheit der Datenverarbeitung sind für die Versicherungswirtschaft ein Kernanliegen, um das Vertrauen der Versicherten zu gewährleisten. Alle Regelungen müssen nicht nur im Einklang mit den Bestimmungen der Europäischen Datenschutzrichtlinie, des Bundesdatenschutzgesetzes und aller bereichsspezifischen Vorschriften über den Datenschutz stehen, sondern die beigetretenen Unternehmen der Versicherungswirtschaft verpflichten sich darüber hinaus, den Grundsätzen der Transparenz, der Erforderlichkeit der verarbeiteten Daten und der Datenvermeidung und -sparsamkeit in besonderer Weise nachzukommen.

Hierzu hat der GDV im Einvernehmen mit seinen Mitgliedsunternehmen die folgenden Verhaltensregeln für den Umgang mit den personenbezogenen Daten der Versicherten aufgestellt. Sie schaffen für die Versicherungswirtschaft weitestgehend einheitliche Standards und fordern die Einhaltung von datenschutzrechtlichen Regelungen. Die für die Mitgliedsunternehmen zuständigen Aufsichtsbehörden haben den Verhaltensregeln zugestimmt. Daraufhin sind sie dem Berliner Beauftragten fur Datenschutz und Informationsfreiheit als für den GDV zuständige Aufsichtsbehörde nach § 38 a Bundesdatenschutzgesetz unterbreitet und von

ihm als mit dem geltenden Datenschutzrecht vereinbar erklärt worden. Die Mitgliedsunternehmen des GDV, die diesen Verhaltensregeln gemäß Artikel 30 beitreten, verpflichten sich damit zu deren Einhaltung.

Die Verhaltensregeln sollen den Versicherten der beigetretenen Unternehmen die Gewähr bieten, dass Datenschutz- und Datensicherheitsbelange bei der Gestaltung und Bearbeitung von Produkten und Dienstleistungen berücksichtigt werden. Der GDV versichert seine Unterstützung bei diesem Anliegen. Die beigetretenen Unternehmen weisen ihre Führungskräfte und ihre Mitarbeiterinnen und Mitarbeiter an, die Verhaltensregeln einzuhalten. Antragsteller und Versicherte werden über die Verhaltensregeln informiert.

Darüber hinaus sollen mit den Verhaltensregeln zusätzliche Einwilligungen möglichst entbehrlich gemacht werden. Grundsätzlich sind solche nur noch für die Verarbeitung von besonders sensiblen Arten personenbezogener Daten – wie Gesundheitsdaten – sowie für die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung erforderlich. Für die Verarbeitung von besonders sensiblen Arten personenbezogener Daten – wie Gesundheitsdaten – hat der GDV gemeinsam mit den zuständigen Aufsichtsbehörden Mustererklärungen mit Hinweisen zu deren Verwendung erarbeitet. Die beigetretenen Unternehmen sind von den Datenschutzbehörden aufgefordert, – angepasst an ihre Geschäftsabläufe – Einwilligungstexte zu verwenden, die der Musterklausel entsprechen.

Die vorliegenden Verhaltensregeln konkretisieren und ergänzen die Regelungen des Bundesdatenschutzgesetzes für die Versicherungsbranche. Als Spezialregelungen für die beigetretenen Mitgliedsunternehmen des GDV erfassen sie die wichtigsten Verarbeitungen personenbezogener Daten, welche die Unternehmen im Zusammenhang mit der Begründung, Durchführung, Beendigung oder Akquise von Versicherungsverträgen sowie zur Erfüllung gesetzlicher Verpflichtungen vornehmen.

Da die Verhaltensregeln geeignet sein müssen, die Datenverarbeitung aller beigetretenen Unternehmen zu regeln, sind sie möglichst allgemeingültig formuliert. Deshalb kann es erforderlich sein, dass die einzelnen Unternehmen diese in unternehmensspezifischen Regelungen konkretisieren. Das mit den Verhaltensregeln erreichte Datenschutz- und Datensicherheitsniveau wird dabei nicht unterschritten. Darüber hinaus ist es den Unternehmen unbenommen, Einzelregelungen mit datenschutzrechtlichem Mehrwert, z. B. für besonders sensible Daten wie Gesundheitsdaten oder für die Verarbeitung von Daten im Internet, zu treffen. Haben die beigetretenen Unternehmen bereits solche besonders datenschutzfreundlichen Regelungen getroffen oder bestehen mit den zuständigen Aufsichtsbehörden spezielle Vereinbarungen oder Absprachen zu besonders datenschutzgerechten Verfahrensweisen, behalten diese selbstverständlich auch nach dem Beitritt zu diesen Verhaltensregeln ihre Gültigkeit.

Unbeschadet der hier getroffenen Regelungen gelten die Vorschriften des Bundesdatenschutzgesetzes. Unberührt bleiben die Vorschriften zu Rechten und Pflichten von Beschäftigten der Versicherungswirtschaft.

II. BEGRIFFSBESTIMMUNGEN

Für die Verhaltensregeln gelten die Begriffsbestimmungen des Bundesdatenschutzgesetzes. Darüber hinaus sind:

Unternehmen:
die diesen Verhaltensregeln beigetretenen Mitgliedsunternehmen des GDV, soweit sie das Versicherungsgeschäft als Erstversicherer betreiben,

Versicherungsverhältnis:
Versicherungsvertrag einschließlich der damit im Zusammenhang stehenden rechtsgeschaftsähnlichen Schuldverhältnisse,

Betroffene:
Versicherte, Antragsteller oder weitere Personen, deren personenbezogene Daten im Zusammenhang mit dem Versicherungsgeschäft verarbeitet werden,

Versicherte:
- Versicherungsnehmer und Versicherungsnehmerinnen des Unternehmens,
- versicherte Personen einschließlich der Teilnehmer an Gruppenversicherungen,

Antragsteller:
Personen, die ein Angebot angefragt haben oder einen Antrag auf Abschluss eines Versicherungsvertrages stellen, unabhängig davon, ob der Versicherungsvertrag zustande kommt,

weitere Personen:
außerhalb des Versicherungsverhältnisses stehende Betroffene, wie Geschädigte, Zeugen und sonstige Personen, deren Daten das Unternehmen im Zusammenhang mit der Begründung, Durchführung oder Beendigung eines Versicherungsverhältnisses erhebt, verarbeitet und nutzt,

Datenerhebung:
das Beschaffen von Daten über die Betroffenen,

Datenverarbeitung:
Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten,

Datennutzung:
jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt,

Automatisierte Verarbeitung:
Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen,

Stammdaten:
die allgemeinen Kundendaten der Versicherten: Name, Adresse, Geburtsdatum, Geburtsort, Kundennummer, Versicherungsnummer(n) und vergleichbare Identifikationsdaten sowie Kontoverbindung, Telekommunikationsdaten, Werbesperren, Werbeeinwilligung und Sperren für Markt- und Meinungsforschung,

Dienstleister:
andere Unternehmen oder Personen, die eigenverantwortlich Aufgaben für das Unternehmen wahrnehmen,

Auftragnehmer:
andere Unternehmen oder Personen, die weisungsgebunden im Auftrag des Unternehmens personenbezogene Daten erheben, verarbeiten oder nutzen,

Vermittler:
selbstständig handelnde natürliche Personen (Handelsvertreter) und Gesellschaften, welche als Versicherungsvertreter oder -makler im Sinne des § 59 Versicherungsvertragsgesetz (VVG) Versicherungsverträge vermitteln oder abschließen.

III. ALLGEMEINE BESTIMMUNGEN

Art. 1 Geltungsbereich

(1) Die Verhaltensregeln gelten für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Zusammenhang mit dem Versicherungsgeschäft durch die Unternehmen. Dazu gehört neben dem Versicherungsverhältnis die Erfüllung gesetzlicher Ansprüche, auch wenn ein Versicherungsvertrag nicht zustande kommt, nicht oder nicht mehr besteht.

(2) Unbeschadet der hier getroffenen Regelungen gelten die Vorschriften des Bundesdatenschutzgesetzes.

Art. 2 Grundsatz

(1) Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfolgt grundsätzlich nur, soweit dies zur Begründung, Durchführung oder Beendigung eines Versicherungsverhältnisses erforderlich ist, insbesondere zur Bearbeitung eines Antrags, zur Beurteilung des zu versichernden Risikos, zur Erfüllung der Beratungspflichten nach § 6 VVG, zur Prüfung einer Leistungspflicht und zur internen Prüfung des fristgerechten Forderungsausgleichs. Sie erfolgt auch zur Missbrauchsbekämpfung oder zur Erfüllung gesetzlicher Verpflichtungen oder zu Zwecken der Werbung sowie der Markt- und Meinungsforschung.

(2) Die personenbezogenen Daten werden grundsätzlich im Rahmen der den Betroffenen bekannten Zweckbestimmung verarbeitet oder genutzt. Eine Änderung oder Erweiterung der Zweckbestimmung erfolgt nur, wenn sie rechtlich zulässig ist und die Betroffenen darüber informiert wurden oder wenn die Betroffenen eingewilligt haben.

Art. 3 Grundsätze zur Qualität der Datenerhebung, -verarbeitung und -nutzung

(1) Die Unternehmen verpflichten sich, alle personenbezogenen Daten in rechtmäßiger und den schutzwürdigen Interessen der Betroffenen entsprechender Weise zu erheben, zu verarbeiten und zu nutzen.

(2) Die Datenerhebung, -verarbeitung und -nutzung richtet sich an dem Ziel der Datenvermeidung und Datensparsamkeit aus, insbesondere werden die Möglichkeiten zur Anonymisierung und Pseudonymisierung genutzt, soweit dies möglich ist, und der Aufwand nicht unverhältnismäßig zu dem angestrebten Schutzzweck ist. Dabei ist die Anonymisierung der Pseudonymisierung vorzuziehen.

(3) Die verantwortliche Stelle trägt dafür Sorge, dass die vorhandenen personenbezogenen Daten richtig und auf dem aktuellen Stand gespeichert sind. Es werden angemessene Maßnahmen dafür getroffen, dass nicht zutreffende oder unvollständige Daten berichtigt, gelöscht oder gesperrt werden.

(4) Die Maßnahmen nach Absatz 3 Satz 2 werden dokumentiert. Grundsätze hierfür werden in das Datenschutzkonzept der Unternehmen aufgenommen (Artikel 4 Absatz 2).

Art. 4 Grundsätze der Datensicherheit

(1) Zur Gewährleistung der Datensicherheit werden die erforderlichen technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik ge-

troffen. Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Das sind insbesondere die in der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz enthaltenen Maßnahmen.

(2) Die in den Unternehmen veranlassten Maßnahmen werden in ein umfassendes, die Verantwortlichkeiten regelndes Datenschutz- und -sicherheitskonzept integriert, welches unter Einbeziehung der betrieblichen Datenschutzbeauftragten erstellt wird.

Art. 5 Einwilligung

(1) Soweit die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, insbesondere Daten über die Gesundheit, auf eine Einwilligung sowie – soweit erforderlich – auf eine Schweigepflichtentbindungserklärung der Betroffenen gestützt wird, stellt das Unternehmen sicher, dass diese auf der freien Entscheidung der Betroffenen beruht, wirksam und nicht widerrufen ist.

(2) Soweit die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von Minderjährigen auf eine Einwilligung sowie – soweit erforderlich – auf eine Schweigepflichtentbindungserklärung gestützt wird, werden diese Erklärungen von dem gesetzlichen Vertreter eingeholt. Frühestens mit Vollendung des 16. Lebensjahres werden diese Erklärungen bei entsprechender Einsichtsfähigkeit des Minderjährigen von diesem selbst eingeholt.

(3) Die Einwilligung und die Schweigepflichtentbindung können jederzeit mit Wirkung für die Zukunft widerrufen werden. Ist die Einwilligung zur Durchfüh-

rung des Vertrages oder der Schadensabwicklung erforderlich, ist ein Widerruf nach den Grundsätzen von Treu und Glauben ausgeschlossen oder führt dazu, dass die Leistung nicht erbracht werden kann. Diese Beschränkung der Widerrufsmöglichkeit gilt nicht für mündlich erteilte Einwilligungen.

(4) Das einholende Unternehmen bzw. der die Einwilligung einholende Vermittler stellt sicher und dokumentiert, dass die Betroffenen zuvor über die verantwortliche(n) Stelle(n), den Umfang, die Form und den Zweck der Datenerhebung, -verarbeitung oder -nutzung sowie die Möglichkeit der Verweigerung und die Widerruflichkeit der Einwilligung und deren Folgen informiert sind.

(5) Grundsätzlich wird die Einwilligung in Schriftform gemäß § 126 des Bürgerlichen Gesetzbuches eingeholt. Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, wird sie so hervorgehoben, dass sie ins Auge fällt. Im Falle besonderer Umstände, z. B. in Eilsituationen oder wenn der Kommunikationswunsch von den Betroffenen ausgegangen ist, und wenn die Einholung einer Einwilligung auf diesem Wege im besonderen Interesse der Betroffenen liegt, kann die Einwilligung auch in anderer Form als der Schriftform, z. B. in Textform oder mündlich erteilt werden.

(6) Wird die Einwilligung mündlich eingeholt, ist dies zu dokumentieren und den Betroffenen mit der nächsten Mitteilung schriftlich oder in Textform, wenn dies dem Vertrag oder der Anfrage des Betroffenen entspricht, zu bestätigen. Wird die Bestätigung in Textform erteilt, muss der Inhalt der Bestätigung unverändert reproduzierbar in den Herrschaftsbereich des Betroffenen gelangt sein.

(7) Eine Einwilligung kann elektronisch erteilt werden, wenn der Erklärungsinhalt schriftlich oder entsprechend Abs. 6 Satz 2 in Textform bestätigt wird. Bei elektronischen Einwilligungen zum Zwecke der Werbung kann die Bestätigung entfallen, wenn die Einwilligung protokolliert wird, die Betroffenen ihren Inhalt jederzeit abrufen können und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann. Bei sonstigen elektronischen Einwilligungen, insbesondere zum Zwecke eines Vertragsabschlusses, kann die Bestätigung entfallen, wenn die Abgabe der Erklärung protokolliert wird und der Inhalt vor der Abgabe der Erklärung zum Vertragsschluss unverändert reproduzierbar in den Herrschaftsbereich der Betroffenen gelangt ist, zum Beispiel durch einen Download, und die Betroffenen unmittelbar danach den Erhalt und die Lesbarkeit, etwa durch Anklicken eines Feldes, versichert haben.

(8) Die Bestätigung der Einwilligung zu Werbezwecken in mündlicher oder in elektronischer Form erfolgt spätestens mit der nächsten Mitteilung. Sonstige mündlich oder elektronisch erteilte Einwilligungen werden zeitnah bestätigt.

Art. 6 Besondere Arten personenbezogener Daten

(1) Besondere Arten personenbezogener Daten im Sinne des Bundesdatenschutzgesetzes (insbesondere Angaben über die Gesundheit) werden grundsätzlich mit Einwilligung der Betroffenen nach Artikel 5 und – soweit erforderlich – aufgrund einer Schweigepflichtentbindung erhoben, verarbeitet oder genutzt. In diesem Fall muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

(2) Darüber hinaus werden besondere Arten personenbezogener Daten auf gesetzlicher Grundlage erhoben, verarbeitet oder genutzt. Dies ist insbesondere dann zulässig, wenn es zur Gesundheitsvorsorge bzw. -versorgung im Rahmen der Aufgabenerfüllung der privaten Krankenversicherungsunternehmen erforderlich ist oder wenn es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche – auch im Rahmen eines Rechtsstreits – erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt.

IV. DATENERHEBUNG

Art. 7 Datenerhebung bei den Betroffenen, Informationspflichten und -rechte und Erhebung von Daten weiterer Personen

(1) Personenbezogene Daten werden grundsätzlich bei den Betroffenen unter Berücksichtigung von §§ 19, 31 VVG selbst erhoben.

(2) Die Unternehmen stellen sicher, dass die Betroffenen über die Identität der verantwortlichen Stelle (Name, Sitz), die Zwecke der Datenerhebung, -verarbeitung oder -nutzung und die Kategorien von Empfängern unterrichtet werden. Diese Informationen werden vor oder spätestens bei der Erhebung gegeben, es sei denn, die Betroffenen haben bereits auf andere Weise Kenntnis von ihnen erlangt.

(3) Die Betroffenen werden auf ihre in Abschnitt VIII festgelegten Rechte hingewiesen.

(4) Personenbezogene Daten weiterer Personen im Sinne dieser Verhaltensregeln werden nur erhoben, wenn dies zur Begründung, Durchführung oder Beendigung des Versicherungsverhältnisses erforderlich ist und keine Anhaltspunkte für eine Beeinträchtigung überwiegender schutzwürdiger Interessen dieser Personen bestehen.

Art. 8 Datenerhebung ohne Mitwirkung der Betroffenen

(1) Abweichend von Artikel 7 Absatz 1 werden Daten nur dann ohne Mitwirkung der Betroffenen erhoben, wenn dies zur Begründung, Durchführung oder Beendigung des Versicherungsverhältnisses erforderlich ist oder die Erhebung bei den Betroffenen einen unverhältnismäßigen Aufwand erfordern wurde und keine Anhaltspunkte für eine Beeinträchtigung überwiegender schutzwürdiger Interessen der Betroffenen bestehen, insbesondere wenn der Versicherungsnehmer bei Gruppenversicherungen zulässigerweise die Daten der versicherten Personen oder bei Lebensversicherungen die Daten der Bezugsberechtigten angibt.

(2) Die Erhebung von Gesundheitsdaten bei Dritten erfolgt – soweit erforderlich – mit wirksamer Schweigepflichtentbindungserklärung der Betroffenen und nach Masgabe des § 213 VVG.

(3) Das Unternehmen, das personenbezogene Daten ohne Mitwirkung der Betroffenen erhebt, stellt sicher, dass die Betroffenen anlässlich der ersten Speicherung über diese, die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle informiert werden. Die Information unterbleibt, soweit die Betroffenen auf andere Weise von der Speicherung Kenntnis erlangt haben, wenn für eigene Zwecke gespeicherte Daten aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Falle unverhältnismäßig ist oder wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen.

V. VERARBEITUNG PERSONENBEZOGENER DATEN

Art. 9 Gemeinsame Verarbeitung von Daten innerhalb der Unternehmensgruppe

(1) Wenn das Unternehmen einer Gruppe von Versicherungs- und Finanzdienstleistungsunternehmen angehort, können die Stammdaten von Antragstellern und Versicherten sowie Angaben über die Art der bestehenden Verträge zur zentralisierten Bearbeitung von bestimmten Verfahrensabschnitten im Geschäftsablauf (z. B. Telefonate, Post, Inkasso) in einem von Mitgliedern der Gruppe gemeinsam nutzbaren Datenverarbeitungsverfahren erhoben, verarbeitet oder genutzt werden, wenn sichergestellt ist, dass die technischen und organisatorischen Maßnahmen den datenschutzrechtlichen Anforderungen entsprechen und die Einhaltung dieser Verhaltensregeln (insbesondere der Artikel 21 und 22) durch die für das gemeinsame Verfahren verantwortliche Stelle gewährleistet ist.

(2) Stammdaten weiterer Personen werden in gemeinsam nutzbaren Datenverarbeitungsverfahren nur erhoben verarbeitet und genutzt, soweit dies für den jeweiligen Zweck erforderlich ist. Dies ist technisch und organisatorisch zu gewährleisten.

(3) Abweichend von Absatz 1 können die Versicherungsunternehmen der Gruppe auch weitere Daten aus Anträgen und Verträgen anderer Unternehmen der Gruppe verwenden. Dies setzt voraus, dass dies zum Zweck der Beurteilung des konkreten Risikos eines neuen Vertrages vor dessen Abschluss erforderlich ist. Die Betroffenen müssen auf das Vorhandensein von Daten in einem anderen Unternehmen der Gruppe hingewiesen haben oder erkennbar vom Vorhandensein ihrer Daten in einem anderen Unternehmen der Gruppe ausgegangen sein sowie in den Datenabruf eingewilligt haben.

(4) Erfolgt eine gemeinsame Erhebung, Verarbeitung oder Nutzung von Daten gemäß Absatz 1, werden die Versicherten darüber bei Vertragsabschluss oder bei Neueinrichtung eines solchen Verfahrens in Textform informiert.

(5) Das Unternehmen hält eine aktuelle Liste aller Unternehmen der Gruppe bereit, die an einer zentralisierten Bearbeitung teilnehmen und macht diese in geeigneter Form bekannt.

(6) Nimmt ein Unternehmen für ein anderes Mitglied der Gruppe Datenerhebungen, -verarbeitungen oder -nutzungen vor, richtet sich dies nach Artikel 21 oder 22 dieser Verhaltensrichtlinie.

Art. 10 Tarifkalkulation und Prämienberechnung

(1) Die Versicherungswirtschaft errechnet auf der Basis von Statistiken und Erfahrungswerten mit Hilfe versicherungsmathematischer Methoden die Wahrscheinlichkeit des Eintritts von Versicherungsfällen sowie deren Schadenhöhe und entwickelt auf dieser Grundlage Tarife. Dazu werten Unternehmen Daten aus Versicherungsverhältnissen ausschließlich in anonymisierter oder – soweit dies für die vorgenannten Zwecke nicht ausreichend ist – pseudonymisierter Form aus.

(2) Eine Übermittlung von Daten an den Gesamtverband der Deutschen Versicherungswirtschaft, den Verband der privaten Krankenversicherung e.V. oder andere Stellen zur Errechnung unternehmensübergreifender Statistiken oder zur Tarifkalkulation erfolgt nur in anonymisierter oder – soweit erforderlich – pseudonymisierter Form. Der Rückschluss auf die Betroffenen ist auszuschließen.

(3) Zur Ermittlung der risikogerechten Prämie werden diese Tarife auf die individuelle Situation des Antragstellers angewandt. Darüber hinaus kann eine Be-

wertung des individuellen Risikos des Antragstellers durch spezialisierte Risikoprüfer, z. B. Ärzte, in die Prämienermittlung einfließen. Hierzu werden auch personenbezogene Daten verwendet, die im Rahmen dieser Verhaltensrichtlinie erhoben worden sind.

Art. 11 Scoring

Für das Scoring gelten die gesetzlichen Regelungen, insbesondere § 28 b BDSG.

Art. 12 Bonitätsdaten

Für die Erhebung, Verarbeitung und Nutzung von Bonitätsdaten gelten die gesetzlichen Regelungen.

Art. 13 Automatisierte Einzelentscheidungen

(1) Entscheidungen, die für die Betroffenen eine negative rechtliche oder wirtschaftliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, werden grundsätzlich nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Dies wird organisatorisch sicher gestellt. Die Informationstechnik wird grundsätzlich nur als Hilfsmittel für eine Entscheidung herangezogen, ohne dabei deren einzige Grundlage zu bilden. Dies gilt nicht, wenn einem Begehren der Betroffenen in vollem Umfang stattgegeben wird.

(2) Sofern automatisierte Entscheidungen zu Lasten der Betroffenen getroffen werden, wird dies den Betroffenen von der verantwortlichen Stelle unter Hinweis auf das Auskunftsrecht mitgeteilt. Auf Verlangen werden den Betroffenen auch der logische Aufbau der automatisierten Verarbeitung sowie die wesentlichen Gründe dieser Entscheidung mitgeteilt und erläutert, um ihnen die Geltendmachung ihres Standpunktes zu ermöglichen. Die Information über den logischen Aufbau umfasst die verwendeten Datenarten sowie ihre Bedeutung für die automatisierte Entscheidung. Die Entscheidung wird auf dieser Grundlage in einem nicht ausschließlich automatisierten Verfahren erneut geprüft.

(3) Der Einsatz automatisierter Entscheidungshilfen wird dokumentiert.

Art. 14 Hinweis- und Informationssystem (HIS)

(1) Die Unternehmen der deutschen Versicherungswirtschaft – mit Ausnahme der privaten Krankenversicherer – nutzen ein Hinweis- und Informationssystem (HIS) zur Unterstützung der Risikobeurteilung im Antragsfall, zur Sachverhaltsaufklarung bei der Leistungsprüfung sowie bei der Bekämpfung von Versicherungsmissbrauch. Der Betrieb und die Nutzung des HIS erfolgen nach den Rege-

lungen des Bundesdatenschutzgesetzes zur geschäftsmäßigen Datenerhebung und -speicherung zum Zweck der Übermittlung (Auskunftei).

(2) Das HIS wird getrennt nach Versicherungssparten betrieben. In allen Sparten wird der Datenbestand in jeweils zwei Datenpools getrennt verarbeitet: in einem Datenpool für die Abfrage zur Risikoprüfung im Antragsfall (A-Pool) und in einem Pool für die Abfrage zur Leistungsprüfung (L-Pool). Die Unternehmen richten die Zugriffsberechtigungen für ihre Mitarbeiter entsprechend nach Sparten und Aufgaben getrennt ein.

(3) Die Unternehmen melden bei Vorliegen festgelegter Einmeldekriterien Daten zu Personen, Fahrzeugen oder Immobilien an den Betreiber des HIS, wenn ein erhöhtes Risiko vorliegt oder eine Auffälligkeit, die auf Versicherungsmissbrauch hindeuten konnte. Vor einer Einmeldung von Daten zu Personen erfolgt eine Abwägung der Interessen der Unternehmen und des Betroffenen. Bei Vorliegen der festgelegten Meldekriterien ist regelmäßig von einem überwiegenden berechtigten Interesse des Unternehmens an der Einmeldung auszugehen. Besondere Arten personenbezogener Daten, wie z. B. Gesundheitsdaten, werden nicht an das HIS gemeldet.

(4) Die Unternehmen informieren die Versicherungsnehmer bereits bei Vertragsabschluss in allgemeiner Form über das HIS unter Angabe der verantwortlichen Stelle mit deren Kontaktdaten. Sie benachrichtigen anlässlich der Einmeldung die Betroffenen über die Art der gemeldeten Daten, den Zweck der Meldung, den Datenempfänger und den möglichen Abruf der Daten.

(5) Ein Abruf von Daten aus dem HIS kann bei Antragstellung und im Leistungsfall erfolgen, nicht jedoch bei Auszahlung einer Kapitallebensversicherung im Erlebensfall. Der Datenabruf ist nicht die alleinige Grundlage für eine Entscheidung im Einzelfall. Die Informationen werden lediglich als Hinweis dafür gewertet, dass der Sachverhalt einer näheren Prüfung bedarf. Alle Datenabrufe erfolgen im automatisierten Abrufverfahren und werden protokolliert für Revisionszwecke und den Zweck, stichprobenartig deren Berechtigung prüfen zu können.

(6) Soweit zur weiteren Sachverhaltsaufklärung erforderlich, können im Leistungsfall auch Daten zwischen dem einmeldenden und dem abrufenden Unternehmen ausgetauscht werden, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Der Datenaustausch wird dokumentiert. Soweit der Datenaustausch nicht gemäß Artikel 15 erfolgt, werden die Betroffenen über den Datenaustausch informiert. Eine Information ist nicht erforderlich, solange die Aufklärung des Sachverhalts dadurch gefährdet wurde oder wenn die Betroffenen auf andere Weise Kenntnis vom Datenaustausch erlangt haben.

(7) Die im HIS gespeicherten Daten werden spätestens am Ende des 4. Jahres nach dem Vorliegen der Voraussetzung für die Einmeldung gelöscht. Zu einer Verlängerung der Speicherdauer auf maximal 10 Jahre kommt es in der Lebensversicherung im Leistungsbereich oder bei erneuter Einmeldung innerhalb der regulären Speicherzeit gemäß Satz 1. Daten zu Anträgen, bei denen kein Vertrag zustande gekommen ist, werden im HIS spätestens am Ende des 3. Jahres nach dem Jahr der Antragstellung gelöscht.

(8) Der Gesamtverband der Deutschen Versicherungswirtschaft gibt unter Beachtung datenschutzrechtlicher Vorgaben einen detaillierten Leitfaden zur Nutzung des HIS an die Unternehmen heraus.

Art. 15 Aufklärung von Widersprüchlichkeiten

(1) Ergeben sich bei oder nach Vertragsschluss für den Versicherer konkrete Anhaltspunkte dafür, dass bei der Antragstellung oder bei Aktualisierungen von Antragsdaten während des Versicherungsverhältnisses unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde oder dass falsche oder unvollständige Sachverhaltsangaben bei der Feststellung eines entstandenen Schadens gemacht wurden, nimmt das Unternehmen ergänzende Datenerhebungen, -verarbeitungen und -nutzungen vor, soweit dies zur Aufklärung der Widersprüchlichkeiten erforderlich ist.

(2) Ergänzende Datenerhebungen, -verarbeitungen und -nutzungen zur Überprüfung der Angaben zur Risikobeurteilung bei Antragstellung erfolgen nur innerhalb von fünf Jahren, bei Krankenversicherungen innerhalb von drei Jahren nach Vertragsschluss. Diese Frist kann sich verlängern, wenn die Anhaltspunkte für eine Anzeigepflichtverletzung dem Unternehmen erst nach Ablauf der Frist durch Prüfung eines in diesem Zeitraum aufgetretenen Schadens bekannt werden. Bestehen konkrete Anhaltspunkte dafür, dass der Versicherungsnehmer bei der Antragstellung vorsätzlich oder arglistig unrichtige oder unvollständige Angaben gemacht hat, verlängert sich dieser Zeitraum auf 10 Jahre.

(3) Ist die ergänzende Erhebung, Verarbeitung oder Nutzung von besonderen Arten personenbezogener Daten, insbesondere von Daten über die Gesundheit, nach Absatz 1 erforderlich, werden die Betroffenen entsprechend ihrer Erklärung im Versicherungsantrag vor einer Datenerhebung nach § 213 Abs. 2 VVG unterrichtet und auf ihr Widerspruchsrecht hingewiesen oder von den Betroffenen wird zuvor eine eigenständige Einwilligungs- und Schweigepflichtentbindungserklärung eingeholt.

Art. 16 Datenaustausch mit anderen Versicherern

(1) Ein Datenaustausch zwischen einem Vorversicherer und seinem nachfolgenden Versicherer wird zur Erhebung tarifrelevanter oder leistungsrelevanter Anga-

ben unter Beachtung des Artikels 8 Abs. 1 vorgenommen. Dies ist insbesondere der Fall, wenn die Angaben erforderlich sind:

1. bei der Risikoeinschätzung zur Überprüfung von Schadenfreiheitsrabatten, insbesondere der Schadensfreiheitsklassen in der Kfz-Haftpflichtversicherung und Vollkaskoversicherung,
2. zur Übertragung von Ansprüchen auf Altersvorsorge bei Anbieter- oder Arbeitgeberwechsel,
3. zur Übertragung von Altersrückstellungen in der Krankenversicherung auf den neuen Versicherer,
4. zur Ergänzung oder Verifizierung der Angaben der Antragsteller oder Versicherten.

In den Fällen der Nummern 1 und 4 ist der Datenaustausch zum Zweck der Risikoprüfung nur zulässig, wenn die Betroffenen bei Datenerhebung im Antrag über den möglichen Datenaustausch und dessen Zweck und Gegenstand informiert werden. Nach einem Datenaustausch zum Zweck der Leistungsprüfung werden die Betroffenen über einen erfolgten Datenaustausch im gleichen Umfang informiert. Artikel 15 bleibt unberührt.

(2) Ein Datenaustausch mit anderen Versicherern außerhalb der für das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) getroffenen Regelungen erfolgt darüber hinaus, soweit dies zur Prüfung und Abwicklung gemeinsamer, mehrfacher oder kombinierter Absicherung von Risiken, des gesetzlichen Übergangs einer Forderung gegen eine andere Person oder zur Regulierung von Schäden zwischen mehreren Versicherern über bestehende Teilungs- und Regressverzichtsabkommen erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen dem entgegen steht.

(3) Der Datenaustausch wird dokumentiert.

Art. 17 Datenübermittlung an Rückversicherer

(1) Um jederzeit zur Erfüllung ihrer Verpflichtungen aus den Versicherungsverhältnissen in der Lage zu sein, geben Unternehmen einen Teil ihrer Risiken aus den Versicherungsverträgen an Rückversicherer weiter. Zum weiteren Risikoausgleich bedienen sich in einigen Fällen diese Rückversicherer ihrerseits weiterer Rückversicherer. Zur ordnungsgemäßen Begründung, Durchführung oder Beendigung des Rückversicherungsvertrages werden in anonymisierter oder – soweit dies für die vorgenannten Zwecke nicht ausreichend ist – pseudonymisierter Form Daten aus dem Versicherungsantrag oder -verhältnis, insbesondere Versicherungsnummer, Beitrag, Art und Höhe des Versicherungsschutzes und des Risikos sowie etwaige Risikozuschläge weitergegeben.

(2) Personenbezogene Daten erhalten die Rückversicherer nur, soweit dies erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen dem entgegensteht. Dies kann der Fall sein, wenn im Rahmen des konkreten Rückversicherungsverhältnisses die Übermittlung personenbezogener Daten an Rückversicherer aus folgenden Gründen erfolgt:

1. Die Rückversicherer führen z. B. bei hohen Vertragssummen oder bei einem schwer einzustufenden Risiko im Einzelfall die Risikoprüfung und die Leistungsprüfung durch,
2. die Rückversicherer unterstützen die Unternehmen bei der Risiko- und Schadenbeurteilung sowie bei der Bewertung von Verfahrensabläufen,
3. die Rückversicherer erhalten zur Bestimmung des Umfangs der Rückversicherungsverträge einschließlich der Prüfung, ob und in welcher Höhe sie an ein und demselben Risiko beteiligt sind (Kumulkontrolle) sowie zu Abrechnungszwecken Listen über den Bestand der unter die Rückversicherung fallenden Verträge,
4. die Risiko- und Leistungsprüfung durch den Erstversicherer wird von den Rückversicherern stichprobenartig kontrolliert zur Prüfung ihrer Leistungspflicht gegenüber dem Erstversicherer.

(3) Die Unternehmen vereinbaren mit den Rückversicherern, dass personenbezogene Daten von diesen nur zu den in Absatz 2 genannten Zwecken verwendet werden. Soweit die Unternehmen einer Verschwiegenheitspflicht gemäß § 203 StGB unterliegen, verpflichten sie die Rückversicherer hinsichtlich der Daten, die sie nach Absatz 2 erhalten, Verschwiegenheit zu wahren und weitere Rückversicherer sowie Stellen, die für sie tätig sind, zur Verschwiegenheit zu verpflichten.

(4) Besondere Arten personenbezogener Daten, insbesondere Gesundheitsdaten, erhal-ten die Rückversicherer nur, wenn die Voraussetzungen des Artikels 6 erfüllt sind.

VI. VERARBEITUNG PERSONENBEZOGENER DATEN FÜR VERTRIEBSZWECKE UND ZUR MARKT- UND MEINUNGSFORSCHUNG

Art. 18 Verwendung von Daten für Zwecke der Werbung

Personenbezogene Daten werden für Zwecke der Werbung nur auf der Grundlage von § 28 Abs. 3 bis 4 BDSG und unter Beachtung von § 7 UWG erhoben, verarbeitet und genutzt.

Art. 19 Markt- und Meinungsforschung

(1) Die Unternehmen führen Markt- und Meinungsforschung unter besonderer Berücksichtigung der schutzwürdigen Interessen der Betroffenen durch.

(2) Soweit die Unternehmen andere Stellen mit der Markt- und Meinungsforschung beauftragen, ist die empfangende Stelle unter Nachweis der Einhaltung der Datenschutzstandards auszuwählen. Vor der Datenweitergabe sind die Einzelheiten des Forschungsvorhabens vertraglich nach den Vorgaben des Artikel 21 oder 22 zu regeln. Dabei ist insbesondere festzulegen:

a) dass die übermittelten und zusätzlich erhobenen Daten frühestmöglich anonymisiert werden,

b) dass die Auswertung der Daten sowie die Übermittlung der Ergebnisse der Markt- und Meinungsforschung an die Unternehmen ausschließlich in anonymisierter Form erfolgen.

(3) Soweit die Unternehmen selbst personenbezogene Daten zum Zweck der Markt- und Meinungsforschung verarbeiten oder nutzen, werden die Daten frühestmöglich anonymisiert. Die Ergebnisse werden ausschließlich in anonymisierter Form gespeichert oder genutzt.

(4) Soweit im Rahmen der Markt- und Meinungsforschung geschäftliche Handlungen vorgenommen werden, die als Werbung zu werten sind, beispielsweise wenn bei der Datenerhebung auch absatzfördernde Äußerungen erfolgen, richtet sich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten dafür nach den in Artikel 18 getroffenen Regelungen.

Art. 20 Datenübermittlung an selbstständige Vermittler

(1) Eine Übermittlung personenbezogener Daten erfolgt an den betreuenden Vermittler nur, soweit es zur bedarfsgerechten Vorbereitung oder Bearbeitung eines konkreten Antrags bzw. Vertrags oder zur ordnungsgemäßen Durchführung der Versicherungsangelegenheiten der Betroffenen erforderlich ist. Die Vermittler werden auf ihre besonderen Verschwiegenheitspflichten wie das Berufs- oder Datengeheimnis hingewiesen.

(2) Vor der erstmaligen Übermittlung personenbezogener Daten an einen Versicherungsvertreter oder im Falle eines Wechsels vom betreuenden Versicherungsvertreter auf einen anderen Versicherungsvertreter informiert das Unternehmen die Versicherten oder Antragsteller vorbehaltlich der Regelung des Abs. 3 vor der Übermittlung ihrer personenbezogenen Daten über den bevorstehenden Datentransfer, die Identität (Name, Sitz) des neuen Versicherungsvertreters und ihr

Widerspruchsrecht. Eine Information durch den bisherigen Versicherungsvertreter steht einer Information durch das Unternehmen gleich. Im Falle eines Widerspruchs findet die Datenübermittlung grundsätzlich nicht statt. In diesem Fall wird die Betreuung durch einen anderen Versicherungsvertreter oder das Unternehmen selbst angeboten.

(3) Eine Ausnahme von Absatz 2 besteht, wenn die ordnungsgemäße Betreuung der Versicherten im Einzelfall oder wegen des unerwarteten Wegfalls der Betreuung der Bestand der Vertragsverhältnisse gefährdet ist.

(4) Personenbezogene Daten von Versicherten oder Antragstellern dürfen an einen Versicherungsmakler übermittelt werden, wenn diese dem Makler eine Maklervollmacht erteilt haben. Für den Fall des Wechsels des Maklers gilt Absatz 2 entsprechend.

(5) Eine Übermittlung von Gesundheitsdaten durch das Unternehmen an den betreuenden Vermittler erfolgt grundsätzlich nicht, es sei denn, es liegt eine Einwilligung der Betroffenen vor. Gesetzliche Übermittlungsbefugnisse bleiben hiervon unberührt.

VII. DATENVERARBEITUNG IM AUFTRAG UND FUNKTIONSÜBERTRAGUNG

Art. 21 Pflichten bei der Datenerhebung und -verarbeitung im Auftrag

(1) Sofern ein Unternehmen personenbezogene Daten gemäß § 11 BDSG im Auftrag erheben, verarbeiten oder nutzen lässt (z. B. Elektronische Datenverarbeitung, Scannen und Zuordnung von Eingangspost, Adressverwaltung, Schaden- und Leistungsbearbeitung ohne selbstständigen Entscheidungsspielraum, Sicherstellung der korrekten Verbuchung von Zahlungseingängen, Zahlungsausgang, Inkasso ohne selbstständigen Forderungseinzug, Entsorgung von Dokumenten) wird der Auftragnehmer mindestens gemäß § 11 Abs. 2 BDSG vertraglich verpflichtet. Es wird nur ein solcher Auftragnehmer ausgewählt, der alle für die Verarbeitung notwendigen technischen und organisatorischen Anforderungen und Sicherheitsvorkehrungen durch geeignete Maßnahmen gewährleistet. Das Unternehmen überzeugt sich vor Auftragserteilung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen und dokumentiert die Ergebnisse.

(2) Jede Datenerhebung, -verarbeitung oder -nutzung ist nur im Rahmen der Weisungen des Unternehmens zulässig. Vertragsklauseln sollen den Beauftragten für den Datenschutz vorgelegt werden, die bei Bedarf beratend mitwirken.

(3) Das Unternehmen hält eine aktuelle Liste der Auftragnehmer bereit. Ist die systematische automatisierte Verarbeitung personenbezogener Daten nicht Hauptgegenstand des Auftrags, können die Auftragsdatenverarbeiter in Kategorien zusammengefasst werden unter Bezeichnung ihrer Aufgabe. Dies gilt auch für Auftragnehmer, die nur einmalig tätig werden. Die Liste wird in geeigneter Form bekannt gegeben. Werden personenbezogene Daten bei den Betroffenen erhoben, sind sie grundsätzlich bei Erhebung über die Liste zu unterrichten.

Art. 22 Funktionsübertragung an Dienstleister

(1) Die Übermittlung von personenbezogenen Daten an Dienstleister zur eigenverantwortlichen Aufgabenerfüllung erfolgt, soweit dies für die Zweckbestimmung des Versicherungsverhältnisses mit den Betroffenen erforderlich ist. Das ist insbesondere der Fall, wenn Sachverständige mit der Begutachtung eines Versicherungsfalls beauftragt sind oder wenn Dienstleister zur Ausführung der vertraglich vereinbarten Versicherungsleistungen, die eine Sachleistung beinhalten, eingeschaltet werden (sog. Assistance).

(2) Die Übermittlung von personenbezogenen Daten an Dienstleister zur eigenverantwortlichen Erfüllung von Datenverarbeitungs- oder sonstigen Aufgaben kann auch dann erfolgen, wenn dies zur Wahrung der berechtigten Interessen des Unternehmens erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen dem entgegen steht. Das kann zum Beispiel der Fall sein, wenn Dienstleister Aufgaben übernehmen, die der Geschäftsabwicklung des Unternehmens dienen, wie beispielsweise die Risikoprüfung, Schaden- und Leistungsbearbeitung, Inkasso mit selbständigem Forderungseinzug oder die Bearbeitung von Rechtsfällen und die Voraussetzungen der Absätze 4 bis 7 erfüllt sind.

(3) Die Übermittlung von personenbezogenen Daten an Dienstleister nach Absatz 1 und 2 unterbleibt, soweit der Betroffene dieser widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse des übermittelnden Unternehmens überwiegt. Die Betroffenen werden in geeigneter Weise darauf hingewiesen.

(4) Das Unternehmen schließt mit den Dienstleistern, die in seinem Interesse tätig werden, eine vertragliche Vereinbarung, die mindestens folgende Punkte enthalten muss:

– Eindeutige Beschreibung der Aufgaben des Dienstleisters;

– Sicherstellung, dass die übermittelten Daten nur im Rahmen der vereinbarten Zweckbestimmung verarbeitet oder genutzt werden;
– Gewährleistung eines Datenschutz- und Datensicherheitsstandards, der diesen Verhaltensregeln entspricht;
– Verpflichtung des Dienstleisters, dem Unternehmen alle Auskünfte zu erteilen, die zur Erfüllung einer beim Unternehmen verbleibenden Auskunftspflicht erforderlich sind oder dem Betroffenen direkt Auskunft zu erteilen.

Diese Aufgabenauslagerungen werden im Verfahrensverzeichnis abgebildet.

(5) Unternehmen und Dienstleister vereinbaren zusätzlich, dass Betroffene, welche durch die Übermittlung ihrer Daten an den Dienstleister oder die Verarbeitung ihrer Daten durch diesen einen Schaden erlitten haben, berechtigt sind, von beiden Parteien Schadenersatz zu verlangen. Vorrangig tritt gegenüber den Betroffenen das Unternehmen für den Ersatz des Schadens ein. Die Parteien vereinbaren, dass sie gesamtschuldnerisch haften und sie nur von der Haftung befreit werden können, wenn sie nachweisen, dass keine von ihnen für den erlittenen Schaden verantwortlich ist.

(6) Das Unternehmen hält eine aktuelle Liste der Dienstleister bereit, an die Aufgaben im Wesentlichen übertragen werden. Ist die systematische automatisierte Verarbeitung personenbezogener Daten nicht Hauptgegenstand des Vertrages können die Dienstleister in Kategorien zusammengefasst werde unter Bezeichnung ihrer Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden. Die Liste wird in geeigneter Form bekannt gegeben. Werden personenbezogene Daten bei den Betroffenen erhoben, sind sie grundsätzlich bei Erhebung über die Liste zu unterrichten.

(7) Das Unternehmen stellt sicher, dass die Auskunftsrechte der Betroffenen gemäß Artikel 23 durch die Einschaltung des Dienstleisters nicht geschmälert werden.

(8) Besondere Arten personenbezogener Daten dürfen in diesem Rahmen nur erhoben, verarbeitet oder genutzt werden, wenn die Betroffenen eingewilligt haben oder die Voraussetzungen des Artikels 6 Absatz 2 vorliegen. Soweit die Unternehmen einer Verschwiegenheitspflicht gemäß § 203 StGB unterliegen, verpflichten sie die Dienstleister hinsichtlich der Daten, die sie nach den Absätzen 1 und 2 erhalten, Verschwiegenheit zu wahren und weitere Dienstleister sowie Stellen, die für sie tätig sind, zur Verschwiegenheit zu verpflichten.

VIII. RECHTE DER BETROFFENEN

Art. 23 Auskunftsanspruch

(1) Betroffene können schriftlich, telefonisch, mit Faxgerät oder elektronischer Post Auskunft über die beim Unternehmen über sie gespeicherten Daten verlangen. Ihnen wird dann entsprechend ihrer Anfrage Auskunft darüber erteilt, welche personenbezogenen Daten welcher Herkunft über sie zu welchen Zwecken beim Unternehmen gespeichert sind. Im Falle einer (geplanten) Übermittlung wird den Betroffenen auch über die Dritten oder die Kategorien von Dritten, an die seine Daten übermittelt werden (sollen), Auskunft erteilt.

(2) Eine Auskunft kann nur unterbleiben, wenn sie die Geschäftszwecke des Unternehmens erheblich gefährden würde, insbesondere wenn aufgrund besonderer Umstände ein überwiegendes Interesse an der Wahrung eines Geschäftsgeheimnisses besteht, es sei denn, dass das Interesse an der Auskunft die Gefährdung überwiegt oder wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen des überwiegenden rechtlichen Interesses eines Dritten geheim gehalten werden müssen.

(3) Im Falle einer Rückversicherung (Artikel 17) oder einer Funktionsübertragung an Dienstleister (Artikel 22) nimmt das Unternehmen die Auskunftsverlangen entgegen und erteilt auch alle Auskünfte, zu denen der Rückversicherer bzw. Dienstleister verpflichtet ist oder es stellt die Auskunftserteilung durch diesen sicher.

Art. 24 Ansprüche auf Berichtigung, Löschung und Sperrung

(1) Erweisen sich die gespeicherten personenbezogenen Daten als unrichtig oder unvollständig, werden diese berichtigt.

(2) Personenbezogene Daten werden unverzüglich gelöscht, wenn die Erhebung oder Verarbeitung von Anfang an unzulässig war, die Verarbeitung oder Nutzung sich auf Grund nachträglich eingetretener Umstände als unzulässig erweist oder die Kenntnis der Daten für die verantwortliche Stelle zur Erfüllung des Zwecks der Verarbeitung oder Nutzung nicht mehr erforderlich ist.

(3) Die Prüfung des Datenbestandes auf die Notwendigkeit einer Löschung nach Absatz 2 erfolgt in regelmäßigen Abständen, mindestens einmal jährlich.

(4) An die Stelle einer Löschung tritt eine Sperrung, soweit der Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten entgegenstehen, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt würden oder die Löschung wegen der

besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Personenbezogene Daten werden ferner gesperrt, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen lässt.

(5) Das Unternehmen benachrichtigt empfangende Stellen, insbesondere Rückversicherer und Versicherungsvertreter über eine erforderliche Berichtigung, Löschung oder Sperrung der Daten.

(6) Soweit die Berichtigung, Löschung oder Sperrung der Daten aufgrund eines Antrags der Betroffenen erfolgte, werden diese nach der Ausführung hierüber unterrichtet.

IX. EINHALTUNG UND KONTROLLE

Art. 25 Verantwortlichkeit

(1) Die Unternehmen gewährleisten als verantwortliche Stellen, dass die Anforderungen des Datenschutzes und der Datensicherheit beachtet werden.

(2) Beschäftigte, die mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind, werden auf das Datengeheimnis gemäß § 5 Bundesdatenschutzgesetz verpflichtet. Sie werden darüber unterrichtet, dass Verstöße gegen datenschutzrechtliche Vorschriften auch als Ordnungswidrigkeit geahndet oder strafrechtlich verfolgt werden und Schadensersatzansprüche nach sich ziehen können. Verletzungen datenschutzrechtlicher Vorschriften, für die einzelne Beschäftigte verantwortlich gemacht werden können, können entsprechend dem jeweils geltenden Recht arbeitsrechtliche Sanktionen nach sich ziehen.

(3) Die Verpflichtung der Beschäftigten auf das Datengeheimnis gilt auch über das Ende des Beschäftigungsverhältnisses hinaus.

Art. 26 Transparenz

(1) Auf Anfrage werden die Angaben über die eingesetzten automatisierten Datenverarbeitungsverfahren zugänglich gemacht, die der Meldepflicht an die betrieblichen Beauftragten für den Datenschutz unterliegen und bei diesen im Verfahrensverzeichnis gespeichert sind (§ 4e Satz 1 Nr. 1 bis 8 BDSG).

(2) Informationen nach Absatz 1 sowie Informationen über datenverarbeitende Stellen, eingesetzte Datenverarbeitungsverfahren oder den Beitritt zu diesen Ver-

haltensregeln, die in geeigneter Form bekannt zu geben sind (Artikel 9 Absatz 5, Artikel 21 Absatz 3, Artikel 22 Absatz 6, Artikel 27 Absatz 5, Artikel 28 Absatz 1 Satz 2 und Artikel 30 Absatz 1), werden im Internet veröffentlicht; in jedem Fall werden sie auf Anfrage in Schriftform (Briefpost) oder einer der Anfrage entsprechenden Textform (Telefax, elektronische Post) zugesandt. Artikel 23 Absatz 2 Satz 1 gilt entsprechend.

Art. 27 Beauftragte für den Datenschutz

(1) Jedes Unternehmen benennt entsprechend den Vorschriften des Bundesdatenschutzgesetzes einen Beauftragten für den Datenschutz als weisungsunabhängiges Organ, welches auf die Einhaltung der anwendbaren nationalen und internationalen Datenschutzvorschriften sowie dieser Verhaltensregeln hinwirkt. Das Unternehmen trägt der Unabhängigkeit vertraglich Rechnung.

(2) Die Beauftragten überwachen die ordnungsgemäße Anwendung der im Unternehmen eingesetzten Datenverarbeitungsprogramme und werden zu diesem Zweck vor der Einrichtung oder nicht nur unbedeutenden Veränderung eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten rechtzeitig unterrichtet und wirken hieran beratend mit.

(3) Dazu können sie in Abstimmung mit der jeweiligen Unternehmensleitung alle Unternehmensbereiche zu den notwendigen Datenschutzmaßnahmen veranlassen. Insoweit haben sie ungehindertes Kontrollrecht im Unternehmen.

(4) Die Beauftragten für den Datenschutz machen die bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut.

(5) Daneben können sich alle Betroffenen jederzeit mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit auch an die Beauftragten für den Datenschutz wenden. Anfragen, Ersuchen und Beschwerden werden vertraulich behandelt. Die für die Kontaktaufnahme erforderlichen Daten werden in geeigneter Form bekannt gegeben.

(6) Die für den Datenschutz verantwortlichen Geschäftsführungen der Unternehmen unterstützen die Beauftragten für den Datenschutz bei der Ausübung ihrer Tätigkeit und arbeiten mit ihnen vertrauensvoll zusammen, um die Einhaltung der anwendbaren nationalen und internationalen Datenschutzvorschriften und dieser Verhaltensregeln zu gewährleisten. Die Datenschutzbeauftragten können sich dazu jederzeit mit der jeweils zuständigen datenschutzrechtlichen Aufsichtsbehörde vertrauensvoll beraten.

Art. 28 Beschwerden und Reaktion bei Verstößen

(1) Die Unternehmen werden Beschwerden von Versicherten oder sonstigen Betroffenen wegen Verstößen gegen datenschutzrechtliche Regelungen sowie diese Verhaltensregeln zeitnah bearbeiten und innerhalb einer Frist von 14 Tagen beantworten oder einen Zwischenbescheid geben. Die für die Kontaktaufnahme erforderlichen Daten werden in geeigneter Form bekannt gegeben. Kann der verantwortliche Fachbereich nicht zeitnah Abhilfe schaffen, hat er sich umgehend an den Beauftragten für den Datenschutz zu wenden.

(2) Die Geschäftsführungen der Unternehmen werden bei begründeten Beschwerden so schnell wie möglich Abhilfe schaffen.

(3) Sollte dies einmal nicht der Fall sein, können sich die Beauftragten für den Datenschutz an die zuständige Aufsichtsbehörde für den Datenschutz wenden. Sie teilen dies den Betroffenen unter Benennung der zuständigen Aufsichtsbehörde mit.

Art. 29 Information bei unrechtmäßiger Kenntniserlangung von Daten durch Dritte

(1) Falls personenbezogene Daten unter den Voraussetzungen von Absatz 2 unrechtmäßig übermittelt worden oder Dritten unrechtmäßig zur Kenntnis gelangt sind, informieren die Unternehmen unverzüglich die zuständige Aufsichtsbehörde. Die Betroffenen werden benachrichtigt, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Würde eine Benachrichtigung unverhältnismäßigen Aufwand erfordern, z. B. wegen der Vielzahl der betroffenen Fälle oder wenn eine Feststellung der Betroffenen nicht in vertretbarer Zeit oder mit vertretbarem technischem Aufwand möglich ist, tritt an ihre Stelle eine Information der Öffentlichkeit.

(2) Die Benachrichtigung erfolgt, wenn die personenbezogenen Daten

a) einem Berufsgeheimnis unterliegen, insbesondere Daten eines Unternehmens der Lebens-, Kranken- oder Unfallversicherung, die nach § 203 StGB geschützt sind,

b) besondere Arten personenbezogener Daten, insbesondere Gesundheitsdaten, sind,

c) sich auf strafbare Handlungen, z. B. des Versicherungsbetruges, oder Ordnungswidrigkeiten, z. B. nach Maßgabe des Straßenverkehrsgesetzes, oder einen entsprechenden Verdacht beziehen oder

d) Bank oder Kreditkartenkonten betreffen und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Davon ist in der Regel auszugehen, wenn diesen Vermögensschäden oder nicht unerhebliche soziale Nachteile drohen.

(3) Die Unternehmen verpflichten ihre Auftragsdatenverarbeiter nach § 11 BDSG, sie unverzüglich über Vorfälle nach den Absätzen 1 und 2 bei diesen zu unterrichten.

(4) Die Unternehmen erstellen ein Konzept für den Umgang mit Vorfällen nach den Absätzen 1 und 2. Sie stellen sicher, dass diese der Geschäftsleitung sowie dem betrieblichen Datenschutzbeauftragten zur Kenntnis gelangen.

X. FORMALIA

Art. 30 Beitrittserfordernis und Übergangsvorschriften

(1) Die Unternehmen, die diesen Verhaltensregeln beigetreten sind, verpflichten sich zu deren Einhaltung ab dem Zeitpunkt des Beitritts. Der Beitritt der Unternehmen wird vom GDV dokumentiert und in geeigneter Form bekannt gegeben.

(2) Soweit zur Einhaltung dieser Verhaltensregeln technische Änderungen der Datenverarbeitungsverfahren in den Unternehmen erforderlich sind, legen die Unternehmen der zuständigen Aufsichtsbehörde innerhalb eines Jahres nach Beitritt einen Zeitplan für die Umsetzung vor und melden die Fertigstellung nach Abschluss der technischen Umsetzung bis zum Ende des zweiten Kalenderjahres nach dem Beitrittsjahr.

(3) Versicherungsnehmer, deren Verträge vor dem Beitritt des Unternehmens zu diesen Verhaltensregeln bereits bestanden, werden über das Inkrafttreten dieser Verhaltensregeln über den Internetauftritt des Unternehmens sowie spätestens mit der nächsten Vertragspost in Textform informiert.

Art. 31 Evaluierung

Diese Verhaltensregeln werden bei jeder ihren Regelungsgehalt betreffenden Rechtsänderung in Bezug auf diese, spätestens aber fünf Jahre nach dem Abschluss der Überprüfung gemäß § 38 a Absatz 2 BDSG insgesamt evaluiert.

2. Beschluss der Sitzung am 18./19. September 2012 in Düsseldorf

Near Field Communication (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

III. Dokumente der Europäischen Union: Artikel 29-Datenschutzgruppe

Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten (WP 192)

Angenommen am 22. März 2012

1. Einleitung

In den letzten Jahren hat sich die Gesichtserkennungstechnologie sehr schnell verbreitet und ist genauer geworden. Darüber hinaus wurde diese Technologie für die Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung von natürlichen Personen in Online- und Mobilfunkdienste integriert. Die Technologie, die einst Science Fiction war, steht heute sowohl öffentlichen als auch privaten Stellen zur Nutzung zur Verfügung. Beispiele für ihre Verwendung im Bereich der Online- und Mobilfunkdienste umfassen soziale Netzwerke und Smartphones.

Die Artikel-29-Datenschutzgruppe (WP29) hat sich bereits im Arbeitspapier über Biometrie (WP80) und in der kürzlich veröffentlichten Stellungnahme 03/2012 (WP193) zu den Entwicklungen im Bereich der biometrischen Technologien mit der Fähigkeit, Daten automatisch zu erfassen und ein Gesicht von einem digitalen Bild zu erkennen, befasst. Die Gesichtserkennung wird als der Biometrie zugehörig betrachtet, da sie in vielen Fällen genügend Informationen enthält, um die eindeutige Identifizierung einer Person zu ermöglichen.

In der Stellungnahme 03/2012 wurde Folgendes festgestellt:

„[biometrics] allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high". (Biometrie ermöglicht die automatisierte Verfolgung und Aufspürung von Personen sowie die Profilerstellung und kann sich folglich erheblich auf die Privatsphäre und auf das Recht des Einzelnen auf Datenschutz auswirken).

Diese Aussage trifft insbesondere im Fall der Gesichtserkennung bei Online- und Mobilfunkdiensten zu, wenn Bilder von Einzelpersonen erfasst (mit und ohne Kenntnis der jeweiligen Person) und dann für die Weiterverarbeitung an einen Remote-Server übermittelt werden. Online-Dienste, die sich häufig im Besitz

von privaten Organisationen befinden und von diesen betrieben werden, haben immense Bildersammlungen angelegt, die von den betroffenen Personen selbst hochgeladen wurden. In einigen Fällen wurden diese Bilder möglicherweise auch rechtswidrig durch das automatische Auslesen aus anderen öffentlichen Webseiten wie Suchmaschinencaches erworben. Kleine mobile Geräte mit hochauflösenden Kameras ermöglichen es den Nutzern, Bilder aufzunehmen und in Echtzeit über ständig bestehende Datenverbindungen eine Verbindung zu Online-Diensten herzustellen. Dadurch können die Nutzer diese Bilder mit anderen teilen oder eine Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung durchführen, um zusätzliche Informationen über die bekannte oder unbekannte, vor ihnen stehende Person zu erhalten.

Da die Verwendung dieser Technologie viele verschiedene Datenschutzbedenken hervorruft, erfordert die Gesichtserkennung in Online- und Mobilfunkdiensten die besondere Aufmerksamkeit der WP29.

Der Zweck dieser Stellungnahme ist es, den Rechtsrahmen zu prüfen und angemessene Empfehlungen zu geben, die auf die Technologie zur Gesichtserkennung anzuwenden sind, wenn diese im Zusammenhang mit Online- und Mobilfunkdiensten genutzt wird. Diese Stellungnahme richtet sich an europäische und nationale Rechtsetzungsbehörden, für die Datenverarbeitung Verantwortliche und die Nutzer solcher Technologien. Die Stellungnahme möchte nicht die Grundsätze wiederholen, auf die in Stellungnahme 03/2012 verwiesen wurde, sondern baut auf diese im Bereich der Online- und Mobilfunkdienste auf.

2. Definitionen

Die Technologie der Gesichtserkennung ist nicht neu und für die einschlägigen Begriffe liegen eine Reihe von Definitionen und Auslegungen vor. Deshalb ist es hilfreich, die Technologie, wie sie in dieser Stellungnahme angesprochen ist, klar zu definieren.

Digitales Bild: Ein digitales Bild ist die Darstellung eines zweidimensionalen Bildes in digitaler Form. Die neuesten Entwicklungen in der Technologie zur Gesichtserkennung machen es jedoch erforderlich, dass dreidimensionale Bilder zusätzlich zu den statischen und den bewegten Bildern hinzugefügt werden (d. h. Fotos, aufgezeichnete Videos und Life-Videos).

Gesichtserkennung: Gesichtserkennung ist die automatische Verarbeitung digitaler Bilder, die Gesichter von natürlichen Personen enthalten, um bei diesen eine Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung[1] durchzu-

[1] Identifizierung, Authentifizierung/Verifizierung und Kategorisierung sind in 03/2012 definiert.

führen. Der Prozess der Gesichtserkennung besteht seinerseits aus einer Reihe eigenständiger Teilprozesse:

a) Bilderfassung: Der Prozess der Erfassung des Gesichts einer Person und der Umwandlung in eine digitale Form (das digitale Bild). Im Falle eines Online- oder Mobilfunkdienstes kann das Bild von einem anderen System erworben worden sein, z. B. wenn ein Foto mit einer digitalen Kamera aufgenommen und dann an einen Online-Dienst übermittelt wurde.

b) Gesichtserkennung: Der Prozess, mit dem ein Gesicht auf einem digitalen Bild erkannt und der Bereich markiert wird.

c) Bildnormung: Mit dem Prozess werden Abweichungen innerhalb der entdeckten Gesichtsregionen ausgeglichen. Dazu gehört beispielsweise die Umwandlung in eine Standardgröße, das Drehen oder Angleichen der Farbverteilung.

d) Merkmalsextraktion: Der Vorgang der Isolierung und Bestimmung wiederholbarer und unverwechselbarer Messwerte vom digitalen Bild einer Person. Die Merkmalsextraktion kann holistisch[2], merkmalsbasiert[3] oder eine Kombination aus beiden Methoden[4] sein. Der Satz der Hauptmerkmale kann für einen späteren Vergleich in einem Referenz-Template[5] gespeichert werden.

e) Enrolment: Beim ersten Kontakt einer Person mit dem Gesichtserkennungssystem können Bild und/oder Referenz-Template für einen späteren Vergleich als Datensatz gespeichert werden.

f) Vergleich: Der Prozess des Messens der Ähnlichkeit zwischen einem Satz an Merkmalen (Sample) mit einem bereits im System registrierten Satz. Die Hauptzwecke des Vergleichs sind Identifizierung und Authentifizierung/Verifizierung. Ein dritter Zweck des Vergleichs ist die Kategorisierung. Darunter versteht man den Prozess der Extraktion von Merkmalen aus dem Bild einer Person, um diese Person in einer oder mehreren breiter angelegten Kategorien zu klassifizieren (z. B. Alter, Geschlecht, Farbe der Kleidung usw.). Ein Kategorisierungssystem erfordert nicht unbedingt einen Enrolment-Prozess.

---

2 Holistische Merkmalsextraktion: eine mathematische Darstellung des gesamten Bildes, wie ein sich aus einer Hauptkomponentenanalyse ergebendes Bild.

3 Merkmalsbasierte Merkmalsextraktion: Lokalisierung bestimmter Gesichtsmerkmale wie Augen, Nase und Mund.

4 Auch als hybride Methode der Merkmalsextraktion bekannt.

5 Template ist in 03/2012 definiert als „Hauptmerkmale, die der Rohform der biometrischen Daten entnommen werden (z. B. Gesichtsmaße von einem Bild) und anstelle der Rohdaten selbst für die spätere Verarbeitung gespeichert werden".

3. Beispiele für die Gesichtserkennung bei Online-und Mobilfunkdiensten

Die Gesichtserkennung kann auf verschiedenen Arten und aus einer Vielzahl von Gründen in Online-und Mobilfunkdienste integriert werden. Im Zusammenhang mit dieser Stellungnahme konzentriert sich die WP 29 auf eine Reihe verschiedener Beispiele, die als Hintergrund der Rechtsanalyse dienen und in denen die Gesichtserkennung für die Zwecke der Identifizierung, Authentifizierung/Verifizierung und Kategorisierung verwendet wird.

3.1. Gesichtserkennung als Mittel der Identifizierung

Beispiel 1: Ein sozialer Netzwerkdienst (SNS)[6] erlaubt es den Nutzern, ihrem Profil ein digitales Bild hinzuzufügen. Außerdem können sie Bilder hochladen, um diese mit anderen registrierten oder nicht registrierten Nutzern zu teilen. Registrierte Nutzer können andere Personen (die nicht unbedingt registrierte Nutzer sind) auf den von ihnen hochgeladenen Bildern manuell identifizieren und markieren. Solche Tags (Markierungen) können von der Person gesehen werden, die den Tag angelegt hat und mit einer größeren Gruppe von Freunden oder mit allen registrierten oder nicht registrierten Nutzern geteilt werden. Der SNS kann markierte Bilder nutzen, um einen Referenz-Template für jeden registrierten Nutzer anzufertigen, und durch die Verwendung von Gesichtserkennungssystemen automatisch Tags für neue Bilder vorschlagen, wenn sie hochgeladen werden.

Internet-Suchmaschinen könnten dann Zugriff auf diese Bilder von natürlichen Personen nehmen, die durch die Nutzer öffentlich verfügbar gemacht werden und sie zwischenspeichern. Die Suchmaschine möchte ihre Suchfunktion möglicherweise verbessern, indem sie es Nutzern ermöglicht, das Bild einer Person zu übermitteln und eine Liste von Bildern mit sehr ähnlichen Merkmalen zu erhalten und diese wieder mit der Profilseite des SNS zu verlinken. Das für die Abfrage genutzte Bild kann direkt mit einer Smartphone-Kamera aufgenommen worden sein.

3.2. Gesichtserkennung als Mittel der Authentifizierung/Verifizierung

Beispiel 2: Ein Gesichtserkennungssystem wird genutzt, um einen Nutzernamen/ein Passwort zu ersetzen, mit dem der Zugang zu einem Online- oder Mobilfunkdienst oder -gerät kontrolliert wird. Beim Enrolment wird mit Hilfe einer Kamera an dem Gerät ein Bild des authorisierten Nutzers des Ge-

[6] In der Stellungnahme 05/2009 zu sozialen Online-Netzwerken werden soziale Online-Netzwerke allgemein definiert *„als Kommunikationsplattformen im Online-Bereich, die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw. solche zu schaffen“.*

räts aufgenommen und ein Referenz-Template erstellt, das in dem Gerät oder entfernt durch den Onlinedienst gespeichert werden kann. Um auf den Dienst oder das Gerät zugreifen zu können, wird ein neues Bild der betreffenden Person aufgenommen, das mit dem Referenzbild verglichen wird. Wenn das System einen positiven Abgleich meldet, wird der Zugang gewährt.

3.3. Gesichtserkennung als Mittel der Kategorisierung

Beispiel 3: Der in Beispiel 1 beschriebene SNS kann einem Dritten, der einen Online-Gesichtserkennungsdienst betreibt, den Zugang zu der Bilderdatei gewähren. Der Dienst ermöglicht es den Kunden, Gesichtserkennungstechnologie in andere Produkte zu integrieren. Die Funktion ermöglicht es diesen anderen Produkten, Bilder von Personen hinzufügen, um Gesichter zu ermitteln und in eine Gruppe zu ordnen oder nach vordefinierten Kriterien zu kategorisieren, z. B. wahrscheinliches Alter, Geschlecht und Laune.

Beispiel 4: Der Nutzer einer Spielekonsole verwendet ein Gestensteuerungssystem, bei dem Bewegungen des Nutzers zur Steuerung des Spiels erkannt werden. Die Kamera(s), die für das Gestensteuerungssystem verwendet wird, gibt/geben die Bilder der Personen an ein Gesichtserkennungssystem weiter, das das wahrscheinliche Alter, das Geschlecht und die Stimmung der Spieler zu erkennen versucht. Daten, einschließlich der Daten aus anderen multimodalen Faktoren ändern dann möglicherweise das Spiel, um das Spielerlebnis des Nutzers zu verbessern, oder ändern die Umgebung, um das bevorzugte Profil des Nutzers wiederzugeben. Auf ähnliche Weise könnte das System Nutzer klassifizieren, um den Zugang zu altersbezogenen Inhalten zu erlauben/zu verweigern oder um im Spiel gezielte Werbung zu schalten.

4. Rechtsrahmen

Der einschlägige Rechtsrahmen für die Gesichtserkennung ist die Datenschutzrichtlinie (95/46/EG), die in dieser Hinsicht bereits in der Stellungnahme 03/2012 diskutiert wurde. In diesem Abschnitt soll nur, basierend auf den Beispielen aus Abschnitt 3, eine Zusammenfassung des Rechtsrahmens im Kontext der Gesichtserkennung in Online- und Mobilfunkdiensten gegeben werden. In der Stellungnahme 03/2012 werden weitere Beispiele der Gesichtserkennung betrachtet.

4.1. Digitale Bilder als personenbezogene Daten

Wenn auf einem digitalen Bild ein klar sichtbares Gesicht einer Person abgebildet ist, das es ermöglicht, diese Person zu identifizieren, gehört das Bild in die Gruppe der personenbezogenen Daten. Das hängt von einer Reihe von Parame-

tern ab, wie der Bildqualität und der jeweiligen Perspektive. Bilder von Szenen, die in der Ferne Personen zeigen oder bei denen die Gesichter unscharf sind, werden in den wenigsten Fällen als personenbezogene Daten gelten. Es muss jedoch angemerkt werden, dass digitale Bilder personenbezogene Daten von mehr als einer Person enthalten können (in Beispiel 4 können z. B. mehr Spieler im Blickfeld sein) und das Vorhandensein Anderer auf einem Foto kann auf eine bestehende Beziehung hinweisen.

Die Stellungnahme 04/2007 zum Begriff „personenbezogene Daten" bekräftigt, dass Daten, *„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"* als personenbezogene Daten gelten.

Definitionsgemäß gilt ein Referenz-Template, das von dem Bild einer Person geschaffen wurde, auch als personenbezogene Daten, da es einen Satz unverwechselbarer Merkmale des Gesichts einer Person enthält, der dann mit einer bestimmten Person verlinkt wird und als Referenz für spätere Vergleiche zur Identifizierung und Authentifizierung/Verifizierung gespeichert wird.

Ein Template oder ein Satz unverwechselbarer Merkmale, die nur in einem Kategorisierungssystem verwendet werden, enthalten im Allgemeinen nicht ausreichend Informationen, um eine Person zu identifizieren. Es sollten nur genügend Informationen darauf enthalten sein, um die Kategorisierung vornehmen zu können (z. B. männlich oder weiblich). In dem Fall würde es sich nicht um personenbezogene Daten handeln, vorausgesetzt, dass das Template (oder das Ergebnis) nicht mit der Akte einer Person, mit ihrem Profil oder mit dem Originalbild (das weiterhin als personenbezogene Daten gilt) in Verbindung gebracht wird.

Da sich digitale Bilder von Personen auf „*biologische Eigenschaften, auf Verhaltensaspekte, physiologische Merkmale, Gesichtszüge oder reproduzierbare Handlungen [beziehen], wobei diese Merkmale und/oder Handlungen für die betreffende Person spezifisch und messbar sind*[7]*"*, sollten sie als biometrische Daten gelten.

4.2. Digitale Bilder als besondere Kategorie personenbezogener Daten

Digitale Bilder von Personen können in bestimmten Fällen als besondere Kategorie personenbezogener Daten[8] angesehen werden. Insbesondere, wenn digitale Bilder von Personen oder Templates weiterverarbeitet werden, um bestimmte Kategorien von Daten zu erhalten, gehören sie ganz bestimmt zu dieser Kategorie.

[7] Definition von Biometrie aus Stellungnahme 03/2012

[8] In bestimmten Ländern hat die Rechtsprechung digitale Bilder von Gesichtern als besondere Kategorie von Daten eingestuft – LJN BK6331 Oberster Gerichtshof der Niederlande vom 23. März 2010

Ein Beispiel hierfür ist, wenn die Daten dazu genutzt werden, Informationen über die ethnische Herkunft, die Religion oder die Gesundheit zu erhalten.

4.3. Verarbeitung personenbezogener Daten im Zusammenhang mit einem Gesichtserkennungssystem

Wie bereits beschrieben, basiert die Gesichtserkennung auf einer Reihe automatisierter Verarbeitungsschritte. Deshalb stellt die Gesichtserkennung eine automatisierte Form der Verarbeitung personenbezogener Daten, einschließlich biometrischer Daten, dar.

Durch die Verwendung biometrischer Daten können Gesichtserkennungssysteme in einzelnen Mitgliedstaaten zusätzlichen Kontrollen oder anderen Rechtsvorschriften wie einer vorherigen Genehmigung oder dem Arbeitsrecht unterliegen. Auf die Verwendung von Biometrie im Beschäftigungskontext wird in Stellungnahme 03/2012 näher eingegangen.

4.4. Für die Datenverarbeitung Verantwortlicher

Die vorstehenden Beispiele zeigen, dass die für die Datenverarbeitung Verantwortlichen üblicherweise Eigentümer der Website und/oder Online-Service-Provider sowie Betreiber mobiler Applikationen, die Gesichtserkennungsdienste anbieten, sind, da sie den Zweck und/oder die Mittel der Verarbeitung[9] festlegen. Das entspricht auch der Schlussfolgerung aus Stellungsnahme 05/2009 ein, die lautet: „Die Anbieter sozialer Netzwerkdienste sind die ‚für die Verarbeitung von Benutzerdaten Verantwortlichen' im Sinne der Datenschutzrichtlinie."

4.5. Berechtigter Grund

Richtlinie 95/46/EG legt die Bedingungen fest, die bei der Verarbeitung personenbezogener Daten eingehalten werden müssen. Das heißt, dass die Verarbeitung zuerst die Anforderungen hinsichtlich der Datenqualität (Artikel 6) erfüllen muss. In diesem Fall muss die Verarbeitung der digitalen Bilder der Personen und der entsprechenden Templates für die Zwecke der Verarbeitung zur Gesichtserkennung „relevant" sein und darf „nicht darüber hinausgehen". Außerdem darf nur dann eine Verarbeitung stattfinden, wenn eine der in Artikel 7 niedergelegten Voraussetzungen erfüllt ist.

Aufgrund der besonderen Risiken, die mit biometrischen Daten einhergehen, muss folglich vor dem Beginn der Verarbeitung von digitalen Bildern für die Gesichtserkennung die in Kenntnis der Sachlage erteilte Einwilligung der betroffe-

[9] Siehe Stellungnahme 01/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter".

nen Person eingeholt werden. In einigen Fällen kann es jedoch erforderlich sein, dass der für die Datenverarbeitung Verantwortliche vorübergehend einige Verarbeitungsschritte zur Gesichtserkennung durchführen muss, um zu bewerten, ob der Nutzer seine Einwilligung in die Verarbeitung erteilt hat oder nicht und ob somit eine Rechtsgrundlage vorhanden ist. In dem Fall kann diese anfängliche Verarbeitung (d. h. Bilderfassung, Gesichtserkennung, Vergleich usw.) eine andere Rechtsgrundlage haben und zwar insbesondere das rechtmäßige Interesse des für die Datenverarbeitung Verantwortlichen an der Einhaltung der Datenschutzbestimmungen. Daten, die während dieser Schritte verarbeitet werden, sollten ausschließlich für die Feststellung genutzt werden, ob der Nutzer seine Einwilligung erteilt hat, und sollten folglich sofort danach gelöscht werden.

Im ersten Beispiel hat der für die Datenverarbeitung Verantwortliche festgestellt, dass an allen hochgeladenen, neuen Bildern von registrierten Nutzern des SNS die Schritte der Gesichtserkennung, der Merkmalsextraktion und des Vergleichs durchgeführt werden sollen. Nur bei registrierten Nutzern, von denen sich ein Referenz-Template in der Datenbank befindet, wird eine Entsprechung mit diesen neuen Bildern festgestellt und folglich automatisch eine Markierung vorgeschlagen. Wenn die Einwilligung der Einzelperson als einziger berechtigter Grund für die gesamte Verarbeitung anzusehen ist, muss der vollständige Dienst blockiert werden, da beispielsweise keine Möglichkeit besteht, die Einwilligung von nicht registrierten Nutzern einzuholen, deren personenbezogene Daten möglicherweise während der Gesichtserkennung und Merkmalsextraktion verarbeitet werden. Außerdem wäre es nicht möglich, die Gesichter der registrierten Nutzer, die ihre Einwilligung erteilt haben, von denen zu unterscheiden, die keine Einwilligung erteilt haben, ohne zuerst eine Gesichtserkennung durchzuführen. Erst nachdem eine Identifizierung stattgefunden hat (oder diese nicht möglich war), könnte ein für die Datenverarbeitung Verantwortlicher feststellen, ob ihm die erforderliche Einwilligung in die jeweilige Verarbeitung erteilt wurde.

Bevor ein registrierter Nutzer ein Bild auf einen SNS hochlädt, muss er in klarer Weise darüber informiert werden, dass diese Bilder durch ein Gesichtserkennungssystem laufen. Noch wichtiger ist, dass die registrierten Nutzer darüber hinaus entscheiden können, ob sie der Aufnahme ihres Referenz-Templates in die Identifizierungs-Datenbank zustimmen. Bei nicht registrierten Nutzern und bei registrierten Nutzern, die ihre Einwilligung nicht erteilt haben, wird folglich ihr Name nicht automatisch für eine Markierung vorgeschlagen, da Bilder, auf denen sie abgebildet sind, das Ergebnis „keine Übereinstimmung“ ergeben.

Die Einwilligung der Person, die das Bild hochlädt, darf nicht verwechselt werden mit der Anforderung eines berechtigten Grunds für die Verarbeitung der personenbezogenen Daten anderer Personen, die möglicherweise auch auf dem Bild sind. Aus diesem Grund möchte der für die Datenverarbeitung Verantwortliche möglicherweise auf einen anderen berechtigten Grund für die Verarbeitung in den

Zwischenschritten (Gesichtserkennung, Bildnormierung und Vergleich) zurückgreifen, wie beispielsweise, dass die Verarbeitung im berechtigten Interesse des für die Datenverarbeitung Verantwortlichen liegt, sofern genügend Einschränkungen und Kontrollen vorhanden sind, die die Grundrechte und -freiheiten der betroffenen Personen schützen, die nicht das Bild selbst hochgeladen haben. Zu diesen Kontrollen würde unter anderem die Sicherstellung gehören, dass keine Daten aus derVerarbeitung aufbewahrt werden, wenn als Ergebnis „keine Übereinstimmung" erhalten wurde (d. h. alle Templates und damit verbundenen Daten werden auf sichere Weise gelöscht). Der für die Datenverarbeitung Verantwortliche könnte auch die Bereitstellung von Werkzeugen in Erwägung ziehen, die es der das Bild hochladenden Person ermöglichen, die Gesichter derjenigen Personen unkenntlich zu machen, für die es in der Referenzdatenbank kein übereinstimmendes Template gibt. Das Enrolment des Templates einer Person in eine Identifizierungsdatenbank (und damit die Möglichkeit, eine Übereinstimmung festzustellen und Markierungsvorschläge zu unterbreiten) wäre nur mit der in Kenntnis der Sachlage erteilten Einwilligung der betroffenen Person möglich.

Im zweiten Beispiel gibt es während des Enrolment-Prozesses eindeutig die Möglichkeit, die Einwilligung der Person einzuholen, die während des Enrolment-Prozesses zum Zugang zum Gerät befugt ist. Damit die Einwilligung gültig ist, muss ein alternatives und gleichermaßen sicheres Zugangskontrollsystem vorhanden sein (wie ein sicheres Passwort). Diese alternative, privatsphärenschutzfreundliche Option sollte der Standard sein. Wenn ein einzelner Nutzer sich unter eine mit dem Gerät verbundene Kamera stellt und damit der ausdrückliche Zweck verbunden ist, Zugang zu erhalten, kann davon ausgegangen werden, dass diese Person ihre Einwilligung in die daraus resultierende Gesichtserkennung erteilt hat, die für die Authentifizierung erforderlich ist, selbst wenn es sich bei dieser Person nicht um einen befugten Nutzer des Geräts handelt. Der Umfang der erteilten Informationen muss ausreichend sein, um sicherzustellen, dass die Einwilligung gültig ist.

Die im dritten Beispiel beschriebene weitere Verbesserung der SNS-Fotobibliothek wäre eine eindeutige Verletzung der Zweckbindung. Deshalb muss vor der Einführung einer solchen Funktion die gültige Einwilligung der Person eingeholt werden und eindeutig angegeben werden, dass eine solche Bilderverarbeitung stattfindet. Das gilt auch für die in Beispiel 1 beschriebene Suchmaschine. Die von der Suchmaschine bezogenen Bilder wurden nicht für die Erfassung durch Gesichtserkennungssysteme eingestellt, sondern mit der Absicht, dass sie gesehen werden. Der Suchmaschinenbetreiber müsste die Einwilligung der betroffenen Personen für die Registrierung in dem zweiten Gesichtserkennungssystem einholen.

Das wäre auch in dem vierten Beispiel der Fall, da der Nutzer nicht davon ausgehen kann, dass Bilder, die für die Gestensteuerung bestimmt waren, weiter verar-

beitet werden. Wenn der für die Datenverarbeitung Verantwortliche die Einwilligung für eine längerfristige Verarbeitung (d. h. zeitlich oder für mehrere Spiele) einholen will, muss er die Nutzer in regelmäßigen Abständen daran erinnern, dass das System in Betrieb ist und standardmäßig ausgeschaltet wird.

Stellungnahme 15/2011 zur Definition von Einwilligung betrachtet die Qualität, die Zugänglichkeit und die Sichtbarkeit von Informationen zur Verarbeitung von personenbezogenen Daten. Die Stellungnahme stellt fest:

„Informationen müssen den Personen direkt gegeben werden. Es reicht nicht aus, dass die Informationen irgendwo ‚verfügbar' sind."

Informationen zur Funktion der Gesichtserkennung in Online- oder Mobilfunkdiensten dürfen also nicht irgendwo versteckt sein, sondern müssen auf eine leicht zugängliche und verständliche Weise verfügbar sein. Dazu gehört auch, dass die Kameras selbst nicht verborgen sind. Die für die Datenverarbeitung Verantwortlichen sollten die berechtigten Erwartungen der Öffentlichkeit in Bezug auf die Privatsphäre berücksichtigen, wenn sie eine Gesichtserkennungstechnologie einsetzen. Sie sollten auf diese Bedenken in angemessener Weise eingehen.

In diesem Zusammenhang kann die Einwilligung in das Enrolment nicht davon abgeleitet werden, dass der Nutzer die allgemeinen Geschäftsbedingungen der zugrunde liegenden Dienste generell angenommen hat, es sein denn, dass bei dem vorrangigen Ziel des Dienstes die Verwendung von Gesichtserkennung zu erwarten ist. Das liegt daran, dass Enrolment in den meisten Fällen eine zusätzliche Funktion ist und nicht in direktem Zusammenhang mit dem Betreiben des Online- oder Mobilfunkdienstes steht. Die Nutzer müssen nicht unbedingt davon ausgehen, dass eine solche Funktion aktiviert ist, wenn sie den Dienst nutzen. Daher sollten Nutzer abhängig vom Zeitpunkt der Einführung der Funktion entweder während der Registrierung oder zu einem späteren Zeitpunkt ausdrücklich die Möglichkeit haben, ihre Einwilligung in diese Funktion zu erteilen.

Damit die Einwilligung gültig ist, müssen angemessene Informationen über die Datenverarbeitung gegeben worden sein. Nutzer sollten immer die Möglichkeit haben, ihre Einwilligung auf einfache Weise zurückzuziehen. Sobald die Einwilligung in die Verarbeitung für Zwecke der Gesichtserkennung zurückgezogen wurde, ist diese unverzüglich zu beenden.

5. Spezifische Risiken und Empfehlungen

Das Risiko eines Gesichtserkennungssystems für die Privatsphäre hängt vollständig von der Art der verwendeten Verarbeitung und dem/den Zweck(en) ihrer Verwendung ab. Es gibt jedoch bestimmte Risiken, die während bestimmter Phasen

der Gesichtserkennung eine größere Bedeutung haben. Der folgende Abschnitt beleuchtet die hauptsächlichen Risiken und gibt Empfehlungen für bewährte Verfahren.

5.1. Rechtswidrige Verarbeitung zu Zwecken der Gesichtserkennung

Im Online-Bereich können die für die Datenverarbeitung Verantwortlichen auf viele Arten Bilder erhalten, beispielsweise, indem sie von den Nutzern der Online-oder Mobilfunkdienste, von deren Freunden oder Kollegen oder von Dritten bereitgestellt werden. Auf den Bildern können die Gesichter der Nutzer selbst abgebildet sein und/oder die Gesichter von anderen registrierten oder nicht registrierten Nutzern oder sie können ohne die Kenntnis der betroffenen Person beschafft worden sein. Unabhängig davon, auf welche Weise diese Bilder beschafft wurden, muss für ihre Verarbeitung eine Rechtsgrundlage vorliegen.

Empfehlung 1: Wenn der für die Datenverarbeitung Verantwortliche das Bild direkt erhält (wie z. B. in den Beispielen 2 und 4), muss er sicherstellen, dass die gültige Einwilligung der betroffenen Personen bereits vor der Erfassung vorliegt, und ausreichende Informationen bereitstellen, wenn eine Kamera für die Zwecke der Gesichtserkennung genutzt wird.

Empfehlung 2: Wenn Einzelpersonen digitale Bilder haben und diese bei Online- oder Mobilfunkdiensten für Zwecke der Gesichtserkennung hochladen, müssen die für die Datenverarbeitung Verantwortlichen sicherstellen, dass die die Bilder hochladenden Personen in die Verarbeitung der Bilder eingewilligt haben, die möglicherweise für Zwecke der Gesichtserkennung durchgeführt wird.

Empfehlung 3: Wenn für die Datenverarbeitung Verantwortliche digitale Bilder von Personen von Dritten erhalten (z. B. wenn sie diese von einer Website kopieren oder von einem anderen für die Datenverarbeitung Verantwortlichen kaufen), müssen sie die Quelle der Bilder und den Kontext, in dem die Originalbilder erworben und verarbeitet werden, sorgfältig prüfen und auch, ob die betroffenen Personen einer solchen Verarbeitung zugestimmt hatten.

Empfehlung 4: Die für die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass digitale Bilder und Templates nur für den angegebenen Zweck genutzt werden, für den sie zur Verfügung gestellt wurden. Die für die Datenverarbeitung Verantwortlichen sollten technische Kontrollen einführen, um das Risiko zu reduzieren, dass digitale Bilder durch Dritte für Zwecke weiterverarbeitet werden, für die der Nutzer keine Einwilligung erteilt hat. Sie sollten für die Nutzer auch Werkzeuge bereitstellen, mit denen diese die Sichtbarkeit der von ihnen hochgeladenen Bilder überprüfen können, wenn die Verfügbarkeit für Dritte standardmäßig eingeschränkt ist.

Empfehlung 5: Die für die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass die Bilder von Personen, die keine registrierten Nutzer des Dienstes sind und die in eine solche Verarbeitung nicht auf eine andere Weise eingewilligt haben, nur soweit verarbeitet werden, wie es im begründeten Interesse des für die Datenverarbeitung Verantwortlichen liegt. Beim ersten Beispiel würde das das Einstellen der Verarbeitung und Löschen aller Daten im Falle des Ergebnisses „keine Übereinstimmung" bedeuten.

Sicherheitsverletzung während der Übermittlung
Im Fall von Online- und Mobilfunkdiensten ist es wahrscheinlich, dass zwischen dem Erwerb des Bildes und den weiteren Verarbeitungsschritten (z. B. dem Hochladen des Bildes von einer Kamera auf eine Website für die Merkmalsextraktion und den Vergleich) eine Datenübermittlung stattfindet.

Empfehlung 6: Der für die Datenverarbeitung Verantwortliche muss geeignete Schritte unternehmen, um die Sicherheit der Datenübermittlung sicherzustellen. Dazu können eine Verschlüsselung der Kommunikationskanäle oder des erworbenen Bildes selbst zählen. Sofern möglich, und insbesondere im Bereich der Authentifizierung/Verifizierung, sollte die Verarbeitung vor Ort vorgezogen werden.

5.2. Gesichtserkennung, Bildnormierung, Merkmalsextraktion

Datenminimierung
Von Systemen zur Gesichtserkennung erstellte Templates enthalten möglicherweise mehr Daten, als für den/die angegebenen Zweck(e) benötigt werden.

Empfehlung 7: Die für die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass die aus einem digitalen Bild für die Erstellung eines Templates extrahierten Daten nur die Informationen enthalten, die für den angegebenen Zweck erforderlich sind, und so eine weitere Verarbeitung verhüten. Templates sollten nicht zwischen Gesichtserkennungssystemen übertragbar sein.

Sicherheitsverletzungen während der Datenaufbewahrung
Die Identifizierung und Authentifizierung/Verifizierung erfordern wahrscheinlich die Speicherung des Templates für die Verwendung bei einem späteren Vergleich.

Empfehlung 8: Der für die Datenverarbeitung Verantwortliche muss überlegen, wo die Daten am besten gespeichert werden. Das kann auch im Gerät des Nutzers oder im System des für die Datenverarbeitung Verantwortlichen geschehen. Der für die Datenverarbeitung Verantwortliche muss geeignete Schritte unternehmen, um die Sicherheit der gespeicherten Daten sicherzustellen. Dazu kann die Verschlüsselung des Templates gehören. Ein unbefugter Zugang zu dem Template oder dem Speicherort sollte nicht möglich sein. Insbesondere im Fall der Ge-

sichtserkennung für Zwecke der Verifizierung können biometrische Verschlüsselungstechniken verwendet werden. Bei diesen Techniken ist der kryptographische Schlüssel direkt an die biometrischen Daten geknüpft und wird nur dann erneut erstellt, wenn das richtige, biometrische Daten einer Person zur Verifizierung vorgelegt wird. Es wird kein Bild oder Template gespeichert (folglich eine Art „nicht verfolgbarer Biometrie“).

Zugang durch die betroffene Person

Empfehlung 9: Der für die Datenverarbeitung Verantwortliche sollte den betroffenen Personen geeignete Mechanismen zur Verfügung stellen, damit sie gegebenenfalls ihr Zugangsrecht sowohl auf die Originalbilder als auch auf die im Zusammenhang mit der Gesichtserkennung generierten Templates ausüben können.

Brüssel, den 22. März 2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien (WP 193)

Angenommen am 27. April 2012

Zusammenfassung

Biometrische Systeme nutzen bestimmte individuelle Merkmale einer Person zur Identifikation und/oder Authentifikation dieser Person und stellen insoweit enge Verknüpfungen mit den betroffenen Personen her. Die Daten einer Person können gelöscht oder geändert werden. Manipulationen oder Änderungen der Datenquelle hingegen sind nicht möglich.

Biometrische Daten werden erfolgreich und wirksam in der Forschung genutzt; sie sind ein wesentliches Element der Forensik und spielen eine wichtige Rolle bei Systemen zur Zugangskontrolle. Sie können helfen, das Sicherheitsniveau zu erhöhen, und sie können dazu beitragen, Identifikations- und Authentifikationsverfahren zu vereinfachen, zu beschleunigen und bequemer zu gestalten. Früher war diese Technologie teuer und hatte entsprechend nur eingeschränkte Auswirkungen auf die Datenschutzrechte natürlicher Personen. Dies hat sich in den letzten Jahren drastisch geändert. DNA-Analysen beanspruchen heute weniger Zeit und sind für nahezu jedermann erschwinglich. Der technische Fortschritt hat dazu geführt, dass Datenspeicher und Rechenkapazitäten billiger wurden. Infolge dieser Entwicklung sind Online-Fotoalben und soziale Netzwerke entstanden, in denen Milliarden von Fotos verwaltet werden. Fingerabdruck-Lesegeräte und Systeme zur Videoüberwachung sind bezahlbare technische Hilfsmittel geworden. Die Entwicklung dieser Technologien hat dazu beigetragen, dass viele Verfahren vereinfacht wurden, zahlreiche Verbrechen aufgeklärt werden konnten und Zugangskontrollsysteme zuverlässiger geworden sind. Diese Entwicklung hat allerdings auch neue Bedrohungen der Grundrechte mit sich gebracht. Die genetische Diskriminierung hat sich zu einem echten Problem entwickelt, und der Diebstahl von Identitäten ist nicht mehr nur eine theoretische Gefahr.

Bei anderen neuen Technologien, die auf große Bevölkerungsgruppen abzielen, und die in jüngster Zeit Anlass zu datenschutzrechtlichen Bedenken gegeben haben, steht die Verknüpfung mit bestimmten Personen nicht unbedingt im Vordergrund bzw. ist diese Verknüpfung mit beträchtlichem Aufwand verbunden. Biometrische Daten hingegen sind direkt mit einer einzigen Person verknüpft. Dies ist nicht immer vorteilhaft, sondern birgt auch erhebliche Nachteile. Die Ausrüstung von Videoüberwachungssystemen und Smartphones mit Funktionen zur Gesichtserkennung, die auf der Nutzung der Datenbanken sozialer Netzwerke beruhen, könnte jegliche Anonymität zunichtemachen und zur Folge haben, dass Einzelpersonen auf Schritt und Tritt überwacht werden. Allerdings könnten Fin-

gerabdruck-Lesegeräte, Geräte zur Erkennung von Venenstrukturen („Venenscanner“) oder auch einfach ein Lächeln in eine Kamera Chipkarten, Codes, Kennwörter und Unterschriften ersetzen.

Diese Zusammenhänge sowie weitere neue Entwicklungen sind Gegenstand dieser Stellungnahme. Ziel dieser Stellungnahme ist es, sowohl die betreffenden Personen als auch die gesetzgebenden Institutionen zu sensibilisieren. Die technischen Innovationen, die allzu häufig nur in ihrer Eigenschaft als Technologien dargestellt werden, die das Erscheinungsbild und die Bedienungsfreundlichkeit von Anwendungen verbessern, könnten auch zu einem schrittweisen Verlust der Privatsphäre führen, wenn keine angemessenen Garantien vorgesehen werden. Daher werden in dieser Stellungnahme technische und organisatorische Maßnahmen erläutert, die die Gefahren im Hinblick auf den Datenschutz und die Verletzung der Privatsphäre verringern und dazu beitragen könnten, Beeinträchtigungen der Privatsphäre und des Grundrechts der Bürger Europas auf den Schutz ihrer personenbezogenen Daten zu verhindern.

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

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

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Umfang der Stellungnahme

Im Jahr 2003 hat die Artikel-29-Datenschutzgruppe (Datenschutzgruppe) für Biometrie (WP 80) Fragen des Datenschutzes im Zusammenhang mit der Nutzung aufkommender Technologien zum elektronischen Lesen und Verarbeiten biometrischer Daten untersucht. In den letzten Jahren haben sich diese Technologien sowohl im öffentlichen als auch im privaten Bereich weithin etabliert. Gleichzeitig entwickelte sich eine Reihe neuer Dienstleistungsangebote. Biometrische Technologien, die früher mit einem erheblichen finanziellen Aufwand einhergingen und beträchtliche Rechenkapazität beanspruchten, sind drastisch billiger geworden, und die erforderlichen Rechenprozesse können erheblich schneller durchgeführt werden. Der Einsatz von Fingerabdruck-Lesegeräten ist inzwischen allgemein üblich. Bei manchen Laptops beispielsweise erfolgt eine biometrische

Zugangskontrolle mit einem Fingerabdruck-Lesegerät. Dank der erzielten Fortschritte liegen die Ergebnisse von DNA-Analysen nun binnen weniger Minuten vor. Einige der neu entwickelten Technologien (beispielsweise die Erkennung von Venenstrukturen oder die Gesichtserkennung) wurden bereits bis zur Marktreife entwickelt. Diese Technologien gehören in unserem Leben in unterschiedlichen Bereichen bereits zum Alltag. Biometrische Technologien sind eng mit gewissen personenbezogenen Merkmalen verbunden. Teilweise können diese Merkmale genutzt werden, um empfindliche Daten in Erfahrung zu bringen. Außerdem ermöglichen biometrische Daten häufig die automatisierte Verfolgung und Aufspürung von Personen sowie die Erstellung von Profilen. Insoweit können sich diese Entwicklungen erheblich auf die Privatsphäre und auf das individuelle Recht auf Datenschutz auswirken. Mit zunehmender Verbreitung dieser Technologien verschärfen diese Auswirkungen sich noch. Früher oder später wird jede einzelne Person in einem oder mehreren biometrischen Systemen erfasst.

In dieser Stellungnahme soll ein überarbeiteter und aktualisierter Rahmen für einheitliche allgemeine Leitlinien und Empfehlungen zur Berücksichtigung von Grundsätzen des Schutzes der Privatsphäre und des Datenschutzes im Zusammenhang mit biometrischen Anwendungen beschrieben werden. Die Stellungnahme richtet sich an gesetzgebende Institutionen auf europäischer und auf nationaler Ebene sowie an die Biometrieindustrie und an die Nutzer der entsprechenden Technologien.

2. Begriffsbestimmungen

Biometrische Technologien sind nicht neu und wurden bereits in mehreren Stellungnahmen der Datenschutzgruppe behandelt. In diesem Abschnitt wurden wichtige Begriffsbestimmungen zusammengestellt und gegebenenfalls aktualisiert.

Biometrische Daten: Wie von der Datenschutzgruppe bereits in der Stellungnahme 4/2007 (WP 136) erläutert, können „biometrische Daten“

> *„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.“*

Biometrische Daten wirken sich insoweit unwiderruflich auf die Verbindung zwischen Körper und Identität aus, als sie die Merkmale des menschlichen Körpers „maschinenlesbar“ machen und damit vielfältige Nutzungsmöglichkeiten erschließen.

Biometrische Daten können in unterschiedlicher Form gespeichert und verarbeitet werden. Manchmal werden die von einer Person erfassten biometrischen Informationen in einem Rohformat gespeichert und verarbeitet, aus dem sich die Herkunft der Daten auch ohne besondere Kenntnisse ermitteln lässt (z. B. bei Porträtfotos, bei gescannten Fingerabdrücken oder bei Stimmenaufzeichnungen). In anderen Fällen werden die erfassten biometrischen Rohdaten so verarbeitet, dass nur bestimmte Merkmale und/oder Elemente extrahiert und als sogenanntes biometrisches Template gespeichert werden können.

Herkunft biometrischer Daten: Biometrische Daten können aus unterschiedlichen Quellen stammen und physische, physiologische, verhaltensbezogene und psychische Merkmale einer Person umfassen. In der Stellungnahme 4/2007 (WP 136) wurde festgestellt:

> Die Quellen biometrischer Daten (z. B. Proben von menschlichem Gewebe) sind *„selbst […] keine biometrischen Daten …“* Sie können jedoch zur Erfassung biometrischer Daten genutzt werden (indem Informationen aus diesen Quellen extrahiert werden).

Wie bereits in WP 80 erläutert, sind biometrische Verfahren zwei Hauptkategorien zuordnen:

– Die erste Gruppe umfasst die Verfahren, die die physischen und physiologischen Merkmale einer Person erfassen (Verifikation von Fingerabdrücken, Finger-Bildanalyse, Iris-Erkennung, Netzhautanalyse, Gesichtserkennung, Erkennung der Handgeometrie oder der Ohrenform, Erfassung des Körpergeruchs, Sprecherverifikation, Analyse von DNA-Mustern, Analyse der Schweißporen usw.).

– Die zweite Gruppe beinhaltet die Verfahren, die die Verhaltensmerkmale einer Person erfassen. Dazu zählen u. a. die Verifikation von Unterschriften und die Analyse von Tastenanschlägen, Gangarten und Bewegungsmustern sowie die Auswertung von Verhaltensweisen, die Rückschlüsse auf unterbewusstes Denken (etwa beim Lügen) zulassen.

Außerdem sollte der sich entwickelnde Bereich der psychologischen Verfahren nicht außer Acht gelassen werden. Beispielsweise werden aufgrund des Verhaltens in konkreten Situationen oder anhand spezifischer Tests psychologische Profile erstellt.

Biometrische Templates: Aus biometrischen Rohdaten (z. B. Gesichtsmessungen an einem Bild) können Schlüsselmerkmale extrahiert werden, um später nicht die eigentlichen Rohdaten, sondern die daraus extrahierten Merkmale zu verarbeiten. So entsteht ein biometrisches Template der betreffenden Daten. Von

entscheidender Bedeutung ist die Definition des Umfangs eines Template (d. h. die Festlegung der Menge der in einem Template enthaltenen Informationen). Einerseits sollte das Template umfangreich genug sein, um die Sicherheitsanforderungen zu erfüllen (wobei Überschneidungen zwischen unterschiedlichen biometrischen Daten ebenso zu vermeiden sind wie die Substitution von Identitäten). Andererseits darf das Template nicht so umfangreich sein, dass sich die biometrischen Daten später vielleicht nicht mehr rekonstruieren lassen. Die Erstellung des Template sollte nur in eine Richtung möglich sein, d. h., es sollte ausgeschlossen sein, dass ausgehend von einem Template die biometrischen Rohdaten wiederhergestellt werden.

Biometrische Systeme: In WP 80 werden biometrische Systeme wie folgt definiert:

> *„Biometrische Systeme sind Anwendungen der Biometrie, die eine automatische Identifikation und/oder Authentifikation/Verifikation von Personen ermöglichen. Authentifikations-/Verifikationsanwendungen werden häufig für verschiedene Aufgaben in völlig unterschiedlichen Bereichen und unter der Verantwortung der unterschiedlichsten Stellen eingesetzt."*

Mit den neuesten technologischen Entwicklungen können biometrische Systeme nun auch zur Kategorisierung/Aufschlüsselung von Daten verwendet werden.

Die mit biometrischen Systemen verbundenen Risiken liegen in der Natur der zu verarbeitenden biometrischen Daten. Eine allgemeinere Definition wäre daher ein System, das biometrische Daten extrahiert und weiterverarbeitet.

Die Verarbeitung biometrischer Daten in einem biometrischen System beinhaltet gewöhnlich mehrere Prozesse (Erfassung, Speicherung, Abgleich usw.):

– ***Biometrische Erfassung:*** Die biometrische Erfassung beinhaltet sämtliche Prozesse in einem biometrischen System, die zur Extrahierung biometrischer Daten aus einer biometrischen Quelle und zur Verknüpfung dieser Daten mit einer bestimmten Person benötigt werden. Umfang und Qualität der zu erfassenden Daten sollten hinreichend sein, um eine zuverlässige Identifikation, Authentifikation, Kategorisierung und Verifikation zu ermöglichen, ohne jedoch Daten in übermäßigem Umfang zu erfassen. Der Umfang der während der Erfassung aus einer biometrischen Quelle extrahierten Daten muss dem Zweck der jeweiligen Verarbeitung und der Leistungsfähigkeit des betreffenden biometrischen Systems angemessen sein.

  Bei der Erfassung kommt eine Person gewöhnlich zum ersten Mal mit einem bestimmten biometrischen System in Kontakt. Meist erfordert die Erfassung die Mitwirkung der betreffenden Person (z. B. bei der Abnahme von Finger-

abdrücken). Entsprechend bietet dieser Schritt die Gelegenheit zur Aufklärung und zu einer fairen Unterrichtung über die vorgesehene Verarbeitung. Allerdings können Personen auch ohne ihr Wissen und ohne ihre Einwilligung erfasst werden (z. B. mit Überwachungskameras mit integrierter Gesichtserkennung). Die Zuverlässigkeit und die Sicherheit des Erfassungsprozesses sind entscheidend für die Leistungsfähigkeit des gesamten Systems. Einer Person kann die Möglichkeit eingeräumt werden, die in einem biometrischen System erfassten biometrischen Daten zu aktualisieren.

– ***Biometrische Speicherung:*** Die während der Erfassung erhaltenen Daten können zur späteren Verwendung dort gespeichert werden, wo die Erfassung erfolgt ist (z. B. in einem Lesegerät). Ebenso kommt jedoch die Speicherung in einer zentralen Datenbank in Betracht, auf die eines oder mehrere biometrische Systeme zugreifen können.

– ***Biometrischer Abgleich:*** Beim biometrischen Abgleich werden die erfassten biometrischen Daten/Templates mit den biometrischen Daten/Templates einer neuen Stichprobe verglichen, um Daten identifizieren, verifizieren/authentifizieren oder kategorisieren zu können.

Biometrische Identifikation: Die Identifikation einer Person durch ein biometrisches System erfolgt gewöhnlich durch den Abgleich biometrischer Daten einer Person (die während der Identifikation erfasst wurden) mit einer Reihe biometrischer Templates in einer Datenbank (One-to-many-Verfahren).

Biometrische Verifikation/Authentifikation: Die Verifikation einer Person durch ein biometrisches System erfolgt gewöhnlich durch den Abgleich der (während der Verifikation erfassten) biometrischen Daten einer Person mit einer Reihe biometrischer Templates in einer Datenbank (One-to-many-Verfahren).

Biometrische Kategorisierung/Aufschlüsselung: Die Kategorisierung/Aufschlüsselung der Merkmale einer Person durch ein biometrisches System erfolgt gewöhnlich, indem festgestellt wird, ob die biometrischen Daten einer Person einer Gruppe mit vordefinierten Merkmalen zuzuordnen sind, um dann bestimmte Maßnahmen einzuleiten. In diesem Fall kommt es nicht darauf an, die betreffende Person zu identifizieren oder zu verifizieren, sondern die Person automatisch einer bestimmten Kategorie zuzuweisen. Anschließend könnten beispielsweise auf einer Werbetafel je nach Alter oder Geschlecht des Betrachters unterschiedliche Werbungen angezeigt werden.

Multimodale Biometrie: Multimodale Biometrie kann als Kombination verschiedener biometrischer Technologien definiert werden, durch die die Zuverlässigkeit oder die Leistungsfähigkeit eines Systems gesteigert werden soll. Multimodale biometrische Verfahren werden auch als „mehrstufige biometrische Ver-

fahren“ bezeichnet. Die entsprechenden Systeme nutzen beim Abgleich mindestens zwei biometrische Merkmale/Verfahren zur Identifikation einer bestimmten Person. Diese Systeme können auf unterschiedliche Weise funktionieren. Sie können unterschiedliche biometrische Daten mit unterschiedlichen Sensoren erfassen, oder sie können ein bestimmtes biometrisches Merkmal unter Einbeziehung mehrerer Informationseinheiten berücksichtigen. In manchen Studien werden dieser Kategorie auch Systeme zugeordnet, bei denen dieselben biometrischen Informationen mehrfach erfasst werden, oder bei denen Merkmale einer bestimmten biometrischen Probe mit mehreren Algorithmen ermittelt werden. Zu diesen multimodalen biometrischen Systemen zählen beispielsweise auf EU-Ebene der elektronische Reisepass (e-Passport) oder in den Vereinigten Staaten der biometrische Identifikationsdienst US-VISIT.

Zuverlässigkeit: Mit biometrischen Systemen sind zu 100 % fehlerfreie Ergebnisse nur schwer zu erzielen. Dies kann auf unterschiedliche Umgebungen bei der Datenerfassung (Beleuchtung, Temperatur usw.), aber auch auf die jeweils verwendeten Geräte und Einrichtungen (Kameras, Scanner usw.) zurückzuführen sein. Die am weitesten verbreiteten Parameter zur Leistungsbewertung sind die FAR *(False Accept Rate)* und die FRR *(False Reject Rate)*. Beide Parameter können dem jeweils eingesetzten System angepasst werden.

– False Accept Rate (FAR): Die FAR gibt Aufschluss über die Wahrscheinlichkeit, dass ein biometrisches System eine Person nicht zuverlässig identifiziert oder einen Betrugsversuch nicht erkennt. Sie gibt den Prozentanteil fälschlicherweise angenommener ungültiger Eingaben an. Die FAR wird auch als Anteil der falsch positiven Ergebnisse bezeichnet.

– False Reject Rate (FRR): Als FRR wird die Wahrscheinlichkeit bezeichnet, dass das System Daten unbegründet ablehnt. Eine unbegründete Ablehnung erfolgt dann, wenn eine Person den jeweils vorhandenen biometrischen Templates nicht zugeordnet wird. Die FFR wird auch als Anteil der falsch negativen Ergebnisse bezeichnet.

Bei geeigneter Anpassung des Systems und angemessener Konfiguration können kritische Fehler bei biometrischen Systemen auf ein in der Praxis annehmbares Niveau reduziert werden. Bei einem perfekten System liegen FAR und FRR bei Null. Meist besteht jedoch eine negative Korrelation derart, dass eine höhere FAR mit einer geringeren FRR einhergeht.

Wichtig ist auch, dass der Zweck der Informationsverarbeitung unter Berücksichtigung sowohl der FAR und der FRR als auch der Populationsgröße als Maßstab für die Entscheidung darüber herangezogen wird, ob die Zuverlässigkeit eines biometrischen Systems als annehmbar zu bewerten ist. Außerdem kann bei der Bewertung der Zuverlässigkeit eines biometrischen Systems berücksichtigt

werden, ob das System Merkmale lebender Objekte erfassen kann. Latente Fingerabdrücke beispielsweise können kopiert und zur Erzeugung falscher Fingerabdrücke verwendet werden. Ein Fingerabdruck-Lesegerät darf nicht derart manipulierbar sein, dass eine falsch positive Identifikation erfolgt.

3. Analyse der restlichen Situation

Der relevante Rechtsrahmen besteht in der Datenschutzrichtlinie (95/46/EG). Die Datenschutzgruppe hat bereits in WP 80 darauf hingewiesen, dass biometrische Daten in den meisten Fällen personenbezogene Daten sind. Entsprechend dürfen diese Daten nur dann verarbeitet werden, wenn eine rechtliche Grundlage besteht und wenn die Verarbeitung gemessen am Zweck der jeweiligen Erfassung und/oder Weiterverarbeitung der Daten in angemessener, relevanter und nicht übermäßiger Form erfolgt.

Zweck

Eine Voraussetzung für die Verwendung biometrischer Daten ist eine klare Definition des Zwecks, für den die biometrischen Daten erfasst und verarbeitet werden. Dabei sind die Risiken im Hinblick auf den Schutz grundlegender individueller Rechte und Freiheiten zu berücksichtigen.

Biometrische Daten können beispielsweise erfasst werden, um die Sicherheit von Verarbeitungssystemen zu gewährleisten oder zu erhöhen, indem personenbezogene Daten durch geeignete Maßnahmen vor unbefugtem Zugriff geschützt werden. Grundsätzlich spricht nichts gegen die Einführung geeigneter Sicherheitsmaßnahmen unter Einbeziehung biometrischer Merkmale der für die Verarbeitung verantwortlichen Personen, um ein Sicherheitsniveau gewährleisten zu können, das den mit den betreffenden Verfahren verbundenen Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Dabei sollte allerdings berücksichtigt werden, dass die Nutzung biometrischer Informationen an sich noch keinen Sicherheitsgewinn bedeutet. Zahlreiche biometrische Daten können nämlich ohne Wissen der betreffenden Person beschafft werden. Je höher das angestrebte Sicherheitsniveau, desto weniger werden biometrische Daten alleine geeignet sein, dieses Ziel zu verwirklichen.

Der Grundsatz der Zweckbindung ist ebenso zu berücksichtigen wie die übrigen Grundsätze des Datenschutzes. Bei der Festlegung der unterschiedlichen Zwecke einer Anwendung sind insbesondere die Grundsätze der Verhältnismäßigkeit, der Notwendigkeit und der Datenminimierung zu beachten. Bei Anwendungen mit unterschiedlichen Funktionen muss die betroffene Person nach Möglichkeit zwischen den jeweiligen Zwecken wählen können. Dies gilt insbesondere, wenn einer oder mehrere Zwecke die Verarbeitung biometrischer Daten erfordern.

Beispiel:
Die Verwendung elektronischer Geräte mit spezifischen Authentifikationsverfahren auf der Grundlage biometrischer Daten wurde in Verbindung mit geeigneten Sicherheitsmaßnahmen in den folgenden Fällen empfohlen:

– Verarbeitung personenbezogener Daten, die von Fernmeldebetreibern durch Abhören mit richterlicher Genehmigung erlangt wurden;

– Zugang zu Verkehrsdaten (und zu Standortdaten), die für gerichtliche Zwecke von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze aufbewahrt werden, und Zugang zu den Räumlichkeiten, in denen diese Daten verarbeitet werden;

– Erfassung und Speicherung genetischer Daten und biologischer Proben.

Fotos im Internet, in sozialen Medien und in Online-Anwendungen zur Verwaltung und Weitergabe von Fotos dürfen nicht zur Erstellung biometrischer Templates oder zum Einlesen von Daten in ein System verwendet werden, das die automatische Erkennung der fotografierten Personen (Gesichtserkennung) ermöglichen würde, ohne dass eine konkrete Rechtsgrundlage (z. B. eine Einwilligung) für diesen neuen Zweck gegeben wäre. Auch wenn eine Rechtsgrundlage für diesen nachgeordneten Verarbeitungszweck besteht, muss die Verarbeitung bezogen auf diesen Zweck angemessen und relevant sein, und die Verarbeitung darf nicht in übermäßigem Umfang erfolgen. Wenn die betroffene Person eingewilligt hat, dass Fotos, auf denen diese Person zu sehen ist, automatisch derart verarbeitet werden, dass die Personen in einem Online-Fotoalbum mit einem Algorithmus zur Gesichtserkennung identifiziert werden können, muss diese Verarbeitung unter Berücksichtigung der geltenden Datenschutzvorschriften erfolgen. Biometrische Daten, die nach der Kennzeichnung der Bilder mit dem Namen, einem Benutzernamen oder einem sonstigen von der betroffenen Person eingegebenen Text nicht mehr benötigt werden, müssen gelöscht werden. Die Erzeugung einer permanenten Datenbank mit biometrischen Daten ist für diesen Zweck nicht unbedingt nicht erforderlich.

Verhältnismäßigkeit

Bei der Nutzung biometrischer Daten stellt sich die Frage der Verhältnismäßigkeit der in den einzelnen Kategorien verarbeiteten Daten vor dem Hintergrund des Zwecks der jeweiligen Verarbeitung. Da biometrische Daten nur dann verwendet werden können, wenn sie angemessen und relevant sind und nicht in übermäßigem Umfang erfasst werden, müssen die Notwendigkeit und die Verhältnismäßigkeit der Verarbeitung streng geprüft werden. Außerdem muss geprüft werden, ob der beabsichtigte Zweck nicht auch unter stärkerer Respektierung der Privatsphäre erreicht werden könnte.

Bei der Analyse der Verhältnismäßigkeit eines vorgeschlagenen biometrischen Systems ist vorab zu prüfen, ob das System erforderlich ist, um den ermittelten Zweck zu erfüllen, d. h., ob dieses System für die Erfüllung dieses Zwecks tatsächlich wesentlich ist oder bloß die bequemste oder kostengünstigste Lösung darstellt. Ein zweiter Faktor ist, ob das System zur Erfüllung des vorgesehenen Zwecks wahrscheinlich effizient ist. In diesem Zusammenhang sind die spezifischen Merkmale der vorgesehenen biometrischen Technologie zu berücksichtigen.[1] Ein dritter Aspekt besteht in der Abwägung, ob die zu erwartende Beeinträchtigung der Privatsphäre im Verhältnis zum erwarteten Nutzen steht. Wenn dieser Nutzen verhältnismäßig gering ist und beispielsweise nur in erhöhter Bequemlichkeit oder in einer geringen Kosteneinsparung besteht, ist die Beeinträchtigung der Privatsphäre nicht als verhältnismäßig zu bewerten. Der vierte Aspekt für die Bewertung der Angemessenheit eines biometrischen Systems besteht in der Prüfung, ob das gewünschte Ergebnis nicht auch mit Mitteln erreicht werden könnte, welche die Privatsphäre weniger beeinträchtigen würden.[2]

Beispiel:
In einem Health- und Fitness-Club wird ein zentrales biometrisches System eingerichtet, das aufgrund der erfassten Fingerabdrücke Zugang zu den Trainingsräumen und zu den entsprechenden Einrichtungen nur den Kunden gewähren soll, die ihre Beiträge ordnungsgemäß gezahlt haben.

Um dieses System einsetzen zu können, müssen die Fingerabdrücke aller Kunden und aller Mitarbeiter erfasst werden. Diese biometrische Anwendung scheint gemessen an der Notwendigkeit der Kontrolle des Zugangs zum Club und der einfacheren Kundenverwaltung als unverhältnismäßig. Andere Maßnahmen wie z. B. die Verwendung einer einfachen Liste oder der Einsatz von RFID-Etiketten oder Magnetstreifenkarten, bei denen die Notwendigkeit der Verarbeitung biometrischer Daten entfiele, wären ebenso gut als praktikabel und wirksam vorstellbar.

Angesichts der potenziell schädlichen Folgen für die betreffenden Personen warnt die Datenschutzgruppe vor den Risiken einer Nutzung biometrischer Daten für Identifikationszwecke in großen zentralen Datenbanken.

Bei derartigen Systemen sollten die erheblichen Auswirkungen auf die Menschenwürde und auf die Grundrechte der betroffenen Personen berücksichtigt werden. Vor dem Hintergrund der Europäischen Konvention zum Schutz der

[1] Biometrische Verfahren werden entweder für Verifikations- oder für Identifikationszwecke verwendet. Ein biometrischer Identifikator könnte aus technischer Sicht für einen Zweck geeignet und für den anderen Zweck als ungeeignet zu bewerten sein. (Technologien mit einer niedrigen FRR beispielsweise sollten vorzugsweise in Systemen für Identifikationszwecke in der Rechtsdurchsetzung eingesetzt werden.)

[2] Beispielsweise mit Smart Cards oder mit sonstigen Methoden, bei denen biometrische Informationen für Authentifikationszwecke nicht erfasst oder zentral verwaltet werden.

Menschenrechte und Grundfreiheiten (EMRK) sowie angesichts der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte im Zusammenhang mit Artikel 8 der Konvention betont die Datenschutzgruppe, dass jegliche Beeinträchtigung des Rechts auf Datenschutz nur unter der Bedingung zulässig ist, dass die Beeinträchtigung im Einklang mit geltenden Rechtsvorschriften steht und erforderlich ist, um in einer demokratischen Gesellschaft ein übergeordnetes öffentliches Interesse zu schützen.[3]

Um sicherzustellen, dass diese Voraussetzungen erfüllt werden, muss das Ziel spezifiziert werden, das mit dem jeweiligen System verfolgt werden soll. Außerdem muss die Verhältnismäßigkeit der in das System einzubindenden Daten gemessen am betreffenden Ziel bewertet werden.

Dazu muss der für die Verarbeitung Verantwortliche feststellen, ob die Verarbeitung und die eingesetzten Mechanismen sowie die Kategorien der zu erfassenden und zu verarbeitenden Daten und der Transfer der in der Datenbank enthaltenen Informationen notwendig und unumgänglich sind. Die getroffenen Sicherheitsmaßnahmen müssen angemessen und wirksam sein. Der für die Verarbeitung Verantwortliche muss die Rechte der Personen berücksichtigen, auf die sich die jeweiligen personenbezogenen Daten beziehen. Außerdem muss der für die Verarbeitung Verantwortliche sicherstellen, dass ein geeigneter Mechanismus zur Anwendung kommt, um die Wahrnehmung dieser Rechte zu ermöglichen.

Beispiel:
Nutzung biometrischer Daten für Identifikationszwecke: Systeme, die das Gesicht oder die DNA einer Person analysieren, können in erheblichem Umfang zur Bekämpfung von Kriminalität und zur Feststellung der Identität einer unbekannten Person beitragen, die einer schweren Straftat verdächtigt wird. Wenn diese Systeme allerdings in großem Umfang eingesetzt werden, können sie auch mit schwerwiegenden Nachteilen einhergehen. Durch Gesichtserkennung können biometrische Daten ohne Wissen der betroffenen Person leicht für vielfältige Nutzungsmöglichkeiten erfasst werden. Der zunehmende Einsatz dieser Technologie würde der Anonymität in öffentlichen Räumen ein Ende setzen und die konsequente Verfolgung einzelner Personen ermöglichen. Technologien zur Analyse von DNA-Proben bergen die Gefahr, dass empfindliche Daten über die Gesundheit einer Person offen gelegt werden könnten.

[3] Siehe Europäischer Gerichtshof, Urteil vom 20. Mai 2003 in den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01 (Rechnungshof/Österreichischer Rundfunk u. a.), Europäischer Gerichtshof für Menschenrechte, Urteil vom 4. Dezember 2008, Beschwerden Nrn. 30562/04 und 30566/04 (S. und Marper/Vereinigtes Königreich) und Urteil vom 19. Juli 2011, Beschwerden Nrn. 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 und 64027/09 (Goggins u. a./Vereinigtes Königreich).

Zuverlässigkeit

Biometrische Daten müssen zuverlässig und für den jeweiligen Zweck der Erfassung relevant sein. Die erforderliche Zuverlässigkeit muss sowohl bei der Erfassung als auch bei der Herstellung der Verbindung zwischen einer Person und den betreffenden biometrischen Daten gegeben sein. Die Zuverlässigkeit zum Zeitpunkt der Erfassung ist unter anderem im Hinblick auf die Verhinderung eines Identitätsbetrugs von Bedeutung.

Biometrische Daten sind individuell, und biometrische Daten ergeben meist individuelle Templates oder Bilder. Bei Nutzung in großem Umfang und insbesondere in Verbindung mit einem erheblichen Anteil der Bevölkerung können biometrische Daten als „Kennzeichen allgemeiner Bedeutung" gemäß der Richtlinie 95/46/EG betrachtet werden. In diesem Fall kommt Artikel 8 Absatz 7 der Richtlinie 95/46/EG zur Anwendung, und die Mitgliedstaaten sind entsprechend verpflichtet, die jeweiligen Verarbeitungsbedingungen zu prüfen.

Datenminimierung

Eine besondere Schwierigkeit kann sich dadurch ergeben, dass biometrische Daten häufig mehr Informationen erfassen als für den eigentlichen Abgleich erforderlich. Der Grundsatz der Datenminimierung ist vom für die Verarbeitung Verantwortlichen durchzusetzen. Dies bedeutet erstens, dass nicht sämtliche verfügbaren Informationen, sondern nur die tatsächlich benötigten Informationen verarbeitet, übertragen und gespeichert werden sollten. Und zweitens sollte der für die Verarbeitung Verantwortliche sicherstellen, dass bereits die Standardkonfiguration des betreffenden Systems den Datenschutz fördert, ohne dass besondere Maßnahmen zur Durchsetzung des Datenschutzes getroffen werden müssen.

Aufbewahrungsfrist

Der für die Verarbeitung Verantwortliche sollte eine Aufbewahrungsfrist für biometrische Daten festlegen, die nicht länger ist als für die Zwecke der Erfassung oder der Weiterverarbeitung der Daten tatsächlich erforderlich. Er muss sicherstellen, dass die Daten und die von diesen Daten abgeleiteten Profile nach diesem als berechtigt zu betrachtenden Zeitraum unwiderruflich gelöscht werden.

Dabei muss eindeutig zwischen allgemeinen personenbezogenen Daten, die vielleicht über einen längeren Zeitraum benötigt werden, und biometrischen Daten unterschieden werden, die nicht mehr von Bedeutung sind (beispielsweise, weil die betroffene Person zu einem bestimmten Bereich ohnehin keinen Zutritt mehr hat).

Beispiel:
Ein Arbeitgeber setzt ein biometrisches System ein, um den Zugang zu einem bestimmten Bereich einzuschränken. Die Tätigkeit eines Mitarbeiters setzt nicht mehr voraus, dass dieser Mitarbeiter Zugang zu dem betreffenden Bereich hat (etwa weil sich die Zuständigkeit des Mitarbeiters geändert hat oder weil der Mitarbeiter inzwischen bei einem anderen Arbeitgeber beschäftigt ist). In diesem Fall müssen die betreffenden biometrischen Daten gelöscht werden, da der ursprüngliche Erfassungszweck nicht mehr gegeben ist.

3.1. Rechtmäßiger Grund

Die Verarbeitung biometrischer Daten muss aus den in Artikel 7 der Richtlinie 95/46/EG genannten rechtmäßigen Gründen erfolgen.

3.1.1. Einwilligung, Artikel 7 Buchstabe a

Der erste in Artikel 7 Buchstabe a genannte rechtmäßige Grund ist die Einwilligung der betroffenen Person zur Verarbeitung ihrer Daten. Gemäß Artikel 2 Buchstabe h der Datenschutzrichtlinie muss die Einwilligung der betroffenen Person ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgen. Diese Einwilligung wird allerdings dann selbstverständlich nicht ohne Zwang erlangt, wenn allgemeine Geschäftsbedingungen oder Sonderregelungen zwingend vorgeschrieben sind. Außerdem muss die Einwilligung widerruflich sein. In diesem Zusammenhang möchte die Datenschutzgruppe in ihrer Stellungnahme zum Begriff der Einwilligung auf einige wichtige Aspekte hinweisen: die Gültigkeit der Einwilligung, das individuelle Recht zum Widerruf der Einwilligung, die Notwendigkeit der Erteilung der Einwilligung vor Beginn der Verarbeitung und die Anforderungen bezüglich der Qualität und der Zugänglichkeit der Informationen.[4]

In vielen Fällen, in denen biometrische Daten verarbeitet werden, ist eine Einwilligung unter Umständen nicht als freiwillig erteilt zu bewerten. Dies gilt beispielsweise dann, wenn keine gültige Alternative wie z. B. die Eingabe eines Kennwortes oder die Verwendung einer Magnetstreifenkarte verfügbar ist. Ein System, das betroffene Personen von einer Nutzung dieses Systems ab-

[4] WP 187, Stellungnahme 15/2011 zum Begriff der Einwilligung.

halten würde (beispielsweise weil die Nutzung für die Benutzer zu zeitaufwendig oder zu kompliziert wäre), könnte nicht als gültige Alternative betrachtet werden. Entsprechend wäre auch eine erteilte Einwilligung nicht als gültig zu bewerten.

Beispiele:
Wenn keine sonstigen rechtmäßigen Gründe gegeben sind, könnte ein biometrisches Authentifikationssystem nur dann als Zugangskontrolle für einen Videoclub eingesetzt werden, wenn die Kunden frei entscheiden können, ob sie das betreffende System tatsächlich nutzen möchten. Entsprechend muss der Besitzer des Videoclubs Mechanismen bereitstellen, welche die Privatsphäre der Kunden weniger beeinträchtigen. Die betreffenden Mechanismen würden auch den Kunden Zugang gewähren, die aus persönlichen Gründen nicht bereit oder nicht in der Lage sind, die Zugangskontrolle durch Fingerabdrücke zu nutzen. Wenn als einzige Möglichkeit anstelle der geforderten Einwilligung zur Nutzung der individuellen biometrischen Daten der Verzicht auf das betreffende Angebot bleibt, ist dies ein deutlicher Anhaltspunkt dafür, dass die Einwilligung nicht freiwillig erteilt wurde und somit nicht als rechtmäßiger Grund bewertet werden kann.

In einem Kindergarten wird ein Venenstruktur-Scanner eingerichtet, um die Zugangsberechtigung sämtlicher Erwachsener (Eltern, Erzieher und Verwaltungspersonal) zu prüfen. Um dieses System einsetzen zu können, müssen die Fingerabdrücke aller Eltern und aller Mitarbeiter erfasst werden. Eine Einwilligungsregelung wäre eine fragliche Rechtsgrundlage insbesondere für die Mitarbeiter, da diesen im Grunde keine Wahl bleibt, als die geforderte Einwilligung zu diesem System zu erteilen. Auch für die Eltern wäre diese Regelung zweifelhaft, da keine alternative Möglichkeit gegeben wäre, Zugang zum Kindergarten zu erhalten.

Es kann zwar mit hoher Wahrscheinlichkeit angenommen werden, dass die Einwilligung wegen des typischen Ungleichgewichts zwischen Arbeitgebern und Arbeitnehmern nicht allzu aussagekräftig wäre. Die Datenschutzgruppe kann die Glaubwürdigkeit der Einwilligung jedoch auch nicht vollständig ausschließen, *„sofern hinreichende Garantien dafür bestehen, dass die Einwilligung tatsächlich freiwillig erteilt wurde“*.[5]

Insoweit sind Einwilligungen im Zusammenhang mit Beschäftigungsverhältnissen grundsätzlich zu prüfen, und entsprechende Regelungen müssen angemessen gerechtfertigt sein. Statt eine Einwilligung anzustreben, könnten Arbeitgeber

[5] WP 187, Stellungnahme 15/2011 zum Begriff der Einwilligung.

prüfen, ob die Verwendung biometrischer Daten von Mitarbeitern für einen rechtmäßigen Zweck nachweislich erforderlich ist und ob die gegebenenfalls festgestellte Notwendigkeit nicht zu einer Beeinträchtigung der Grundrechte und Freiheiten der Mitarbeiter führt. Wenn die Notwendigkeit angemessen begründet werden kann, könnte das rechtmäßige Interesse des für die Verarbeitung Verantwortlichen gemäß Artikel 7 Buchstabe f der Richtlinie 95/46/EG die Rechtsgrundlage für eine Verarbeitung sein. Der Arbeitgeber muss immer bestrebt sein, das die Privatsphäre am wenigsten beeinträchtigende Verfahren einzusetzen und nach Möglichkeit auf biometrische Prozesse zu verzichten.

Wie in Abschnitt 3.1.3, beschrieben, können jedoch Fälle vorkommen, in denen ein biometrisches System im rechtmäßigen Interesse des für die Verarbeitung Verantwortlichen liegen kann. In diesen Fällen wäre eine Einwilligung nicht erforderlich.

Eine Einwilligung ist nur dann gültig, wenn hinreichende Auskünfte zur Verwendung der biometrischen Daten erteilt werden. Da biometrische Daten als individuelle und universale Identifikatoren dienen können, ist die Bereitstellung klarer und leicht zugänglicher Informationen über die Nutzung der jeweiligen Daten als unabdingbare Voraussetzung für eine faire Verarbeitung zu betrachten. Dies ist entsprechend eine entscheidende Bedingung für das Vorliegen einer gültigen Einwilligung im Zusammenhang mit der Nutzung biometrischer Daten.

Beispiele:
Eine gültige Einwilligung zur Nutzung eines Zugangskontrollsystems unter Verwendung von Fingerabdrücken setzt voraus, dass darüber informiert wurde, ob das betreffende biometrische System ein für dieses System spezifisches Template erzeugt. Wenn ein eingesetzter Algorithmus dasselbe biometrische Template auch in anderen biometrischen Systemen erzeugt, muss die betroffene Person wissen, dass sie in auch in anderen biometrischen Systemen wiedererkannt werden könnte.

Ein Nutzer lädt sein Foto in ein Fotoalbum im Internet hoch. Die Erfassung dieses Fotos in einem biometrischen System erfordert eine ausdrückliche Einwilligung auf der Grundlage umfassender Informationen dahin gehend, was mit den biometrischen Daten geschieht und für welchen Zeitraum und für welche Zwecke die Daten verarbeitet werden.

Eine Einwilligung kann jederzeit widerrufen werden, wenn die für die Verarbeitung Verantwortlichen genötigt sind, technische Einrichtungen in ihre Systeme aufzunehmen, welche die Nutzung biometrischer Daten in ihren Systemen erheblich verändern könnten. Ein biometrisches System, das auf der Grundlage einer

Einwilligung genutzt wird, muss daher in der Lage sein, sämtliche von diesem System erzeugten Verknüpfungen mit einer bestimmten Identität wirksam rückgängig zu machen.

3.1.2. Vertrag, Artikel 7 Buchstabe b

Die Verarbeitung biometrischer Daten kann für die Erfüllung eines Vertrags erforderlich sein, an dem die betroffene Person als Partei beteiligt ist. Ebenso kann die Verarbeitung der Daten Voraussetzung für die Durchführung vorvertraglicher Maßnahmen sein, die auf Antrag der betroffenen Person erfolgen. Allerdings ist darauf hinzuweisen, dass dies im Allgemeinen nur für ausschließlich biometrische Dienste von Bedeutung ist. Diese Rechtsgrundlage kann nicht zur Legitimierung einer nachgeordneten Leistung herangezogen werden, die darin bestünde, eine Person in einem biometrischen System zu erfassen. Wenn eine derartige Leistung von der eigentlichen Leistung getrennt werden kann, ist der Vertrag über die eigentliche Leistung nicht als rechtmäßige Grundlage für die Verarbeitung biometrischer Daten zu betrachten. Personenbezogene Daten sind keine Güter, die als Gegenleistung für eine erbrachte Leistung verlangt werden könnten. Daher können entsprechende Verträge sowie Verträge, denen zufolge eine Leistung nur unter der Bedingung erbracht wird, dass jemand zur Verarbeitung seiner biometrischen Daten im Gegenzug für eine anderweitige Leistung zustimmt, keine Rechtsgrundlage für eine derartige Verarbeitung sein.

Beispiele:
a) Zwei Brüder geben in einem Labor Haarproben für eine DNA-Analyse ab, um festzustellen, ob sie tatsächlich leibliche Brüder sind. Der mit diesem Labor geschlossene Vertrag über die Durchführung dieser Analyse stellt eine hinreichende Rechtsgrundlage für die Erfassung und die Verarbeitung der betreffenden biometrischen Daten dar.

b) Jemand lädt in einem sozialen Netz ein Foto in sein Fotoalbum hoch, um seinen Freunden dieses Foto zeigen zu können. Wenn die vertraglichen Bestimmungen (Nutzungsbedingungen) die Inanspruchnahme des betreffenden Dienstes daran knüpfen, dass der jeweilige Nutzer in einem biometrischen System erfasst wird, ist diese Bestimmung nicht als hinreichende Rechtsgrundlage für die Erfassung der Daten zu bewerten.

3.1.3. Rechtliche Verpflichtung, Artikel 7 Buchstabe c

Ein weiterer Rechtsgrund für die Verarbeitung personenbezogener Daten ist gegeben, wenn die Verarbeitung erforderlich ist, um eine rechtliche Verpflichtung

des für die Verarbeitung Verantwortlichen zu erfüllen. In manchen Ländern ist dies beispielsweise bei der Erstellung und/oder Vorlage von Reisepässen[6] und Visa[7] erforderlich.

3.1.4. Berechtigtes Interesse des für die Verarbeitung Verantwortlichen, Artikel 7 Buchstabe f

Gemäß Artikel 7 der Richtlinie 95/46/EG kann die Verarbeitung biometrischer personenbezogener Daten auch dann gerechtfertigt sein, wenn diese Daten *„zur Verwirklichung des berechtigten Interesses [erforderlich sind], das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen."*

Insoweit kann es vorkommen, dass die Verwendung biometrischer Systeme im berechtigten Interesse des für die Verarbeitung Verantwortlichen liegt. Das Interesse ist jedoch nur dann berechtigt, wenn der für die Verarbeitung Verantwortliche nachweisen kann, dass sein Interesse objektiv stärker wiegt als das Recht der betroffenen Personen darauf, der Erfassung in einem biometrischen System zu widersprechen. Wenn beispielsweise die Sicherheit von Hochrisikobereichen durch einen speziellen Mechanismus gewährleistet werden muss, mit dem genau geprüft werden kann, ob Personen tatsächlich zugangsberechtigt sind, kann die Verwendung eines biometrischen Systems als im berechtigten Interesse des für die Verarbeitung Verantwortlichen liegend bewertet werden. Im folgenden Beispiel eines biometrischen Systems zur Kontrolle des Zugangs zu einem Labor ist ein angemessener Schutz dieses Bereichs durch Maßnahmen, welche die Privatsphäre weniger beeinträchtigen würden, nicht verfügbar. Daher kann der für die Verarbeitung Verantwortliche den Mitarbeitern keinen alternativen Mechanismus anbieten, ohne die Sicherheit des zu schützenden Bereichs zu beeinträchtigen. Insoweit liegt es im berechtigten Interesse des für die Verarbeitung Verantwort-

---

6 In Reisepässe wurden Fingerabdrücke gemäß der Verordnung (EU) 2252/2004 des Rates vom 13. Dezember 2004 aufgenommen. Rechtsgrundlage für die Aufnahme von Fingerabdrücken in Aufenthaltstitel ist die Verordnung (EU) 1030/2002 des Rates vom 13. Juni 2002.

7 Die Registrierung biometrischer Identifikatoren in das Visa-Informationssystem (VIS) ist in der Verordnung (EG) Nr. 767/2008 l vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) geregelt; siehe auch Stellungnahme Nr. 3/2007 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen (KOM(2006)269 endg.). WP 134; Stellungnahme 2/2005 – Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (KOM (2004) 835 endgültig) WP 110; Stellungnahme Nr. 7/2004 zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS, WP 96.

lichen, das betreffende System einzurichten und eine begrenzte Anzahl an Mitarbeitern zu erfassen. Die Einwilligung dieser Mitarbeiter ist dazu nicht erforderlich. Auch wenn ein berechtigtes Interesse des für die Verarbeitung Verantwortlichen als gültiger Rechtsgrund für die Verarbeitung zu bewerten ist, sind alle sonstigen Grundsätze des Datenschutzes zu beachten, insbesondere der Grundsatz der Verhältnismäßigkeit und der Datenminimierung.

Beispiel:
In einem Unternehmen, das an gefährlichen Viren forscht, ist das Labor durch Türen geschützt, die erst nach erfolgreicher Prüfung eines Fingerabdrucks und nach einer Iris-Erkennung geöffnet werden. Dieser Kontrollmechanismus wurde eingerichtet, um sicherzustellen, dass nur die mit den jeweiligen Risiken vertrauten, für die betreffenden Verfahren geschulten und von dem jeweiligen Unternehmen für vertrauenswürdig befundenen Personen Versuche mit diesen gefährlichen Materialien durchführen können. Das berechtigte Interesse des Unternehmens, sicherzustellen, dass nur die betreffenden Personen Zugang zu einem geschützten Bereich erhalten, um auf diese Weise die mit einem Zutritt verbundenen Sicherheitsrisiken zu reduzieren, wiegt erheblich stärker als der etwaige Wunsch der jeweiligen Personen, eine Verarbeitung ihrer biometrischen Daten zu verhindern.

Grundsätzlich kann die Verwendung biometrischer Daten im Interesse der allgemeinen Sicherheit von Vermögenswerten und von Personen nicht als berechtigtes Interesse betrachtet werden, das gegenüber den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen überwiegen würde. Im Gegenteil: Die Verarbeitung biometrischer Daten ist nur dann als erforderliches Mittel zur Gewährleistung der Sicherheit von Vermögenswerten und/oder von Personen zu bewerten, wenn anhand objektiver und dokumentierter Umstände nachgewiesen werden kann, dass im konkreten Fall ein erhebliches Risiko besteht. Dazu muss der für die Verarbeitung Verantwortliche nachweisen, dass die betreffenden Gegebenheiten ein konkretes und erhebliches Risiko bedingen, das der für die Verarbeitung Verantwortliche mit besonderer Sorgfalt bewerten muss. Um dem Grundsatz der Verhältnismäßigkeit gerecht zu werden, muss der für die Verarbeitung Verantwortliche bei derart hohen Risiken prüfen, ob alternative Maßnahmen verfügbar sind, mit denen die angestrebten Ziele ebenso verwirklicht werden könnten, die Privatsphäre der betroffenen Personen aber weniger beeinträchtigt würde. Wenn derartige alternative Maßnahmen in Betracht kommen, ist der für die Verarbeitung Verantwortliche verpflichtet, diese alternativen Möglichkeiten zu nutzen. Außerdem sollte regelmäßig geprüft werden, ob die betreffenden Gegebenheiten immer noch bestehen. Aufgrund dieser Prüfungen müssen jegliche Verarbeitungsprozesse, die sich als nicht mehr gerechtfertigt erweisen, eingestellt oder zumindest ausgesetzt werden.

3.2. Für die Verarbeitung Verantwortliche und Auftragsverarbeiter

Gemäß der Richtlinie 95/46/EG unterliegen die für die Verarbeitung Verantwortlichen bei der Verarbeitung personenbezogener Daten bestimmten Verpflichtungen. Im Zusammenhang mit biometrischen Daten können unterschiedliche Typen von Rechtssubjekten (z. B. Arbeitgeber, Rechtsdurchsetzungsbehörden oder Einwanderungsbehörden) die Funktion des für die Verarbeitung Verantwortlichen übernehmen.

Die Datenschutzgruppe erinnert an die Leitlinien in ihrer Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter".[8] Diese Stellungnahme enthält eindeutige Erläuterungen dahin gehend, wie diese Kernbegriffe der Richtlinie zu verstehen sind.

3.3. Automatisierte Verarbeitung (Artikel 15 der Richtlinie)

Wenn auf der Verarbeitung biometrischer Daten beruhende Systeme eingesetzt werden, sollte sorgfältig auf potenziell diskriminierende Folgen für die vom System zurückgewiesenen Personen geachtet werden. Wenn eine Maßnahme eine natürliche Person beeinträchtigen könnte, weil die Datenverarbeitung ausschließlich automatisch erfolgt, sind zudem geeignete Garantien vorzusehen (z. B. die Möglichkeit manueller Eingriffe sowie Abhilfemaßnahmen oder Mechanismen, die den betroffenen Personen die Darstellung ihrer Standpunkte ermöglichen), damit das individuelle Recht darauf gewahrt werden kann, sich der Unterwerfung unter diese Maßnahme zu entziehen.

In Artikel 15 der Richtlinie 95/46/EG heißt es: *„Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens."*

3.4. Transparenz und Aufklärung der betroffenen Person

Gemäß dem Grundsatz von Treu und Glauben bei der Verarbeitung muss betroffenen Personen bekannt sein, dass ihre biometrischen Daten erfasst und/oder verwendet werden (Artikel 6 der Richtlinie 95/46/EG). Jegliche Systeme, die derar-

[8] WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter".

tige Daten ohne Wissen der betroffenen Personen erfassen würden, sind zu vermeiden.

Der für die Verarbeitung Verantwortliche muss sicherstellen, dass die betroffenen Personen über die wesentlichen Elemente der Verarbeitung gemäß Artikel 10 der Datenschutzrichtlinie (Identität des für die Verarbeitung Verantwortlichen, Zweckbestimmung der Verarbeitung, Datentyp, Dauer der Verarbeitung, Zugriffs-, Änderungs- und Löschungsrechte der betroffenen Personen, das Recht der betroffenen Personen zum Widerruf ihrer Einwilligung und Informationen über die Empfänger bzw. über die Empfängerkategorien, denen die jeweiligen Daten offen gelegt werden) angemessen unterrichtet werden. Da der für die Verarbeitung Verantwortliche bei biometrischen Systemen verpflichtet ist, die betroffene Person entsprechend zu unterrichten, dürfen biometrische Daten nicht ohne Wissen der betroffenen Personen erfasst werden.

3.5. Recht auf Zugang zu biometrischen Daten

Betroffene Personen haben einen Anspruch darauf, dass die für die Verarbeitung Verantwortlichen ihnen Zugang zu ihren Daten (im Allgemeinen einschließlich ihrer biometrischen Daten) gewähren. Außerdem haben betroffene Personen ein Anrecht auf Zugang zu möglichen Profilen, die auf der Grundlage dieser biometrischen Daten erstellt werden. Wenn der für die Verarbeitung Verantwortliche die Identität der betroffenen Personen prüfen muss, um diesen Zugang zu gewähren, ist entscheidend, dass dies geschieht, ohne weitere personenbezogene Daten zu verarbeiten.

3.6. Datensicherheit

Die für die Verarbeitung Verantwortlichen müssen geeignete technische und organisatorische Maßnahmen treffen, um die zufällige oder unbefugte Zerstörung, den zufälligen Verlust, die unbefugte Änderung oder Weitergabe, den ungefugten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und die unbefugte Verarbeitung personenbezogener Daten in jeglicher sonstiger Form zu verhindern.[9]

Alle erfassten und gespeicherten Daten müssen angemessen gesichert werden. Mit der Auslegung eines Systems befasste Personen müssen durch Hinzuziehung geeigneter Sicherheitsexperten sicherstellen, dass Sicherheitsbedrohungen in angemessener Weise gehandhabt werden. Dies gilt insbesondere für die Portierung bestehender Systeme auf das Internet.

[9] Artikel 17 Absatz 1 der Richtlinie 95/46/EG.

3.7. Garantien für Personen mit besonderen Bedürfnissen

Die Verwendung biometrischer Daten kann die Würde, die Privatsphäre und das Recht auf Datenschutz gefährdeter Personen (z. B. kleiner Kinder und älterer Menschen) sowie derjenigen beeinträchtigen, die aus körperlichen Gründen nicht in der Lage sind, sich dem Erfassungsprozess zu unterziehen. In Anbetracht der potenziell nachteiligen Konsequenzen für die betroffenen Personen müssen bei der Folgenabschätzung im Hinblick auf sämtliche Maßnahmen, welche die Würde einer Person beeinträchtigen könnten, strengere Anforderungen erfüllt werden. In diesem Zusammenhang sind die Notwendigkeit und die Verhältnismäßigkeit der Maßnahmen sowie die der jeweils betroffenen Person verbleibenden Möglichkeiten zur Wahrnehmung ihrer Datenschutzrechte zu prüfen, damit die betreffende Maßnahme als zulässig bewertet werden kann. Dem Risiko einer Stigmatisierung und Diskriminierung der betreffenden Personen aufgrund ihres Alters oder infolge der Tatsache, dass es bestimmten Personen nicht möglich ist, die betreffenden Systeme zu nutzen, muss durch geeignete Garantien begegnet werden.

Bezüglich der Einführung einer allgemeinen rechtlichen Verpflichtung zur Erfassung biometrischer Identifikatoren für diese Gruppen (insbesondere für kleine Kinder und für ältere Menschen) im Zusammenhang mit Identifikationen im Rahmen von Grenzkontrollen ist die Datenschutzgruppe der Ansicht, *„dass die Erfassung und die Verarbeitung der Fingerabdrücke – im Interesse der Würde des Betreffenden und der Zuverlässigkeit des Verfahrens – bei Kindern und älteren Menschen eingeschränkt werden sollten und dass die Altersgrenzen den für andere große biometrische Datenbanken der EU (insbesondere Eurodac) geltenden Altersgrenzen entsprechen sollten.“*[10]

In jedem Fall sollten spezifische Garantien (z. B. geeignete Alternativverfahren) eingerichtet werden, um die Wahrung der Menschenwürde und der Grundrechte von Personen sicherzustellen, bei denen eine Erfassung nicht möglich ist, und um auszuschließen, dass diese Personen Opfer eines unzulänglichen technischen Systems werden.[11]

3.8. Sensible Daten

Gewisse biometrische Daten können als sensible Daten gemäß Artikel 8 der Richtlinie 95/46/EC betrachtet werden. Dies gilt insbesondere für Daten, aus

[10] WP 134 – Stellungnahme Nr. 3/2007 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen (KOM(2006)269 endg.).

[11] Siehe WP 134 – Stellungnahme Nr. 3/2007, S. 8.

denen die rassische und ethnische Herkunft hervorgehen, sowie für Gesundheitsdaten. Die DNA-Daten einer Person beispielsweise enthalten häufig auch Daten über die Gesundheit der betreffenden Person oder können Aufschluss über die rassische oder die ethnische Herkunft geben. In diesem Fall sind DNA-Daten als sensible Daten zu betrachten, bei denen zusätzlich zu den allgemeinen Grundsätzen des Datenschutzes gemäß der Richtlinie die in Artikel 8 vorgesehenen besonderen Garantien zu berücksichtigen sind. Bei der Bewertung der Sensibilität der mit einem biometrischen System zu verarbeitenden Daten sollten auch die Umstände der Verarbeitung berücksichtigt werden.[12]

3.9. Die Rolle nationaler Datenschutzbehörden

Angesichts der zunehmenden Normierung der Interoperabilität biometrischer Technologien wird allgemein anerkannt, dass die zentrale Speicherung biometrischer Daten sowohl die Gefahr der Nutzung biometrischer Daten zur Verknüpfung von Datenbanken (mit der Möglichkeit der Erzeugung detaillierter Profile einzelner Personen) als auch spezifische Risiken dahin gehend birgt, dass diese Daten – insbesondere bei unbefugten Zugriffen – zu nicht annehmbaren Zwecken genutzt werden.

Die Datenschutzgruppe empfiehlt, dass für Systeme, die biometrische Daten zur Verknüpfung von Datenbanken verwenden, zusätzliche Garantien vorgeschrieben werden, da diese Formen der Verarbeitung spezifische Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können (Artikel 20 der Richtlinie 95/46/EG). Um geeignete Garantien sicherzustellen und insbesondere um die Risiken für die betroffenen Personen zu mindern, sollte der jeweils für die Verarbeitung Verantwortliche die zuständige nationale Datenschutzbehörde konsultieren, bevor die betreffenden Maßnahmen eingeführt werden.

4. Neue Entwicklungen, technische Trends und Szenarien

4.1. Einleitung

Biometrische Technologien werden vorwiegend von Verwaltungsbehörden schon lange genutzt. In letzter Zeit spielen zunehmend auch kommerzielle Organisationen eine entscheidende Rolle bei der Nutzung dieser Technologien und bei der Entwicklung neuer Produkte.

Einer der wichtigsten Gründe für diese Entwicklung liegt darin, dass diese Technologien einen derartigen Reifegrad erlangt haben, dass biometrische Systeme, die ursprünglich nur unter kontrollierten Bedingungen gut funktionierten, inzwi-

[12] Siehe WP 29, *Advice paper on special categories of data („sensitive data")*, siehe Ares (2011)444105 – 20.4.2011.

schen in großem Umfang auch in anderen Umgebungen eingesetzt werden können. Insoweit sind biometrische Daten manchmal als Ersatz für konventionelle Identifikationsmethoden oder als Verbesserung dieser Methoden zu betrachten. Dies gilt insbesondere für Methoden, die auf mehreren Identifikationsfaktoren beruhen und die etwa bei starken Authentifikationssystemen benötigt werden. Außerdem werden biometrische Technologien zunehmend in Anwendungen eingesetzt, mit denen Personen zwar mit geringerer Zuverlässigkeit, dafür aber rasch und bequem identifiziert werden können.

Die Nutzung biometrischer Technologien verlagert sich zudem allmählich vom ursprünglichen Anwendungsbereich hin zu neuen Einsatzgebieten: von der Identifikation und der Authentifikation hin zu Verhaltensanalysen, Überwachungen und Verfahren zur Betrugsbekämpfung.

Fortschritte bei Computer- und Netztechnologien tragen ebenfalls zur Entstehung gleichsam der zweiten Generation biometrischer Systeme bei. Diese Systeme beruhen auf der Analyse von Verhaltensweisen und psychologischen Merkmalen. Die Systeme werden entweder isoliert eingesetzt oder mit anderen klassischen Systemen zu multimodalen Systemen kombiniert. Und schließlich kommen biometrische Systeme zunehmend im Zusammenhang mit der intelligenten Erfassung von Umgebungen sowie mit den allgegenwärtigen neuen Entwicklungen im Bereich der Computertechnik zur Anwendung.

4.2. Neue Tendenzen bei biometrischen Systemen

Verschiedene biometrische Technologien können als ausgereifte Technologien betrachtet werden, die bei der Rechtsdurchsetzung sowie in der elektronischen Verwaltung (e-Government) und in kommerziellen Systemen zur Anwendung kommen. Zu den betreffenden Verfahren zählen die Erkennung von Fingerabdrücken und Handgeometrien, Iris-Erkennungen und gewisse Formen der Gesichtserkennung. Außerdem werden gewisse biometrische Technologien zur Analyse körperlicher Merkmale entwickelt. Einige dieser Technologien sind grundsätzlich neu; andere Technologien beziehen Impulse aus neuen Verarbeitungskapazitäten.

Typische Elemente dieser neuen Systeme sind die Einbeziehung körperlicher Merkmale zur Kategorisierung/Identifikation von Personen sowie die Möglichkeit der Erfassung der betreffenden Merkmale aus größeren Entfernungen. Die erfassten Daten werden zur Erstellung von Profilen sowie zur Fernüberwachung oder auch zu nochmals komplexeren Aufgaben (beispielsweise zur intelligenten Umgebungsüberwachung) genutzt.

Diese Möglichkeiten haben sich aus der kontinuierlichen Entwicklung von Sensoren ergeben, welche die Erfassung neuer physiologischer Merkmale ermög-

lichen und neue Wege zur Verarbeitung traditioneller biometrischer Daten erschließen.

Zu beachten ist auch die Nutzung der sogenannten weichen biometrischen Daten. Die berücksichtigten sehr allgemeinen Merkmale ermöglichen zwar keine eindeutige Identifikation von Personen, können aber dazu beitragen, die Leistungsfähigkeit anderer Identifikationssysteme zu verbessern.

Ein weiteres wesentliches Merkmal der neuen biometrischen Systeme ist das Potenzial zur Erfassung von Informationen aus größerer Entfernung oder zur Erfassung im Laufe von Bewegungen, ohne dass dazu eine Unterstützung oder Mitwirkung der betreffenden Person erforderlich wäre. Wenngleich diese Technologie noch nicht vollständig ausgereift ist, werden doch gewaltige Anstrengungen insbesondere im Bereich der Rechtsdurchsetzung unternommen.

Außerdem ist die rasche Verbreitung multimodaler Systeme festzustellen, die mehrere biometrische Merkmale gleichzeitig berücksichtigen bzw. die biometrische Daten jeweils mehrfach erfassen oder bestimmen, und die so angepasst werden können, dass die Balance zwischen der Sicherheit und der bequemen Handhabbarkeit biometrischer Systeme verbessert werden kann. Durch den Einsatz dieser Systeme können die FAR reduziert, die Leistungen von Erkennungssystemen verbessert und die Erfassung von Daten umfangreicherer Populationen erleichtert werden, indem mit ergänzenden Datenquellen ein Ausgleich für die mangelnde Universalität einer Quelle biometrischer Daten geschaffen wird.

Biometrische Systeme werden sowohl im öffentlichen als auch im privaten Bereich zunehmend eingesetzt. Im öffentlichen Sektor werden biometrische Daten traditionell in der Rechtsdurchsetzung genutzt. Im Finanzbereich, im Banksektor und im Bereich e-Health sowie beispielsweise im Bildungsbereich, im Einzelhandel und in der Telekommunikationsbranche werden biometrische Daten ebenfalls immer häufiger genutzt. Diese Entwicklung wird durch die neuen Möglichkeiten infolge der Konvergenz bzw. der Zusammenführung bestehender Technologien verstärkt. Ein Beispiel ist etwa der Einsatz von Überwachungskameras zur Erfassung und zur Analyse biometrischer Daten und zur Verarbeitung menschlicher Verhaltenssignaturen.

Angesichts dieser Entwicklungen ist auch festzustellen, dass sich der Schwerpunkt bei der Entwicklung biometrischer Systeme von Identifikationsinstrumenten hin zu „weichen" Erkennungssystemen verlagert (d. h. von der Identifikation hin zur Erkennung von Verhaltensmerkmalen oder von spezifischen Bedürfnissen der betreffenden Personen). Damit werden Nutzungen ermöglicht, die sich von sicherheitstechnischen Anwendungen in großem Maßstab erheblich unterscheiden. Anwendungen im Bereich der persönlichen Sicherheit sowie bei Spielen und im Einzelhandel werden in erheblichem Umfang von einer verbesserten Inter-

aktion zwischen Menschen und Maschinen profitieren, die sich nicht auf die bloße Identifikation oder Kategorisierung von Personen beschränkt.

4.3. Auswirkungen auf die Privatsphäre und auf den Datenschutz

Von Anfang an wurden biometrische Systeme in verschiedenen Bereichen (unter anderem im Hinblick auf den Schutz der Privatsphäre und den Datenschutz) mit erheblichen Vorbehalten betrachtet. Dies hat sich mit Sicherheit auf die soziale Akzeptanz dieser Systeme und auf die Debatte über die Rechtmäßigkeit und die Grenzen einer Nutzung dieser Systeme sowie über die Sicherheitsvorkehrungen und die Garantien zur Abschwächung der bekannten Risiken ausgewirkt.

Ein wesentlicher Vorbehalt gegenüber biometrischen Systemen war schon immer der Schutz der individuellen Rechte. Daran hat sich nichts geändert. Allerdings bieten auch neue Systeme und Weiterentwicklungen bereits verfügbarer Systeme Anlass zu Bedenken. Die Bedenken richten sich unter anderem auf die Möglichkeit der verdeckten Erfassung, Speicherung und Verarbeitung von Daten sowie auf die Erfassung von Material mit äußerst sensiblen Informationen, da diese Nutzungen einen Eingriff in die intimsten persönlichen Bereiche darstellen können.

Von Anfang an wurde die Gefahr einer Zweckentfremdung biometrischer Technologien und Systeme *(„Function Creep")* als problematisch bewertet. Bei traditionellen biometrischen Systemen ist dieses Risiko hinlänglich bekannt, und in diesem Bereich werden auch entsprechende Sicherheitsvorkehrungen getroffen. Es steht jedoch außer Zweifel, dass das umfangreiche technische Potenzial neuer Computersysteme die Gefahr einer schleichenden Ausweitung der Nutzung von Systemen für nicht bestimmungsgemäße Zwecke erhöht.

Verdeckte Techniken ermöglichen die Identifikation von Personen ohne deren Wissen. Dies ist als schwerwiegende Bedrohung der Privatsphäre und als allmählicher Verlust der Kontrolle über personenbezogene Daten zu bewerten. Dies wiederum hat erhebliche Auswirkungen auf die Möglichkeit der betroffenen Personen, von ihrem Recht auf freiwillige Einwilligung Gebrauch zu machen oder auch nur Informationen über die Verarbeitung der Daten zu erhalten. Zudem können manche Systeme Informationen über den Gemütszustand oder über körperliche Merkmale heimlich erfassen und Gesundheitsinformationen offen legen. Dies wäre als unverhältnismäßige Verarbeitung von Daten sowie als Verarbeitung sensibler Daten gemäß Artikel 8 der Richtlinie 95/46/EG zu bewerten.

Angesichts der Tatsache, dass biometrische Technologien keine 100%ige Zuverlässigkeit gewährleisten können, besteht immer auch das Risiko einer fehlerhaften Identifikation. Entscheidungen aufgrund derartiger falsch positiver Befunde können die individuellen Rechte beeinträchtigen. Identitätsdiebstähle unter Ver-

wendung gefälschter oder gestohlener biometrischer Daten können erhebliche Schäden nach sich ziehen. Anders als bei sonstigen Identifikationssystemen können den betreffenden Personen nach einer Fälschung der bereits erfassten Identitätsmerkmale nicht einfach neue Merkmale zugeordnet werden.

Ein wichtiger Aspekt ist auch die Erstellung von Profilen im Zusammenhang mit automatisierten Entscheidungen sowie bei der Vorhersage situationsbezogener Verhaltensweisen oder Vorlieben. Gewisse biometrische Daten können Aufschluss über physische Merkmale einer Person geben. Die betreffenden Informationen können genutzt werden, um die betreffenden Personen ausfindig zu machen oder entsprechende Profile zu erstellen; ebenso können diese Informationen aber auch zur Diskriminierung, Stigmatisierung oder unerwünschten Konfrontation mit nicht erwarteten oder nicht erwünschten Informationen führen.

4.4. Spezifische biometrische Systeme und Technologien

4.4.1. Die Erkennung von Venenstrukturen und kombinierte Verwendungen

Zwei wesentliche Technologien beruhen auf der Erkennung von Venenstrukturen: Sowohl Handflächen als auch Finger werden insbesondere in Japan inzwischen häufig anhand der Venenstrukturen identifiziert.

Technisch gesehen beruht die Erkennung von Venenstrukturen auf einem Template der mit einer Infrarotkamera erfassten Venen. Die Erfassung erfolgt, wenn eine Person einen Finger oder eine Hand vor eine Infrarot-Lichtquelle bringt. Das aufgenommene Bild wird so verarbeitet, dass das jeweilige Gefäßnetz sichtbar wird. Der wesentliche Vorteil dieser Technologie liegt darin, dass die betroffene Person bei der Erfassung der biometrischen Merkmale keine physische Probe hinterlassen muss.[13] (Die Identifikation erfolgt berührungslos.) In diesem Zusammenhang ist auch zu beachten, dass biometrische Daten gegenwärtig nur schwer ohne die Einwilligung der betroffenen Personen erfasst werden können. Da der Blutfluss analysiert werden kann, ist mit diesem Verfahren schließlich auch festzustellen, ob die von einem System untersuchte Person lebt.

Die Erkennung von Venenstrukturen kann auch genutzt werden, um den virtuellen Zugang zu Anwendungen oder den physischen Zugang zu Räumlichkeiten zu regeln. Häufig sehen die Hersteller die Möglichkeit vor, die betreffenden Sensoren auch in andere Produkte einzubauen (insbesondere im Zusammenhang mit Bankgeschäften).

[13] Einige Autoren sind der Ansicht, dass Technologien im Zusammenhang mit der Erkennung von Venenstrukturen Rückschlüsse auf Erkrankungen wie z. B. Bluthochdruck oder Gefäßanomalien zulassen könnten.

Im Zusammenhang mit der Nutzung von Systemen zur Erkennung von Venenstrukturen können sich die folgenden Risiken für den Datenschutz ergeben:

- Zuverlässigkeit: Die Leistungsfähigkeit von Venenstruktur-Analysen ist hoch. Daher gilt diese Technologie als realistische Alternative zur Analyse von Fingerabdrücken. Außerdem zeichnet sich die Erkennung von Venenstrukturen durch eine niedrige FER (*Failure to Enrol Rate* = Erfassungsfehlerquote) aus, da sich die Venen im Gegensatz zu Fingern oder Händen nicht verändern. Trotzdem wurden diese Technologien bislang noch nicht an einem größeren Bevölkerungsregister erprobt. (In Japan wird die ermittelte Struktur mit dem jeweils auf einem Magnetstreifen gespeicherten Template verglichen.) Manchmal kann diese Technologie auch durch klimatische Bedingungen beeinträchtigt werden, die sich auf das Gefäßsystem auswirken (Wärme, Druck usw.).

- Auswirkung: Systeme zur Untersuchung der Venenstrukturen haben hinsichtlich des Datenschutzes nur begrenzte Relevanz, da die betreffenden biometrischen Daten nicht einfach abgegriffen werden können, und da sich die Analyse von Venenstrukturen gegenwärtig auf Anwendungen im privaten Bereich beschränkt.

- Einwilligung und Transparenz: Da Daten zu Venenstrukturen ausschließlich unter Einsatz von Lichtquellen und Kameras in der Nähe des Infrarotspektrums erfasst werden können, ist davon auszugehen, dass der jeweils betroffenen Person die Verarbeitung der Daten bewusst ist und dass die betroffene Person ihre Einwilligung zum Ausdruck gebracht hat, indem sie ihren Finger oder ihre Hand auf das Lesegerät gelegt hat. Wie bei allen biometrischen Systemen ist jedoch auch bei diesen Systemen diese Annahme unter gewissen Umständen mit Vorbehalten zu bewerten (beispielsweise wenn die betroffene Person bei dem für die Verarbeitung Verantwortlichen beschäftigt ist).

- Sonstige Zwecke bzw. Verarbeitungszwecke: Gegenwärtig sind mit Strukturdaten nur geringe Risiken hinsichtlich einer Nutzung für anderweitige Zwecke verbunden. Dieses Risiko kann sich jedoch erhöhen, wenn diese Form der Verarbeitung weitere Verbreitung findet und Betrugsversuche durch Spoofing (Täuschung) erleichtert werden.

- Verknüpfbarkeit: Venenstrukturdaten enthalten keine Informationen, die mit anderen Daten verknüpft werden könnten (außer mit Venenstrukturdaten aus anderen Verarbeitungsprozessen).

- Nachverfolgung/Erstellung von Profilen: Das Risiko einer Nachverfolgung/Profilerstellung aufgrund von Venenstrukturdaten ist begrenzt, solange dieser Typ biometrischer Daten nicht allgemein verbreitet ist und beispielsweise in einer zentralen Zahlungskarten-Datenbank gespeichert wird.

- Verarbeitung sensibler Daten: Die einzigen sensiblen Daten, die aus Venenstrukturdaten abzuleiten wären, betreffen die Gesundheit der jeweiligen Personen. Eine entsprechende formale Bewertung ist bislang jedoch noch nicht erfolgt.

- Widerruflichkeit: Venenstrukturen dürften auch über längere Zeiträume sehr stabil sein. Diese Annahme ist jedoch noch empirisch zu belegen. (Systeme zur Analyse von Venenstrukturen werden noch nicht so lange eingesetzt, dass bestätigte Ergebnisse verfügbar wären.) Daher sind Venenstrukturen wohl als unwiderruflich zu behandeln.

- Schutz gegen Spoofing: Umfangreiche Untersuchungen zu Spoofing-Angriffen im Zusammenhang mit Venenstrukturdaten wurden bislang noch nicht durchgeführt. In letzter Zeit wurde jedoch in einer Studie festgestellt, dass mit Geräten zur Erkennung von Handflächen-Venenstrukturen Spoofing-Angriffe möglich sind.[14] Die wesentliche Schwierigkeit beim Spoofing in Verbindung mit Venenstrukturdaten besteht darin, die benötigten biometrischen Daten überhaupt zu erfassen.

4.4.2. Fingerabdrücke und kombinierte Nutzungen

Systeme zur Erkennung von Fingerabdrücken zählen zu den ältesten und am häufigsten untersuchten und eingesetzten biometrischen Systemen. Die Nutzung von Fingerabdrücken ist in der Rechtsdurchsetzung seit über 100 Jahren sowohl für Überprüfungen als auch für Identifikationszwecke üblich. Die Identifikation aufgrund von Fingerabdrücken beruht auf der Tatsache, dass jeder Mensch Fingerabdrücke mit individuellen messbaren Merkmalen hinterlässt, die mit bereits erfassten Abdrücken verglichen werden können.

Die Erfassung setzt voraus, dass die betreffende Person physisch anwesend ist und dass – je nach beabsichtigtem Verwendungszweck – gut geschulte Mitarbeiter verfügbar sind, um eine hinreichend gute Qualität der Daten gewährleisten zu können. Die Bedeutung der Abnahme der Fingerabdrücke ist nicht zu unterschätzen. Die Zuverlässigkeit eines Abgleichs hängt von der Bildqualität und vom jeweiligen Abbildungsverfahren ab. Je nach Verfahren werden Abdrücke nur von einem oder zwei Fingern oder aber auch von allen zehn Fingern genommen. Die Abdrücke können flach aufgesetzt oder abgerollt werden. Je nach Systemkönnen Fingerabdrücke zur bloßen Überprüfung (1:1) oder zur Identifikation und zum Abgleich mit gesicherten Spuren (1:n) verwendet werden. Einigen Studien zufolge können von einem Teil der Bevölkerung jedoch aus unterschiedlichen Gründen keine Abdrücke genommen werden. Dies ist insoweit problematisch, als

[14] Siehe http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

insbesondere bei umfangreichen Systemen geeignete Alternativverfahren verfügbar sein müssen, damit niemandem seine individuellen Rechte vorenthalten werden.

Auch wenn die Erfassung von Fingerabdrücken nicht als Verfahren zu betrachten ist, das die Privatsphäre erheblich beeinträchtigen würde, kann dies doch so empfunden werden. Infolge der verbreiteten Nutzung bei der Rechtsdurchsetzung wird die Abnahme von Fingerabdrücken häufig mit dem negativen Image einer Behandlung als Tatverdächtiger assoziiert.

Fingerabdrücke sind durch individuelle Merkmale gekennzeichnet, die zur Verifikation/Identifikation genutzt werden können. Im Allgemeinen sind jedoch weiterhin gründliche detaillierte Analysen erforderlich. Die Entwicklung neuer Verfahren (d. h. der Einsatz hoch auflösender Scanner) wird die Nutzung anderer Merkmale ermöglichen. Auch die Techniken zur Identifikation anhand umfangreicher Datenbanken wurden weiterentwickelt.

Die modernsten Systeme sind sogenannte AFIS (*Automated Fingerprint Identification Systems* = automatisierte daktyloskopische Identifizierungssysteme). Diese Systeme werden bei der Rechtsdurchsetzung eingesetzt. Sie ermöglichen den Austausch von Daten und die Durchsuchung unterschiedlicher länderübergreifender Bestände. Der Austausch von Daten ist allerdings je nach Standort, Formaten und Qualität mit unterschiedlichen Problemen verbunden.

AFIS auf EU-Ebene beispielsweise sind Eurodac und das Visa-Informationssystem. Mit einem Bestand von ca. 70 Mio. Fingerabdrücken dürften diese Systeme zu den weltweit größten Datenbanken zählen. Im Zusammenhang mit der Nutzung umfangreicher Datenbanken hat die Datenschutzgruppe bereits in früheren Stellungnahmen auf Probleme hinsichtlich der Gewährleistung der erforderlichen Verhältnismäßigkeit hingewiesen. Zu klären sind insbesondere die Zuverlässigkeit der Ergebnisse (falsch positive und falsch negative Ergebnisse) sowie die wirksame Kontrolle des Zugangs zu diesen Datenbanken und die Verwendung der Fingerabdrücke von Kindern und alten Menschen.

In biometrischen Systemen, die auf erfassten Fingerabdrücken beruhen, werden häufig Templates eingesetzt. Die Anbieter betrachten diese Systeme gewöhnlich als Instrumente zum Schutz der betreffenden Personen. Je nach System bzw. je nach dem zur Erzeugung der Templates eingesetzten Algorithmus kann die Gefahr einer Verknüpfung der Templates mit anderen Fingerabdruck-Datenbanken bestehen, die die Identifikation einzelner Personen ermöglichen würde.

Problematisch ist auch, dass mit Systemen zur Erzeugung von Fingerabdrücken unter Verwendung künstlicher Finger oder künstlicher Fingerabdrücke Identitätsdiebstähle begangen werden könnten. Mit verschiedenen Ansätzen wird

versucht, der entsprechenden Gefährdung dieser Systeme zu begegnen (etwa durch Erkennung in Echtzeit oder durch den Einsatz von Systemen, bei denen jeweils mehrere Finger berücksichtigt werden, durch die Beaufsichtigung der Erfassung und der Identifikation und durch die Verifikation durch geeignete Personen).

Die datenschutzrechtlichen Bedenken hinsichtlich der Verwendung von Fingerabdrücken lassen sich wie folgt zusammenfassen:

- Zuverlässigkeit: Ungeachtet ihrer letztlich hohen Zuverlässigkeit sind Fingerabdruck-Analysen wegen der verwendeten Informationen (schlechte Qualität des Datenmaterials oder inkonsistente Erfassungsverfahren) sowie wegen der Darstellung der Fingerabdrücke (ausgewählte Merkmale oder Qualität der Analysealgorithmen) angreifbar. Infolge der genannten Faktoren kann es zu falsch positiven oder falsch negativen Ergebnissen kommen.

- Auswirkung: Die Unumkehrbarkeit des Prozesses kann die Möglichkeit beeinträchtigen, dass die betroffenen Personen ihre Rechte wahrnehmen oder dass Entscheidungen rückgängig gemacht werden, die aufgrund falscher Identifikationen getroffen wurden. Das Vertrauen auf die Zuverlässigkeit von Fingerabdruck-Analysen kann die Korrektur von Fehlern erschweren und weitreichende Folgen für die betroffenen Personen nach sich ziehen. Dies muss bei der Bewertung der Verhältnismäßigkeit einer Verarbeitung gemessen an der jeweils aufgrund der bewerteten Fingerabdrücke zu treffenden konkreten Entscheidung berücksichtigt werden. Außerdem ist darauf hinzuweisen, dass mangelnde Sicherheitsvorkehrungen Identitätsdiebstähle begünstigen können, die mit nachdrücklichen Auswirkungen auf die betroffenen Personen verbunden sein können.

- Verknüpfbarkeit: Fingerabdrücke können insoweit missbraucht werden, als die entsprechenden Informationen mit anderen Datenbanken verknüpft werden können. Diese Möglichkeit der Verknüpfung mit anderen Datenbanken kann Verwendungen zur Folge haben, die mit dem ursprünglichen Zweck nicht in Einklang stehen. Mit gewissen Techniken (z. B. mit Systemen zur Konvertierung biometrischer Daten oder durch biometrische Verschlüsselung) kann dieses Risiko verringert werden.

- Verarbeitung sensibler Daten: Einigen Studien zufolge können abgenommene Fingerabdrücke Aufschluss über die ethnische Herkunft der betroffenen Personen geben.[15]

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm und http://www.crime-scene-investigator.net/fingerprintpatterns.html.

- Weitere Zwecke bzw. Verarbeitungszwecke: Die zentrale Speicherung von Daten – insbesondere in großen Datenbanken – verringert Risiken im Hinblick auf die Sicherheit und die Verknüpfbarkeit der Daten sowie hinsichtlich der Gefahr eines Function Creep. Das Fehlen geeigneter Garantien kann dazu führen, dass Fingerabdrücke zu anderen Zwecken genutzt werden als ursprünglich vorgesehen.

- Einwilligung und Transparenz: Die Einwilligung ist ein zentraler Aspekt bei der Verwendung von Fingerabdrücken außerhalb des Bereichs der Rechtsdurchsetzung. Fingerabdrücke können von latenten Abdrücken und sogar von Fotografien leicht auch ohne Wissen der betroffenen Personen kopiert werden. Ebenfalls problematisch im Zusammenhang mit dem Aspekt der Einwilligung sind die Einwilligung eines Kindes und die Rolle der Eltern (z. B. bei der Abnahme von Fingerabdrücken in Schulen) sowie die Gültigkeit einer Einwilligung zur Abgabe von Fingerabdrücken im Zusammenhang mit Beschäftigungsverhältnissen.

- Widerruflichkeit: Fingerabdrücke ändern sich nicht und sind insoweit als äußerst stabile Daten zu bewerten. Entsprechend sollten diese Daten als unwiderruflich betrachtet werden. Unter gewissen Bedingungen ist allerdings vorstellbar, dass auch Fingerabdruck-Templates widerrufen werden.

- Schutz gegen Spoofing: Fingerabdrücke können leicht erfasst werden, weil Menschen zahllose Abdrücke hinterlassen. Außerdem können bei vielen Systemen und Sensoren falsche Fingerabdrücke verwendet werden, insbesondere wenn diese Systeme keine spezifischen Mechanismen zum Schutz gegen Spoofing enthalten. Der Erfolg eines Angriffs hängt weitgehend vom jeweiligen Sensortyp (optisch, kapazitiv usw.) und vom Material ab, das der Angreifer verwendet.

Beispiel:
Ein Krankenhaus verwendet Fingerabdrücke in einer zentralen Datenbank zur Authentifikation von Patienten, um bei Strahlenbehandlungen sicherzustellen, dass der betreffende Patient die richtige Behandlung erhält. Fingerabdrücke werden gegenüber Venenstrukturen bevorzugt, weil Strahlenbehandlungen das Gefäßsystem beeinträchtigen. Außerdem wird eine zentrale Datenbank verwendet, weil angesichts des Gesundheitszustands der Patienten (Alter und Pathologie) mit hoher Wahrscheinlichkeit damit zu rechnen wäre, dass Namensschilder verloren gingen und der Zugang zur betreffenden Behandlung verhindert würde. Vor diesem Hintergrund könnte die Verwendung von Fingerabdrücken eine angemessene Lösung sein.

4.4.3. Gesichtserkennung und kombinierte Verwendungen

Ähnlich wie Fingerabdrücke werden auch biometrische Daten aufgrund von Gesichtserkennungen seit Jahren in erheblichem Umfang genutzt. Neuerdings werden Gesichter jedoch nicht nur zur Identifikation, sondern auch zur Feststellung physiologischer und psychologischer Merkmale (ethnische Herkunft, Gefühle, Wohlbefinden usw.) analysiert. Aus der Tatsache, dass die betreffenden Daten auch aus einem Bild ermittelt werden können und dass Fotos auch aus größerer Entfernung ohne Wissen der betroffenen Personen aufgenommen werden können, wird deutlich, welche datenschutzrechtlichen Probleme mit diesen Technologien verbunden sein können.

Die Bedeutung der Gesichtserkennung als Mittel zur Identifikation von Personen und zur Verifikation von Sachverhalten wurde auch im Bereich der Rechtsdurchsetzung sowie von anderen öffentlichen Stellen und von privaten Einrichtungen erkannt. Seit vielen Jahren werden Fotos in Reisepässen, Führerscheinen, Ausweisen und Fahndungsfotos verwendet. Vielfach werden Fotos auf Ansteckschilder oder auf sonstige unternehmensinterne Ausweise gedruckt. Die betreffenden Bilder werden gewöhnlich unter kontrollierten Lichtverhältnissen aufgenommen und beschränken sich auf eine Profilansicht der jeweiligen Person. Ein Satz derart kontrollierter Bilder bietet sich als Grundlage für die automatisierte Verarbeitung und die Erkennung von Personen an. Die entsprechenden Möglichkeiten wurden inzwischen weiterentwickelt, und die verfügbare Technologie ist inzwischen derart ausgereift, dass eine Identifikation anhand von Bildern möglich ist, die mit den unterschiedlichsten Kameras, aus ganz verschiedenen Blickwinkeln und unter unterschiedlichen Beleuchtungsbedingungen aufgenommen wurden. Zahlreiche Bilder sind im Internet öffentlich zugänglich (z. B. Fotos, die in soziale Netze oder in sonstige öffentliche Alben hochgeladen wurden). Die betreffenden Risiken beschränken sich nicht auf traditionelle Bilder, da Funktionen zur Gesichtserkennung inzwischen erfolgreich auch in Echtzeit-Video-Feeds genutzt werden können. Wenn für die Verarbeitung Verantwortliche in vorhandene Systeme neue Verarbeitungsfunktionen aufnehmen (z. B. durch die Einbindung einer Funktion zur Gesichtserkennung in ein System zur Videoüberwachung), muss ihnen bewusst sein, dass sie damit eine Änderung der vorgesehenen Zwecke des ursprünglichen Systems bewirken. Entsprechend müssen sie die Auswirkungen dieser Änderung auf den Schutz der Privatsphäre neu bewerten.

Systeme zur Gesichtserkennung gehen mit folgenden Risiken in Bezug auf den Datenschutz einher:

- Zuverlässigkeit: Wenn die Qualität der Bilder nicht garantiert werden kann, besteht die Gefahr einer Beeinträchtigung der Zuverlässigkeit. Wird ein Gesicht nicht vollständig erfasst (weil es durch Haare oder einen Hut verdeckt ist), können ein Abgleich und eine Kategorisierung natürlich nur mit einer

hohen Fehlerquote erfolgen. Unterschiedliche Haltungen und Lichtverhältnisse sind weitere große Herausforderungen für eine zuverlässige Gesichtserkennung.

- Auswirkung: Die spezifischen Auswirkungen auf den Datenschutz eines Systems zur Gesichtserkennung hängen vom jeweiligen Zweck und von den betreffenden Umständen ab. Ein System, das die Besucher einer Sehenswürdigkeit nach demografischen Gesichtspunkten kategorisiert, aber nicht über eine Speicherfunktion verfügt, wirkt sich hinsichtlich des Datenschutzes anders aus als ein System, das im Bereich der Rechtsdurchsetzung zur verstärkten Überwachung potenzieller Unruhestifter einsetzt wird.

- Einwilligung und Transparenz: Ein Risiko für den Datenschutz, das bei vielen anderen Systemen zur Verarbeitung biometrischer Daten nicht gegeben ist, besteht darin, dass Fotos aus zahlreichen Blickwinkeln und unter den unterschiedlichsten Bedingungen ohne Wissen der betroffenen Personen aufgenommen und verarbeitet werden können. In Stellungnahme 15/2011 zum Begriff der Einwilligung betont die Datenschutzgruppe, dass nur eine „informierte" Einwilligung Rechtsgrundlage für die Verarbeitung von Daten sein kann. Wenn die betroffene Person keine Kenntnis von der Verarbeitung von Fotos zum Zweck der Gesichtserkennung hat, ist diese Rechtsgrundlage nicht gegeben. Und selbst wenn die betroffene Person weiß, dass eine Kamera eingesetzt wird, ist vielleicht nicht erkennbar, ob die Gesichtserkennungmit einer laufenden Überwachungskamera oder anhand statischer Fotos erfolgt.

- Sonstige Zwecke bzw. Verarbeitungszwecke: Einmal erfasst, können digitale Bilder leicht weitergegeben oder kopiert und dann in anderen Systemen umfassender bearbeitet werden als ursprünglich vorgesehen. Dabei ist unerheblich, ob die Bilder rechtmäßig oder widerrechtlich aufgenommen wurden. Dies wird z. B. im Bereich der sozialen Medien deutlich, wo Nutzer ihre persönlichen Fotos hochladen, um die Fotos ihrer Familie, ihren Freunden und ihren Kollegen zu zeigen. Sobald in einem sozialen Medium Bilder verfügbar sind, können sie durch die betreffende Plattform zu vielfältigen Zwecken verwendet werden. Manche dieser Verwendungszwecke werden unter Umständen erst nachträglich eingeführt (d. h. nach dem Aufnehmen und/oder dem Hochladen der betreffenden Bilder).

- Verknüpfbarkeit: Viele Online-Dienste bieten Nutzern die Möglichkeit, Bilder hochzuladen, die sie mit dem jeweiligen Nutzerprofil verknüpfen können. Systeme zur Gesichtserkennung können eingesetzt werden, um die Profile unterschiedlicher Online-Dienste (über das jeweilige Profilbild) miteinander zu verknüpfen. Ebenso können jedoch auch Verknüpfungen zwischen Online-Medien und Offline-Datenbeständen hergestellt werden. Es ist durchaus möglich, eine Person in Echtzeit anhand eines Fotos zu identifizieren, indem diese

öffentlichen Profilbilder durchsucht werden. Auch Fremddienste können Profilbilder und sonstige öffentlich zugängliche Bilder durchsuchen, um riesige Bilddatenbanken zu erstellen. Die Bilder in diesen Datenbanken können dann Identitäten in der realen Welt zugeordnet werden.

- Nachverfolgung/Erstellung von Profilen: Außerdem könnte ein Identifikationssystem genutzt werden, um die Identität einer abgebildeten Person in der realen Welt zu ermitteln. Ein System zur Gesichtserkennung in einem Einkaufszentrum oder einem ähnlichen öffentlichen Bereich könnte eingesetzt werden, um Wege und Gewohnheiten einzelner Kunden zu verfolgen. Aufgrund der ermittelten Informationen könnten Warteschlangen gesteuert oder Produkte präsentiert werden, um das Einkaufserlebnis attraktiver zu gestalten. Mit der Möglichkeit der Verfolgung oder Lokalisierung einzelner Personen geht die Möglichkeit einher, Profile zu erstellen und gezielte Werbung anzubringen oder sonstige spezifische Dienste anzubieten.

- Verarbeitung sensibler Daten: Wie bereits erläutert, könnten durch die Verarbeitung biometrischer Daten sensible Daten ermittelt werden. Insbesondere könnten Bilder erfasst werden, die Aufschluss über die rassische oder ethnische Herkunft oder vielleicht auch den Gesundheitszustand geben könnten.

- Widerruflichkeit: Eine Person kann ihr Gesicht leicht verändern (beispielsweise durch einen Bart, eine Brille oder einen Hut). Diese Veränderungen können hinreichend sein, um Systeme zur Gesichtserkennung zu täuschen, insbesondere wenn diese Systeme in einer nicht kontrollierten Umgebung eingesetzt werden. Die wesentlichen Merkmale eines Gesichts sind jedoch unveränderlich, und die Systeme können die Erkennungsgenauigkeit verbessern, indem sie mehrere unterschiedliche „Gesichter“ einer Person erfassen und miteinander verknüpfen.

- Schutz gegen Spoofing: Viele Systeme zur Gesichtserkennung können leicht Gegenstand von Spoofing-Angriffen werden. Die Hersteller bemühen sich um entsprechende Schutzmechanismen beispielsweise unter Nutzung von 3D-Bildern oder von Videoaufnahmen. Die meisten in öffentlichen Anwendungen eingesetzten Systeme sind jedoch nicht mit derartigen Schutzmechanismen ausgerüstet.

Beispiel:
Als extremes Beispiel wäre etwa ein Einkaufszentrum der Zukunft vorstellbar, in dem eine Videoüberwachung Personen erkennt, Bewegungen automatisch verfolgt und anhand der erfassten Gesichter emotionelle Reaktionen wie z. B. ein Lächeln oder Anzeichen von Verärgerung feststellen kann. Das System könnte regelmäßige Kunden erkennen, die ins Parkhaus einfahren

und diese Kunden zu bevorzugten Parkplätzen lotsen. Wenn die Kunden das Einkaufszentrum betreten, könnte das System aufgrund der erkannten Kleidung je nach Angebot, früherem Einkaufsverhalten und zuvor definierten Indikatoren unterschiedliche Ladengeschäfte vorschlagen. Ebenso könnte in den Schaufenstern kundenspezifische Werbung platziert oder der Zugang zu bestimmten Läden, Restaurants und sonstigen Orten verweigert werden. Potenzielle Autodiebe könnten identifiziert und verfolgt werden, noch bevor sie sich an einem Auto zu schaffen machen. Wenn nötig, könnten telematisch geführte Luftfahrzeuge (Drohnen) mit Kameras und Sensoren Verdächtige verfolgen, bis der betreffende Verdacht entweder bestätigt oder als unbegründet bewertet wurde. In Kleidungsstücken verborgene Objekte (Messer oder Diebesgut) könnten erkannt werden. Diese Technologie würde nicht nur auf neuen biometrischen Systemen beruhen, sondern würde Informationen kombinieren und verarbeiten, die bereits in den Datenbeständen weiterer Systeme erfasst sind.

Eine ähnliche Anwendung wurde mit dem Projekt INDECT *(Intelligent information system supporting observation, searching and detection for security of citizens in urban environment)* entwickelt, in dem Technologien kombiniert werden, mit denen potenzielle terroristische und kriminelle Handlungen bereits im Vorfeld bekämpft werden sollen. Die Datenschutzgruppe weist nachdrücklich darauf hin, dass eine derartige Nutzung biometrischer Daten eine angemessene Rechtsgrundlage und strenge Prüfungen der Notwendigkeit und der Verhältnismäßigkeit der entsprechenden Maßnahmen voraussetzen würde.

4.4.4. Sprecherverifikation und kombinierte Verwendungen

Systeme zur Stimmerkennung („Sprecherverifikation“) werden nicht nur zur biometrischen Identifikation genutzt. Verhältnismäßig häufig werden auch spezifische Merkmale von Stimmstrukturen identifiziert, um die Sprecher entsprechend zu kategorisieren. Eine entsprechende Anwendung wäre beispielsweise die Analyse der Reaktionen einer Person während eines Telefonats, um Stressmuster und Unregelmäßigkeiten im Sprechverhalten zu erkennen und aus den erkannten Informationen auf betrügerisches Verhalten schließen zu können.

Hersteller berichten, dass durch die Einrichtung einer derartigen Technologie bei Finanzdienstleistern Betrugsfälle zuverlässiger erkannt und berechtigte Forderungen rascher erfüllt werden konnten.

In Verbindung mit einem Kategorisierungssystem stellen sich die Risiken im Hinblick auf den Datenschutz etwas anders dar als bei biometrischen Identifika-

tionssystemen. Bei diesen Systemen dürfte eine Erfassung und langfristige Speicherung biometrischer Templates nicht erforderlich sein. Wenn jedoch ein Telefonat aufgezeichnet wird (was etwa bei Finanzinstituten häufig der Fall ist), müssen geeignete Kontrollen eingerichtet sein, um die Sicherheit dieser Daten zu gewährleisten.

- Zuverlässigkeit: Datenschutzrechtlich problematisch sind bei derartigen Systemen die Erkennungsquoten, insbesondere im Hinblick auf falsch positive und falsch negative Ergebnisse, d. h. hinsichtlich des Anteils der Personen, die fälschlicherweise als Betrüger identifiziert bzw. die nicht als Betrüger erkannt werden. Bei einem Kategorisierungssystem sind höhere Fehlerquoten vielleicht eher annehmbar als bei Verifikations- oder Identifikationssystemen. Es müssen jedoch geeignete Prozesse zur zeitnahen Handhabung der Fälle eingerichtet sein, in denen möglicherweise eine unzutreffende Kategorisierung vorgenommen wurde.

- Einwilligung und Transparenz: Bei derartigen Technologien kommen jedoch auch für den Datenschutz vorteilhafte Ansätze in Betracht, etwa indem darauf geachtet wird, dass Anrufe auf ihre Eignung für eine entsprechende Analyse geprüft werden oder indem die betroffenen Personen über den durchgeführten Prozess unterrichtet werden. In einer Fallstudie wurden einzelne Personen, die Englisch nicht als Hauptsprache verwendeten oder deren Hörvermögen oder kognitive Fähigkeiten beeinträchtigt waren oder die keinen Zugang zu einem Telefon hatten, als für das betreffende System zur Sprecherverifikation ungeeignet bewertet. Den betreffenden Personen war freigestellt, eine telefonische Mitteilung abzulehnen und ihr Anliegen in herkömmlicher Weise vorzubringen. Den Personen, die nicht bereit oder nicht in der Lage waren, sich der Erkennung durch ein entsprechendes System zu unterziehen, sollten jedoch keine Nachteile entstehen.

- Weitere Zwecke bzw. Verarbeitungszwecke: Bei dieser Technologie werden in den meisten Fällen spezielle Infrastrukturänderungen benötigt, da der öffentliche und der private Sektor ihre jeweiligen IT-Infrastrukturen so konsolidieren müssen, dass Technologien wie z. B. Voice over IP (VoIP) genutzt werden können. Gleichzeitig werden Spracherkennungstechnologien leichter einzubinden sein, ohne dass datenschutzrechtliche Verpflichtungen des für die Verarbeitung Verantwortlichen angemessen berücksichtigt würden.

- Widerruflichkeit: Auch wenn jemand seine Stimme bewusst verstellen kann, sind die zugrunde liegenden Sprechmuster doch verhältnismäßig stabil und können entsprechend hilfreich sein, um eine Person zuverlässig zu identifizieren. Dies gilt insbesondere, wenn die betreffende Person nicht über die Erkennung unterrichtet wurde (und sich daher auch nicht veranlasst sieht, ihre Stimme zu verstellen).

- Schutz gegen Spoofing: Sprachaufzeichnungen können genutzt werden, um Stimmerkennungssysteme durch Spoofing anzugreifen. Verfahren zum Schutz gegen Spoofing beinhalten Fragen und Antworten zum jeweiligen Hintergrund. (Beispielsweise wird etwa nach dem aktuellen Datum gefragt oder aufgefordert, seltene Wörter nachzusprechen.)

4.4.5. DNA-Analysen

Die Weiterentwicklung von Geräten zur Sequenzierung und zum Abgleich von DNA-Proben sowie die Verfügbarkeit kostengünstiger Geräte zur Durchführung von DNA-Analysen machen die Überprüfung gewisser Annahmen des bereits vorliegenden Arbeitspapiers über Biometrie (WP 80) erforderlich.

Eine der wesentlichen Änderungen bei Technologien zur Erstellung von DNA-Profilen ist die Beschleunigung der Prozesse zur Sequenzierung und zum Abgleich von DNA-Proben. Die in den letzten Jahren aufgrund von Forschungen im akademischen Bereich sowie infolge der Entwicklungstätigkeit von Biotechnologieunternehmen erzielten Fortschritte haben dazu geführt, dass sich der Zeitaufwand für die Erzeugung eines DNA-Profils von ursprünglich einigen Tagen auf wenige Stunden und schließlich auf weniger als eine Stunde reduziert hat.

Die Entstehung eines Marktes für DNA-bezogene Online-Dienste gefährdet das Recht auf den Schutz personenbezogener Daten. Dies gilt insbesondere dann, wenn die betreffenden Dienstedie Übertragung biometrischer Proben und Daten zwischen mehreren Ländern (einschließlich Ländern außerhalb der EU) erfordern, sowie wenn mehrere Auftragsverarbeiter beteiligt sind und bei der Verarbeitung genetischer Daten oder gesundheitsbezogener Daten geeignete Garantien fehlen.

Sehr wahrscheinlich wird es in der näheren Zukunft möglich sein, Profile aufgrund von DNA-Proben in Echtzeit (oder nahezu in Echtzeit) auch mit tragbaren Geräten zu erstellen. Damit wird die Entwicklung biometrischer Identifikations- und Authentifikationssysteme auf der Grundlage von DNA-Proben beginnen, die sich gegenüber Systemen zur Authentifikation aufgrund von Fingerabdrücken, Stimmen und Gesichtern durch eine größere Zuverlässigkeit auszeichnen.

Weiterentwicklungen bei der Erstellung von DNA-Profilen sind auf das zunehmende Interesse von Verwaltungseinrichtungen, Richtern und Rechtsdurchsetzungsbehörden am Einsatz biotechnologischer Verfahren in der Kriminalistik zurückzuführen. Wegen der Zuverlässigkeit des Abgleichs von DNA-Proben sowie aufgrund der Tatsache, dass DNA-Proben ohne Wissen der betroffenen Person kontrolliert werden können, haben mehrere Mitgliedstaaten im Laufe der Zeit verschiedene Initiativen ins Leben gerufen, um aufgrund von an Tatorten gesicherten Spuren zentrale Datenbanken mit DNA-Proben und mit DNA-Profilen verurteilter Personen aufzubauen.

Im Mai 2005 haben sieben EU-Mitgliedstaaten den Prümer Vertrag unterzeichnet, um die Zusammenarbeit bei grenzübergreifenden strafrechtlichen Untersuchungen und Gerichtsverfahren durch den Austausch geeigneter Informationen zu verbessern. Der Vertrag schafft insoweit eine neue Grundlage für die Zusammenarbeit, als er den Unterzeichnern bestimmte Rechte für den Zugang zu nationalen DNA-Datenbanken einräumt. Das betreffende Datenmaterial beschränkt sich allerdings auf die Verwendung für repressive Maßnahmen (Verfolgung von Straftaten) sowie auf die Nutzung von Fingerabdrücken, personenbezogenen und nicht personenbezogenen Daten und auf Fahrzeugregistrierungsdaten. Seit damals haben viele Mitgliedstaaten den Vertrag unterzeichnet, und die wesentlichen Inhalte des Vertrags wurden in den Beschluss 2008/615/JI des Rates übernommen.

Nach Maßgabe dieses Rechtsrahmens werden mehrere EU-Mitgliedstaaten in näherer Zukunft über eine funktionsfähige nationale Datenbank mit DNA-Profilen verurteilter Personen sowie mit DNA-Daten aufgrund von Spurensicherungen an Tatorten verfügen. Dies gibt Anlass zu gewissen Bedenken hinsichtlich dieser besonderen Form der Datenverarbeitung.

Einer der wesentlichen Aspekte im Zusammenhang mit der Einrichtung von DNA-Datenbanken ist die Tatsache, dass die aus DNA-Proben (Loci) abgeleiteten genetischen Daten Aufschluss über den Gesundheitszustand der betroffenen Personen sowie über Dispositionen für Krankheiten oder die ethnische Herkunft geben könnten (zwar nicht bereits während der Erfassung, jedenfalls aber zu einem späteren Zeitpunkt). Insoweit ist die Erstellung von DNA-Datenbanken als erhebliches Risiko für die Achtung der Menschenwürde und für die Wahrung der Grundrechte zu bewerten. Dieses Risiko wurde in der Entschließung 2009/C 296/01 des Rates berücksichtigt. Mit konkreten Vorschriften sollen DNA-Analysen auf Chromosomenbereiche ohne genetische Aussagekraft beschränkt werden. Dazu wird eine spezielle Gruppe von DNA-Markern verwendet, die nach aktuellem Kenntnisstand keine Informationen über spezifische Erbmerkmale enthalten. (Diese Gruppe von Markern wird auch als „ESS“ (*European Standard Set* = Europäischer Standardsatz) bezeichnet.

Da bestimmte Marker in einer nationalen DNA-Datenbank jedoch zu einem späteren Zeitpunkt Aufschluss über gewisse Erbmerkmale oder über sonstige sensible Informationen geben könnten, müssen Entwicklungen in der Biologie mit kontinuierlicher Aufmerksamkeit verfolgt werden. Gegebenenfalls müssten gewisse in der betreffenden Datenbank enthaltene Informationen sogar umgehend gelöscht werden. Und da diese DNA-Datenbanken Profile verurteilter Personen erfassen, sollten statistische Analysen der vorhandenen Daten streng eingeschränkt werden, um die Erstellung von Profilen aufgrund des Geschlechts oder der rassischen Herkunft zu verhindern.

In Bezug auf DNA-Datenbanken für polizeiliche oder strafrechtliche Zwecke hat der Europäische Gerichtshof für Menschenrechte festgestellt, dass zwischen der Verarbeitung personenbezogener Daten und der Verarbeitung genetischer Profile von Tatverdächtigen und von verurteilten Personen klar zu unterscheiden ist.[16]

Außerdem besteht die Gefahr, dass DNA-Analysen zur Identifikation von Familienmitgliedern oder Verwandten im Zusammenhang mit nicht aufgeklärten Straftaten oder mit verurteilten Personen herangezogen werden könnten, weil die in der Datenbank gespeicherten DNA-Profile aufgrund von Teilgruppen der erfassten Marker oder mithilfe von Platzhaltern durchsucht werden könnten. Angesichts dieser Möglichkeit sind die Auswirkungen der Ableitung von Informationen aus familienbezogenen Suchabfragen zu prüfen.

Außerdem ist darauf hinzuweisen, dass mit der Nutzung von Genom-Datensätzen auch im Bereich der Forschung bestimmte Risiken verbunden sind. Die Datenschutzgruppe ist der Ansicht, dass der Zugang zu Proben und Datensätzen streng auf den Bereich der Forschung beschränkt und nur für Forschungszwecke gestattet sein sollte. Darüber hinaus muss geklärt werden, unter welchen Bedingungen Forschungsergebnisse (unter Berücksichtigung des jeweils persönlichen Anspruchs auf entsprechende Unterrichtung) gegenüber Einzelpersonen offen gelegt oder in medizinische Unterlagen eingebunden werden können.

Im Zusammenhang mit der Nutzung von Systemen zur Analyse von DNA-Proben können sich die folgenden Risiken für den Datenschutz ergeben:

- Zuverlässigkeit: Auch wenn die Zuverlässigkeit von DNA-Analysen sehr hoch ist, sollte berücksichtigt werden, dass die Qualität der Ergebnisse von der Anzahl der analysierten Marker (Loci) abhängt. Die eingesetzten Testsysteme sollten die größtmögliche Zuverlässigkeit gewährleisten.

- Auswirkung: Die Durchführung von DNA-Analysen kann als äußerst schwerer Eingriff in die Privatsphäre betrachtet werden. Genetische Daten können sensible Informationen enthalten. Anhand statistischer Analysen der vorhandenen Daten können Profile erstellt werden, die Diskriminierungen der betroffenen Personen zur Folge haben können.

- Sonstige Zwecke bzw. Verarbeitungszwecke: Mit neuen Technologien können inzwischen zunehmend größere Datenbestände ausgetauscht werden. Daher muss klar sein, wer Zugang zu den Informationen in einer DNA-Datenbank erhält. Familienbezogene Suchabfragen und Abfragen nach rassischer Herkunft

[16] EGMR, Urteil vom 4.12.2008, S. und Marper/Vereinigtes Königreich (Anträge Nrn. 30562/04 und 30566/04), insbesondere Randnummer 125.

können als neue Technologien betrachtet werden, die dem ursprünglichen Zweck der Verarbeitung der gegenwärtig verfügbaren DNA-Datenbanken zuwiderlaufen.

- Einwilligung und Transparenz: Inzwischen werden Dienste zur Durchführung von DNA-Analysen anhand biologischer Proben angeboten, die auf dem Postweg eingesandt werden (beispielsweise Speichelproben), und bei denen die Ergebnisse im Internet bereitgestellt werden. Unzureichende Identitätsprüfungen könnten dazu führen, dass Einzelpersonen oder sonstige Rechtssubjekte Proben anderer Personen übermitteln und dadurch sensible personenbezogene Daten Dritter in Erfahrung bringen.

- Verknüpfbarkeit: Angesichts des Umfangs und der Vielfalt der Informationen, die aus der Sequenzierung von DNA-Proben abgeleitet werden können, besteht bei DNA-Analysen ein hohes Missbrauchsrisiko, da die gewonnenen Daten leicht mit anderen Datenbanken verknüpft werden können, um dann personenbezogene Profile zu erstellen. Familienbezogene Suchabfragen ermöglichen die Herstellung von Verknüpfungen mit Verwandten.

- Verarbeitung sensibler Daten: DNA-Proben können Informationen über den Gesundheitszustand sowie über die Disposition für bestimmte Krankheiten oder die ethnische Herkunft einer Person enthalten. Bei der Auswahl der relevanten Loci ist daher von äußerster Bedeutung, dass der Grundsatz der Datenminimierung berücksichtigt wird. DNA-Informationen können aus vielen Proben auch über einen längeren Zeitraum gewonnen werden. Daher sollte sichergestellt werden, dass der Zugang zu den Proben streng auf befugte Benutzer und auf zugelassene Verwendungen beschränkt wird.

- Widerruflichkeit: DNA-Informationen sind nicht widerruflich.

- Schutz gegen Spoofing: DNA-Daten sind für Spoofing-Angriffe naturgemäß äußerst schwierig einzusetzen. Häufig ist es jedoch nicht schwer, sich DNA-Proben (z. B. Haare) ohne Wissen der betroffenen Person zu beschaffen.

4.4.6. Biometrische Identifikation von Unterschriften

Die Erfassung biometrischer Daten zu Unterschriften ist ein Beispiel für neue Nutzungen herkömmlicher biometrischer Technologien. Biometrische Daten zu Unterschriften werden durch biometrische Verfahren ermittelt, bei denen das Verhalten einer Person aufgrund der Dynamik der jeweiligen Handschrift bewertet wird. Herkömmliche Systeme zur Erkennung von Unterschriften beruhen auf der Analyse statischer oder geometrischer Merkmale des jeweiligen Unterschriftsbildes. (Die Analysen erfolgen also aufgrund der Darstellung einer Unterschrift.) Biometrische Verfahren zur Erkennung von Unterschriften hingegen analysieren

die dynamischen Merkmale einer Unterschrift (d. h., wie die Unterschrift vorgenommen wurde). Entsprechend heißt es häufig, diese Verfahren analysieren „dynamische Unterschriften".

Typische dynamische Merkmale, die von biometrischen Systemen zur Erkennung von Unterschriften (z. B. von einem Digitalisierungstablett) ermittelt werden, sind der Schreibdruck, der Schreibwinkel, die Geschwindigkeit und die Beschleunigung der Stiftführung, die Bildung der Buchstaben und die Strichrichtung sowie eine Reihe weiterer individueller dynamischer Merkmale. Welche dieser Merkmale berücksichtigt werden, ist von Anbieter zu Anbieter unterschiedlich. Gewöhnlich werden diese Merkmale mithilfe druckempfindlicher Geräte festgestellt. Einige Systeme zur Erkennung von Unterschriften können Verifikationen durchführen, indem sie Analysen statischer Merkmale (d. h. des Schriftbildes) mit Analysen dynamischer Merkmale (Schreibdruck, Schreibwinkel, Schreibgeschwindigkeit usw.) verknüpfen.

Im Zusammenhang mit der Nutzung von Systemen zur biometrischen Erkennung von Unterschriften können sich die folgenden Risiken für den Datenschutz ergeben:

- Zuverlässigkeit: Unterschriften werden nicht immer in der gleichen Weise geleistet. Entsprechend können die Erfassung und die Verifikation von Identitäten problematisch sein.

- Auswirkung: Auf Verhaltensmerkmalen beruhende biometrische Daten wie beispielsweise eine Unterschrift können sich im Laufe der Zeit ändern, oder die betreffenden Personen können ihr Verhalten bewusst ändern. Auch physiologische Ursachen können Änderungen einer Unterschrift zur Folge haben und einer erfolgreichen Verifikation entgegenstehen. Entsprechend müssen alternative Verfahren verfügbar sein, um die Identität von Personen zu verifizieren.

- Schutz gegen Spoofing: Das Schriftbild einer herkömmlichen Unterschrift kann leicht nachgebildet und (von einer entsprechend erfahrenen Person) nachgeahmt, fotokopiert oder mit einer Grafik-Software erfasst werden. Sicherer ist die Verifikation anhand einer dynamischen Unterschrift, weil im Verifikationsprozess auch die komplexeren und für die Handschrift einer Person ganz typischen dynamischen Merkmale geprüft werden.

5. Allgemeine Leitlinien, sektorbezogene Empfehlungen und technische und organisatorische Maßnahmen

Der Einsatz eines biometrischen Systems hängt vom Zusammenwirken mehrerer Akteure ab:

- Hersteller: Entwicklung und Prüfung biometrischer Sensoren und Feststellung der Leistungsfähigkeit biometrischer Technologien;
- integrierte Dienstleister: Entwicklung des Endproduktes, das schließlich an die Kunden verkauft wird; Auswahl der biometrischen Technologie und teilweise Festlegung der Zwecke, für die das jeweilige System eingesetzt wird; (dabei werden die jeweiligen Kunden berücksichtigt;)
- Wiederverkäufer: Vermarktung des Endproduktes bei den Kunden: Aufklärung der Kunden über die Leistungsfähigkeit und die Risiken der Systeme sowie möglicherweise über den maßgeblichen Rechtsrahmen;
- mit der Einrichtung der Systeme befasste Fachkräfte: Einrichtung des Produktes in den Räumlichkeiten der Kunden;
- Kunden: Entscheidung für den Erwerb eines biometrischen Systems; Festlegung des Zwecks und der Mittel zur Verarbeitung der Daten; insoweit sind die Kunden als für die Verarbeitung Verantwortliche zu betrachten;
- betroffene Personen: Bereitstellung biometrischer Daten zur Verwendung im System.

Einige Akteure übernehmen eine oder mehrere der oben beschriebenen Rollen. Mit jeder Rolle ist eine eigene Zuständigkeit verbunden, um eine mit der Wahrung der Privatsphäre zu vereinbarende Verwendung biometrischer Systeme zu gewährleisten. Eine mit der Einrichtung eines Systems beauftragte Person beispielsweise kann keine vom jeweiligen integrierten Dienstleister entwickelte Sicherheitsfunktion aktivieren.

5.1. Allgemeine Grundsätze

Die Sicherheit biometrischer Daten sollte ein wesentlicher Aspekt sein, weil biometrische Daten nicht widerruflich sind. Entsprechend gefährdet die Verletzung des Schutzes biometrischer Daten auch die weitere sichere Verwendung des Datenmaterials für Identifikationsprozesse und beeinträchtigt das Recht der betroffenen Personen auf den Schutz ihrer Daten. Dabei ist zu beachten, dass die Auswirkungen einer Beeinträchtigung der Sicherheit nicht mehr rückgängig gemacht werden können.

Die entsprechenden Risiken erhöhen sich mit der Anzahl der eingesetzten Anwendungen zur Verarbeitung dieser Daten. (Dies gilt insbesondere für das Risiko einer Verletzung des Schutzes personenbezogener Daten und eines Function Creep.) Je mehr biometrische Daten verwendet werden, desto wahrscheinlicher wird auch ein Diebstahl biometrischer Daten.

Die Datenschutzgruppe stellt gegenwärtig einen Trend dahin gehend fest, Fernzugriffe auf biometrische Systeme zuzulassen (beispielsweise über Internet-

Schnittstellen). Mit diesem Trend ist eine Reihe neuer Sicherheitsprobleme verbunden, die in der IT-Branche durchaus bekannt sind. Bereits in einer frühen Phase der Systementwicklung sollten daher IT-Fachkräfte, die über angemessene Erfahrungen mit der technischen Sicherheit der einzusetzenden Systeme verfügen, mit der Einrichtung eines geeigneten Systems beauftragt werden.

Die Datenschutzgruppe empfiehlt einen weitreichenden technischen Schutz bei der Verarbeitung biometrischer Daten. Dabei sollten die modernsten technischen Mittel zum Einsatz kommen. In diesem Zusammenhang sollten bestehende Industrienormen für den Schutz von Systemen berücksichtigt werden, in denen biometrische Informationen verarbeitet werden.

5.2. Eingebauter Datenschutz (Privacy by Design)

Die Einrichtung von Funktionen zur Gewährleistung des Datenschutzes bereits bei der Systemauslegung (*Privacy by Design* = „eingebauter Datenschutz“) bedeutet, dass die Wahrung der Privatsphäre proaktiv bereits bei der Entwicklung der eigentlichen Technologie berücksichtigt wird.

Das Konzept des „eingebauten Datenschutzes“ betrifft bei biometrischen Systemen die gesamte Wertschöpfungskette:

– Bei der Entwicklung neuer Technologien und Sensoren sollten Hersteller die Grundsätze des eingebauten Datenschutzes berücksichtigen. Nach diesen Grundsätzen sind unter anderem Rohdaten automatisch zu löschen, nachdem ein Template berechnet wurde. Außerdem sind biometrische Daten grundsätzlich verschlüsselt zu speichern. (Dies gilt sowohl für die Speicherung in einer zentralen Datenbank als auch für die Speicherung auf einer Smart Card.) Zudem sollten sich die Hersteller auf die Entwicklung biometrischer Technologien konzentrieren, die schon durch ihre Auslegung einen besseren Datenschutz gewährleisten;

– auch integrierte Dienstleister und Wiederverkäufer sollten die Grundsätze des eingebauten Datenschutzes bei der Beschreibung des zu vermarktenden Endproduktes berücksichtigen, indem sie datenschutzgerechtere Technologien auswählen und geeignete Garantien für das Endprodukt vorsehen (beispielsweise durch eine dezentrale Gestaltung der Datenbank);

– die Kunden (als potenziell für die Verarbeitung Verantwortliche) sollten die Grundsätze des eingebauten Datenschutzes berücksichtigen, wenn sie ein bestimmtes biometrisches System bestellen oder die technischen Merkmale eines Systems spezifizieren. In diesem Zusammenhang sollten Hersteller und integrierte Dienstleister in ihren Produkten eine gewisse Flexibilität vorsehen,

um den Grundsätzen der Verhältnismäßigkeit, der Zweckbindung, der Datenminimierung und der Sicherheit Rechnung zu tragen.

Diese Grundsätze wurden bei einigen biometrischen Geräten bereits erfolgreich in der Praxis berücksichtigt. Um unbefugten Zugriffen auf biometrische Daten entgegenzuwirken, haben manche Hersteller in einem bestimmten biometrischen Lesegerät Verschlüsselungsfunktionen sowie Schaltungen vorgesehen, die das Auslesen und Manipulieren von Daten verhindern.

Die Datenschutzgruppe empfiehlt, bei der Auslegung biometrischer Systeme formale „Entwicklungslebenszyklen" mit folgenden Schritten zu berücksichtigen:

1. Spezifikation von Anforderungen gemäß einer Risikoanalyse und/oder gemäß einer speziellen PIA (*Privacy Impact Assessment* = Datenschutz-Folgenabschätzung);
2. Beschreibungen und Begründungen dahin gehend, wie durch die jeweilige Auslegung die bestehenden Anforderungen erfüllt werden;
3. Validierung mithilfe von Funktions- und Sicherheitstests;
4. Verifikation der Konformität der endgültigen Gestaltung mit dem geltenden Rechtsrahmen.

Die Datenschutzgruppe befürwortet die Definition von Zertifizierungsplänen, welche die Umsetzung des Grundsatzes des eingebauten Datenschutzes gewährleisten und die Aufklärung der für die Verarbeitung Verantwortlichen über die datenschutzrechtlichen Risiken biometrischer Systeme verbessern könnten.

5.3. Rahmen der Datenschutz-Folgenabschätzung

5.3.1. Allgemeine Grundsätze

Die PIA (*Privacy Impact Assessment* = Datenschutz-Folgenabschätzung) ist ein Prozess, bei dem ein Rechtssubjekt die mit der Verarbeitung personenbezogener Daten verbundenen Risiken bewertet und zusätzliche Maßnahmen zur Verringerung dieser Risiken definiert. Bezüglich der RFID-Technologie beispielsweise hat die Datenschutzgruppe festgestellt, dass das Rechtssubjekt, das die betreffende Anwendung beschreibt, auch für die Durchführung der PIA zuständig ist. Dieses Rechtssubjekt kann sowohl der für die Verarbeitung Verantwortliche als auch der Anbieter sein, der die jeweilige RFID-Anwendung konzipiert.

Wegen der mit der Nutzung biometrischer Daten verbundenen spezifischen Risiken empfiehlt die Arbeitsgruppe, dass derjenige, der den Zweck eines Geräts und die jeweils eingesetzten Mittel beschreibt (d. h. der Hersteller, der integrierte

Dienstleister oder der Endkunde), im Zusammenhang mit der Auslegung eines Systems zur Verarbeitung des betreffenden Datentyps auch Datenschutz-Folgenabschätzungen durchführt und dass diese Folgenabschätzungen als wesentlicher Bestandteil der Systemauslegung behandelt werden.

Bei der PIA sollten die folgenden Aspekte berücksichtigt werden:

- Art der erfassten Informationen,
- Zweck der Informationserfassung,
- Zuverlässigkeit des Systems (in der Annahme, dass ein positives bzw. negatives Ergebnis einer biometrischen Prüfung wesentliche Entscheidungen für die betroffene Person zur Folge haben kann),
- Rechtsgrundlage und rechtliche Konformität; ist eine Einwilligung vorgeschrieben?
- Zugang zum jeweiligen Gerät und interne und externe Weitergabe von Informationen durch den für die Verarbeitung Verantwortlichen, wobei personenbezogene Daten durch geeignete Sicherheitstechniken und -verfahren gegen unbefugte Zugriffe zu schützen sind,
- bereits getroffene und die Privatsphäre weniger beeinträchtigende Maßnahmen; ist im Hinblick auf das jeweilige biometrische Gerät bereits ein alternatives Verfahren denkbar (beispielsweise die Vorlage eines Ausweises)?
- Entscheidungen bezüglich der Aufbewahrungszeit und der Löschung von Daten; welche Zeiträume wurden vorgesehen? Gelten für sämtliche Daten die gleichen Aufbewahrungszeiten? Besteht ein automatisierter Mechanismus oder ein geeigneter Alternativprozess?
- Rechte der betroffenen Personen.

Die Datenschutz-Folgenabschätzung sollte sich nicht nur auf die Identifikation der bestehenden Risiken konzentrieren. Vielmehr sollten auch geeignete datenschutzrechtliche Maßnahmen vorgesehen werden; außerdem sollte erläutert werden, wie der für die Verarbeitung Verantwortliche zu geeigneten Lösungen gelangt ist, mit denen die im vorherigen Schritt ermittelten datenschutzrechtlichen Risiken verringert werden können.

Wenn der Hersteller oder der integrierte Dienstleister die PIA durchgeführt hat, kann die Einführung des jeweiligen biometrischen Systems eine weitere Bewertung erfordern, bei der die besonderen Bedingungen des für die Verarbeitung Verantwortlichen zu berücksichtigen sind. Wenn ein biometrisches System beispielsweise in das Informationssystem eines Kunden integriert wird, sollte der Kunde eine weitere PIA durchführen, bei der die sicherheitstechnischen Maßnahmen und Verfahren im eigenen IT-System geprüft werden.

5.3.2. Die Spezifität biometrischer Daten

Biometrische Daten erfordern insoweit besondere Aufmerksamkeit, als anhand dieser Daten einzelne Personen aufgrund ihrer individuellen verhaltensbezogenen oder physiologischen Merkmale zweifelsfrei identifiziert werden können.

Daher sollte mit PIAs möglichst bewertet werden, wie die drei folgenden Risiken durch das zu analysierende System vermieden oder zumindest in erheblichem Umfang eingeschränkt werden können:

Das erste Risiko ist die Gefahr des Identitätsbetrugs, insbesondere in Verbindung mit Identifikations- und Authentifikationverfahren. Das betreffende biometrische System darf nicht durch Spoofing-Angriffe zu täuschen sein und muss gewährleisten, dass die Person, die einen Abgleich vornehmen möchte, tatsächlich mit der im System registrierten Person identisch ist. Diese Bedrohung erscheint bei biometrischen Daten, die ohne Wissen der betroffenen Person nicht erfasst werden können (d. h. beispielsweise in Bezug auf Venenstrukturen), weniger einsichtig.[17] Bei Geräten zur Verarbeitung von Fingerabdrücken oder zur Gesichtserkennung ist dies jedoch ein wesentlicher Aspekt. Fingerabdrücke werden nämlich überall hinterlassen, einfach indem jemand einen Gegenstand berührt. Und Gesichter können auf einem Foto erfasst werden, ohne dass der betreffenden Person dies bewusst ist.

Das zweite Risiko besteht in einer Modifikation des ursprünglichen Zwecks entweder durch den für die Verarbeitung Verantwortlichen selbst oder durch einen Dritten (einschließlich der Rechtsdurchsetzungsbehörden. Diese allgemeine Bedrohung im Hinblick auf personenbezogene Daten wird bei biometrischen Daten zur zentralen Bedrohung. Die Hersteller sollten alle verfügbaren Sicherheitsmaßnahmen treffen, um jegliche unangemessene Nutzung der Daten zu verhindern und um sicherzustellen, dass für eine Verarbeitung nicht mehr benötigte Daten umgehend gelöscht werden.

Ebenso wie andere Daten können auch rechtmäßig verarbeitete oder gespeicherte biometrische Daten bzw. die Quellen biometrischer Daten von dem für die Verarbeitung Verantwortlichen nicht für neue oder anderweitige Zwecke verarbeitet oder erfasst werden, wenn keine neue rechtmäßige Begründung für den neuen Verarbeitungszwecke gegeben ist.

Das dritte Risiko ist die Verletzung des Schutzes personenbezogener Daten; dieses Risiko erfordert je nach Art der gefährdeten biometrischen Daten besondere Maß-

[17] Angesichts der zunehmenden Verbreitung dieser Technologie gilt dies auch dann, wenn schwer abzusehen ist, wie sich Angriffe auf Systeme zur Verarbeitung von Venenstrukturen in den folgenden Jahren gestalten könnten.

nahmen. Wenn bei einem System, das biometrische Daten mithilfe eines Algorithmus erzeugt, der ein biometrisches Template in einen bestimmten Code konvertiert, entweder die eigentlichen biometrischen Daten oder die betreffenden Algorithmen gestohlen oder gefährdet werden, müssen die betreffenden Daten oder Algorithmen ersetzt werden. Wenn eine Verletzung des Schutzes personenbezogener Daten mit dem Verlust direkt identifizierter biometrischer Daten einhergeht, die in engem Zusammenhang mit der Quelle dieser biometrischen Daten stehen (z. B. Fingerabdrücke oder Porträtbilder), muss die betreffende Person umfassend unterrichtet werden, damit sie sich verteidigen kann, wenn diese gefährdeten biometrischen Daten als Beweismittel gegen diese Person verwendet werden.

5.4. Technische und organisatorische Maßnahmen

Wegen der Art des Datenmaterials erfordert die Verarbeitung biometrischer Daten spezielle technische und organisatorische Maßnahmen und Vorkehrungen, um Beeinträchtigungen der betroffenen Personen infolge einer Verletzung des Schutzes personenbezogener Daten zu vermeiden. Dies gilt insbesondere angesichts der Gefahr eines rechtswidrigen Verhaltens nach der unbefugten „Rekonstruktion" eines biometrischen Merkmals anhand eines Referenz-Template oder aufgrund der Verknüpfung mit anderen Datenbanken sowie für die Gefahr einer nicht bestimmungsgemäßen Nutzung ohne Wissen der betroffenen Personen und/oder die Gefahr, dass gewisse biometrische Daten genutzt werden könnten, um Informationen über die rassische Herkunft oder über den Gesundheitszustand bestimmter Personen zu erhalten.

5.4.1. Technische Maßnahmen

- *Verwendung biometrischer Templates*

Biometrische Daten sollten nach Möglichkeit grundsätzlich als biometrische Templates gespeichert werden.

Die Templates sollten in einer für das jeweilige biometrische System spezifischen Form extrahiert werden, und eine Verwendung in ähnlichen Systemen durch die jeweils für die Verarbeitung Verantwortlichen muss ausgeschlossen werden, um sicherzustellen, dass die betreffenden Personen nur in den biometrischen Systemen identifiziert werden können, bei denen eine entsprechende Rechtsgrundlage gegeben ist.

- *Speicherung auf einem persönlichen Gerät im Vergleich zu einer zentralen Speicherung*

Wenn die Verarbeitung biometrischer Daten zulässig ist, sollten personenbezogene biometrische Informationen vorzugsweise nicht zentral gespeichert werden.

Insbesondere im Zusammenhang mit Verifikationen hält die Datenschutzgruppe für empfehlenswert, dass biometrische Systeme biometrische Daten aus verschlüsselten Templates auf Medien lesen, die sich ausschließlich im Besitz der betroffenen Personen befinden (z. B. Smart Cards oder ähnliche Speichermedien). Die biometrischen Merkmale der betroffenen Personen können mit den auf der Karte und/oder den sonstigen Medien gespeicherten Templates verglichen werden. Dazu sollten Standard-Vergleichsverfahren zum Einsatz kommen, die ebenfalls unmittelbar auf der betreffenden Karte und/oder dem betreffenden Medium definiert sind. Auf diese Weise sollte die Erstellung einer Datenbank mit biometrischen Informationen im Allgemeinen nach Möglichkeit vermieden werden. Wenn die Karte und/oder das Speichermedium verloren gehen oder verlegt werden, besteht die Gefahr eines Missbrauchs der biometrischen Informationen nach gegenwärtigem Kenntnisstand nur in eingeschränktem Umfang. Um das Risiko eines Identitätsdiebstahls zu verringern, sollten auf den entsprechenden Systemen identifikationsrelevante Daten zur betreffenden Person ebenfalls nur in eingeschränktem Umfang gespeichert werden.

Für spezifische Zwecke sowie wenn objektive Erfordernisse gegeben sind, kommt jedoch auch eine zentrale Datenbank mit biometrischen Informationen und/oder Templates in Betracht. Das eingesetzte biometrische System und die ausgewählten Sicherheitsmaßnahmen sollten die genannten Risiken begrenzen und gewährleisten, dass die Weiterverwendung der betreffenden biometrischen Daten für sonstige Zwecke ausgeschlossen ist oder zumindest zurückverfolgt werden kann. Um das unbefugte Lesen, Kopieren, Modifizieren oder Löschen biometrischer Daten zu verhindern, sollten Mechanismen auf der Grundlage von Verschlüsselungstechnologien eingesetzt werden.

Wenn die biometrischen Daten auf einem System gespeichert werden, das der physischen Kontrolle der betroffenen Person unterliegt, sollte ein spezifischer Verschlüsselungscode als wirksame Maßnahme vorgesehen werden, um diese Daten vor unbefugten Zugriffen zu schützen. Außerdem bieten diese dezentralen Systeme schon aufgrund ihrer Auslegung einen besseren Schutz der biometrischen Daten, da die betroffene Person die physische Kontrolle über ihre biometrischen Daten behält und da kein gemeinsames Ziel existiert, auf das sich Angriffe richten könnten.

Die Datenschutzgruppe betont ferner, dass der Begriff einer zentralen Datenbank eine Vielzahl technischer Anwendungen von der Speicherung in einem Lesegerät bis hin zu Datenbanken auf einem Netz-Host beinhaltet.

- *Möglichkeit der Erneuerung und des Widerrufs*

Da die Quelle biometrischer Daten nicht geändert werden kann, müssen biometrische Systeme zur Verknüpfung von Identitäten so ausgelegt sein, dass der Prozess der Erfassung sowie die Verarbeitung biometrischer Daten die Möglichkeit bieten, aus der gleichen Quelle mehrere voneinander unabhängige biometrische

Templates zu extrahieren, damit die Daten beispielsweise bei einer Verletzung des Schutzes personenbezogener Daten oder infolge einer technischen Weiterentwicklung ersetzt werden können.

Biometrische Systeme sollten so ausgelegt werden, dass die Verknüpfung mit einer Identität aufgehoben werden kann, um die Verknüpfung zu erneuern oder endgültig zu löschen (z. B. wenn die erteilte Einwilligung widerrufen wurde).[18]

• *Verschlüsselung*
Aus Sicherheitsgründen sollten angemessene Maßnahmen zum Schutz der durch das jeweilige biometrische System gespeicherten und verarbeiteten Daten getroffen werden. Daher sind biometrische Informationen grundsätzlich verschlüsselt zu speichern. Um sicherzustellen, dass die Codes nur für die entsprechend befugten Personen zugänglich sind, muss ein geeigneter Rahmen für die Verwaltung der Codes definiert werden.

Angesichts der verbreiteten Nutzung öffentlicher und privater Datenbanken mit biometrischen Informationen sowie im Bestreben, die Interoperabilität biometrischer Systeme zu verbessern, sollte die Nutzung spezifischer Technologien oder Datenformate angestrebt werden, bei denen eine Verknüpfung biometrischer Datenbanken und die ungeprüfte Offenlegung von Daten nicht möglich sind.

• *Schutz gegen Spoofing:*
Um die Zuverlässigkeit eines biometrischen Systems zu erhalten und Fälle von Identitätsbetrug auszuschließen, müssen die Hersteller Systeme einrichten, mit denen festgestellt werden kann, ob die biometrischen Daten echt sind und ob die Verknüpfung mit einer natürlichen Person noch besteht. Bei Systemen zur Gesichtserkennung kann entscheidend sein, dass die Systeme echte Gesichter zuverlässig beispielsweise von Bildern unterscheiden, die ein Betrüger vor sein eigenes Gesicht hält.

• *Biometrischer Ver- und Entschlüsselung*
Die biometrische Verschlüsselung ist ein Verfahren, bei dem biometrische Merkmale in die Prozesse zur Verschlüsselung und zur Entschlüsselung von Daten einbezogen werden. Dazu wird im Allgemeinen ein Auszug der verfügbaren biometrischen Daten als Code zur Verschlüsselung eines Identifikators verwendet, der zur Nutzung des betreffenden Dienstes benötigt wird.

---

[18] Ein Beispiel ist etwa die TURBINE-Technologie zum Schutz biometrischer Templates durch fotografische Umwandlung von Fingerabdruckdaten in einen nicht mehr konvertierbaren Code, der Bit für Bit verglichen werden kann. Es wird davon ausgegangen, dass sich die biometrischen Proben und die Original-Templates aus den umgewandelten biometrischen Daten nicht mehr wiederherstellen lassen. Um das Vertrauen der Nutzer auf die Technologie zusätzlich zu erhöhen, wird auch dieser Code widerruflich definiert. Entsprechend kann gegebenenfalls ein neuer unabhängiger Code erzeugt werden, um biometrische Identitäten neu zu definieren (siehe auch http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf).

Dieser Ansatz hat viele Vorteile.[19] Bei diesen Systemen werden der Identifikator und die biometrischen Daten nicht in ihrer ursprünglichen Form gespeichert. Nur das Ergebnis der Identifikatorprüfung wird biometrisch verschlüsselt im System abgelegt. Zudem können die personenbezogenen Daten insoweit widerrufen werden, als die Möglichkeit besteht, einen weiteren Identifikator zu erzeugen und biometrisch zu verschlüsseln. Und schließlich sind diese Systeme sicherer und benutzerfreundlicher, da sich die Benutzer bei diesen Systemen keine langen und komplexen Kennwörter merken müssen.

Die Verschlüsselung ist jedoch insoweit problematisch, als Verschlüsselungen und Entschlüsselungen unveränderliche Codes voraussetzen und biometrische Daten unterschiedliche Strukturen ergeben, durch die sich die jeweils generierten Codes ändern können. Daher muss das System in der Lage sein, auch bei leicht abweichenden biometrischen Daten dieselben Codes zu erzeugen, ohne die Quote falsch positiver Ergebnisse zu erhöhen.

Die Datenschutzgruppe ist sich einig dahin gehend, dass die biometrische Verschlüsselung ein vielversprechendes Forschungsgebiet darstellt und so weit ausgereift ist, dass die politische Diskussion auch in der breiten Öffentlichkeit erfolgen kann und dass Prototypen entwickelt und praktische Anwendungen in Erwägung gezogen werden können.

• *Automatisierte Mechanismen zur Löschung von Daten*

Um zu verhindern, dass biometrische Informationen länger als für die ursprünglich vorgesehenen Zwecke bzw. für die anschließende Verarbeitung erforderlich gespeichert werden, sind geeignete automatisierte Mechanismen zur Löschung der Daten auch dann einzurichten, wenn die Aufbewahrungszeit rechtmäßig verlängert werden kann. Dadurch ist die umgehende Löschung personenbezogener Daten sicherzustellen, die für den Einsatz des jeweiligen biometrischen Systems nicht mehr benötigt werden.

Wenn das Lesegerät über einen integrierten Speicher verfügt, können die Hersteller biometrische Templates auch auf einem flüchtigen Speicher erfassen, bei dem garantiert ist, dass die Daten gelöscht werden, sobald die Verbindung zum Lesegerät getrennt wird. Damit ist gewährleistet, dass bei einem Verkauf oder bei einer Deinstallation des Lesegeräts keine biometrische Datenbank mehr gespeichert ist. Die automatische Löschung der Daten kann auch durch Schaltungen bewirkt werden, die ein Auslesen der gespeicherten Daten verhindern (Anti-Pulling-Switches), indem das betreffende Datenmaterial bei einem Diebstahlversuch sofort gelöscht wird.

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

- *Umfangreiche biometrische Datenbanken und Datenbanken mit „schwachen Verknüpfungen“*

In manchen Ländern werden umfangreiche biometrische Datenbanken hauptsächlich für zwei Zwecke eingesetzt: zur Unterstützung strafrechtlicher Untersuchungen und um sicherzustellen, dass Ausweispapiere (Reisepässe, Ausweise, Führerscheine) ordnungsgemäß erfasst werden. In Datenbanken für strafrechtliche Untersuchungen werden im Allgemeinen Informationen über Straftäter und über verdächtige Personen verwaltet. Diese Datenbanken müssen so gestaltet sein, dass Personen anhand der jeweiligen biometrischen Daten identifiziert werden können. Datenbanken zur Bekämpfung von Identitätsbetrug enthalten dagegen biometrische Daten der gesamten Bevölkerung und sollten ausschließlich genutzt werden, um einzelne Personen zu authentifizieren (beispielsweise, wenn jemand seine Ausweispapiere verloren hat oder wenn der Sicherheits-Chip des Reisepasses mit den entsprechenden biometrischen Daten zerstört wurde).

Wenn eine zentrale Datenbank genutzt wird, um gegen Fälle von Identitätsbetrug vorzugehen, ist die Datenschutzgruppe der Ansicht, dass geeignete technische Maßnahmen vorgesehen werden müssen, um jegliche nicht mit dem ursprünglichen Zweck zu vereinbarende Nutzung der Datenbank zu verhindern. Erstens erfordert der Grundsatz der Datenminimierung, dass ausschließlich die zur Authentifikation einer Person erforderlichen Daten erfasst werden. Beispielsweise wird davon ausgegangen, dass der Vergleich der Abdrücke von zwei Fingern hinreichende Informationen für die Authentifikation einer Person ergibt.

Außerdem können für die Verarbeitung Verantwortliche Datenbanken mit „schwachen Verknüpfungen“ nutzen, bei denen die Identität einer Person nicht mit einem einzelnen Satz biometrischer Daten verknüpft ist, sondern vielmehr einer ganzen Gruppe biometrischer Daten zugeordnet wird. Die Gestaltung dieser Datenbank sollte die Authentifikation einer Person mit sehr hoher Wahrscheinlichkeit gewährleisten (d. h. z. B. mit einer Wahrscheinlichkeit von 99,9 %, die hinreichend sein müsste, um Betrüger abzuschrecken). Außerdem müsste durch die Gestaltung der Datenbank sichergestellt sein, dass die Datenbank nicht für Identifikationen genutzt werden kann (weil nämlich jeder einzelne Satz biometrischer Daten zahlreichen Personen zugeordnet werden kann).

Die Datenschutzgruppe befürwortet den Einsatz dieser Systeme, wenn umfangreiche biometrische Datenbanken genutzt werden, um gegen Fälle von Identitätsbetrug vorzugehen.

Beispiel: Technische Maßnahmen für Authentifikationssysteme
Biometrische Daten haben jeweils eine individuelle Quelle, die lebenslang mit der betroffenen Person verbunden sein kann. Wenn diese Quelle von einem Authentifikationssystem als Grundlage genutzt wird, ist zu beachten,

dass diese Quelle nicht geändert werden kann. Bei sonstigen Authentifikationstechnologien, bei denen die Nutzer in der Regel ein bestimmtes Merkmal „wissen“ oder „besitzen“ müssen (beispielsweise eine Benutzerkennung oder ein Kennwort), kann das definierte Ausweiskriterium immer geändert werden. Daher müssen beim Einsatz biometrischer Authentifikationssysteme spezielle Garantien vorgesehen werden, um die Verknüpfung der biometrischen Daten mit sonstigen personenbezogenen Daten zu verhindern:

– Template-Daten sollten nicht zentral gespeichert werden, da die Sicherheit der Speicherung biometrischer Daten von wesentlicher Bedeutung für die Gesamtsicherheit des jeweiligen biometrischen Systems ist. Vorzugsweise sollte eine verteilte Speicherung (z. B. auf Smart Cards) erfolgen. In diesem Fall befinden sich sowohl die Quelle der Daten als auch das Template im Besitz der betroffenen Person.
– Die Speicherung und Übertragung biometrischer Daten müssen derart geschützt erfolgen, dass die Daten nicht durch geeignete Verschlüsselungstechnologien abgefangen, unbefugt offen gelegt oder geändert werden können.
– Bestimmte Typen biometrischer Daten sind nicht geheim (z. B. Gesichter). Diese Daten können nach einer Verletzung des Schutzes personenbezogener Daten sowie nach einer Offenlegung oder einem Missbrauch nicht gesperrt, blockiert oder geändert werden. Daher sollte die Authentifikation mit weiteren Merkmalen kombiniert werden, bei denen Sperrungen oder Änderungen vorgenommen werden können.

5.4.2. Organisatorische Maßnahmen

Um den erforderlichen Datenschutz zu gewährleisten, müssen organisatorische Maßnahmen geplant und durchgeführt werden. Der für die Verarbeitung Verantwortliche muss beispielsweise ein klares Verfahren entwickeln, mit dem festgestellt werden kann, wer auf die im System gespeicherten Informationen zugreifen kann. Außerdem muss in diesem Verfahren geregelt sein, ob die Zugriffe unbeschränkt oder nur auf gewisse Informationen erfolgen können sowie gegebenenfalls, aus welchen Gründen Einschränkungen vorgenommen wurden. Sämtliche Eingriffe müssen rückverfolgbar sein.

Die Datenschutzgruppe stellt fest, dass die Auslagerung an externe Dienstleister sogar in Verbindung mit der Bearbeitung von Visaanträgen möglich ist (siehe Abschnitte 13 und 43 der Verordnung (EG) Nr. 810/2009 vom 13. Juli 2009 über einen Visakodex der Gemeinschaft) und dass diese Auslagerung infolge des Aufkommens von Cloud-Speichern zunehmend häufiger erfolgt.

In diesem Fall muss der für die Verarbeitung Verantwortliche eine detaillierte Regelung dahin gehend treffen, wie die jeweiligen Unterauftragnehmer kontrolliert werden können (beispielsweise durch unangekündigte Nachprüfungen). Außerdem muss er Garantien in Bezug auf die betreffenden Mitarbeiter, Verfahren zum Schutz der individuellen Rechte usw. vorsehen.

Brüssel, den 27. April 2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Stellungnahme 05/2012 zum Cloud Computing (WP 196)

Angenommen am 1. Juli 2012

Zusammenfassung

In dieser Stellungnahme analysiert die Artikel-29-Datenschutzgruppe alle relevanten Fragen, die im Europäischen Wirtschaftsraum (EWR) tätige Cloud Computing-Diensteanbieter und ihre Kunden betreffen. Dabei werden alle einschlägigen anzuwendenden Grundsätze aus der EU-Datenschutzrichtlinie (95/46/EG) und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung) aufgeführt.

Trotz der anerkannten wirtschaftlichen und gesellschaftlichen Vorteile des Cloud Computing zeigt die vorliegende Stellungnahme, wie die weit verbreitete Nutzung von Diensten des Cloud Computing zu einer Reihe von Datenschutzrisiken führen kann. Hier geht es in erster Linie um die fehlende Kontrolle über personenbezogene Daten und über unzureichende Informationen darüber, wie, wo und durch wen die Daten verarbeitet bzw. im Unterauftrag verarbeitet werden. Diese Risiken müssen von öffentlichen Einrichtungen und Privatunternehmen sorgfältig bewertet werden, wenn sie in Betracht ziehen, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen. Die vorliegende Stellungnahme untersucht Fragen, die mit der gemeinsamen Nutzung von Ressourcen mit anderen Parteien verbunden sind; die fehlende Transparenz in einer Outsourcing-Kette, die aus zahlreichen Auftragsverarbeitern und Unterauftragnehmern besteht; das Fehlen eines gemeinsamen, weltweiten Rahmens für die Datenportabilität und die Ungewissheit bezüglich der Zulässigkeit der Übermittlung personenbezogener Daten an Cloud-Anbieter, die außerhalb des EWR niedergelassen sind. Ähnlich wird in der Stellungnahme hervorgehoben, dass der Mangel an Transparenz in Bezug auf die Informationen, die ein für die Verarbeitung Verantwortlicher der betroffenen Person über die Art der Verarbeitung ihrer personenbezogenen Daten geben kann, Anlass zu ernster Besorgnis ist. Die betroffenen Personen müssen[1] darüber informiert werden, wer ihre Daten für welche Zwecke verarbeitet, damit sie ihre diesbezüglichen Rechte ausüben können.

Eine wichtige Schlussfolgerung dieser Stellungnahme ist, dass Unternehmen und Verwaltungen, die Cloud Computing nutzen wollen, als ersten Schritt eine umfassende und gründliche Risikoanalyse durchführen sollten. Alle Cloud-Anbieter,

[1] Die im nachstehenden Teil dieses Dokuments verwendeten Schlüsselbegriffe „MUSS“ bzw. „MÜSSEN“,“DARF NICHT“ bzw. „DÜRFEN NICHT“, „ERFORDERLICH“, „SOLLTE(N)“, „SOLLTE(N) NICHT“, „EMPFOHLEN“, „KANN“ bzw. „KÖNNEN“ und „OPTIONAL“ sind wie in RFC 2119 beschrieben auszulegen. Das Dokument ist verfügbar unter http://www.ietf.org/rfc/rfc2119.txt. Aus Gründen der Lesbarkeit werden diese Wörter in dem Dokument jedoch nicht alle in Großbuchstaben gedruckt.

die Dienste im EWR anbieten, sollten dem Cloud-Anwender alle Informationen geben, die dieser benötigt, um die Vor- und Nachteile der Inanspruchnahme eines solchen Dienstes gründlich gegeneinander abwägen zu können. Beim Anbieten von Diensten des Cloud Computing sollten Sicherheit, Transparenz und Rechtssicherheit für die Anwender die wichtigsten Aspekte sein.

In den Empfehlungen dieser Stellungnahme wird die Verantwortung eines Cloud-Anwenders als für die Verarbeitung Verantwortlicher hervorgehoben, und es wird folglich empfohlen, dass der Anwender einen Cloud-Anbieter auswählt, der die Einhaltung der EU-Datenschutzbestimmungen gewährleistet. In der Stellungnahme werden geeignete vertragliche Absicherungsklauseln angesprochen. Dabei wird gefordert, dass jeder Vertrag zwischen dem Cloud-Anwender und dem Cloud-Anbieter ausreichende Garantien in Bezug auf technische und organisatorische Maßnahmen enthält. Die Empfehlung, dass der Cloud-Anwender überprüfen sollte, ob der Cloud-Anbieter die Rechtmäßigkeit jeder grenzüberschreitenden Datenübermittlung garantieren kann, ist ebenfalls von Bedeutung.

Wie bei jedem Entwicklungsprozess stellt auch der Aufstieg des Cloud Computing zu einem weltweiten technologischen Paradigma eine Herausforderung dar. Für sich betrachtet, kann diese Stellungnahme als wichtiger Schritt zur Festlegung der Aufgaben angesehen werden, die von der Datenschutzgemeinde in den folgenden Jahren übernommen werden müssen.

Inhalt

1. Einleitung

Für Manche stellt das Cloud Computing eine der größten technologischen Revolutionen der letzten Jahre dar. Andere sehen es lediglich als natürliche Weiterentwicklung einer Reihe von Technologien, die dem Wahrwerden des langersehnten Traums des Utility Computing dienen. Auf jeden Fall haben zahlreiche Stakeholder dem Cloud Computing bei der Entwicklung ihrer technologischen Strategien Priorität eingeräumt.

Das Cloud Computing besteht aus einer Reihe von Technologien und Service-Modellen, die sich auf eine internetbasierte Nutzung und Lieferung von IT-Anwendungen, auf die Verarbeitungsfähigkeit, die Aufbewahrung und den Speicherplatz konzentrieren. Das Cloud Computing kann wichtige Wirtschaftsvorteile schaffen, da nach Bedarf bereitgestellte Ressourcen im Internet ziemlich einfach konfiguriert, erweitert und genutzt werden können. Außerdem kann das Cloud Computing Sicherheitsvorteile bieten. Insbesondere kleine bis mittlere Unternehmen können zu geringen Kosten erstklassige Technologien erwerben, die ansonsten außerhalb ihrer finanziellen Möglichkeiten lägen.

Es gibt eine große Bandbreite an Leistungen, die Cloud-Anbieter anbieten. Diese reichen von virtuellen Verarbeitungssystemen (die unter der direkten Kontrolle des für die Verarbeitung Verantwortlichen konventionelle Server ersetzen und/oder parallel zu ihnen arbeiten) über Dienste, die die Anwendungsentwicklung und erweitertes Hosting unterstützen, bis zu webbasierten Softwarelösungen, die Anwendungen ersetzen können, die auf herkömmliche Weise auf den Computern der Endnutzer installiert sind. Dazu gehören Textverarbeitungsanwendungen, Agenden und Kalender, Ablagesysteme für Online-Dokumente, die Speicherung und ausgelagerte E-Mail-Lösungen. Einige der am häufigsten verwendeten Definitionen für diese unterschiedlichen Arten von Diensten sind im Anhang zu dieser Stellungnahme enthalten.

In dieser Stellungnahme analysiert die Artikel-29-Datenschutzgruppe (nachfolgend WP 29) das anzuwendende Recht und die Verpflichtungen der für die Verarbeitung Verantwortlichen, die im Europäischen Wirtschaftsraum (nachfolgend EWR) tätig sind, und der Anbieter von Cloud-Diensten im EWR. Die vorliegende Stellungnahme konzentriert sich auf die Situation, in der angenommen wird, dass eine Beziehung des Typs „für die Verarbeitung Verantwortlicher – Auftragsverarbeiter“ vorliegt, wobei der Anwender als für die Verarbeitung Verantwortlicher und der Cloud-Anbieter als Auftragsverarbeiter klassifiziert wird. In den Fällen, in denen der Cloud-Anbieter auch als für die Verarbeitung Verantwortlicher handelt, muss er zusätzliche Anforderungen erfüllen. Vor der Nutzung von Cloud Computing ist eine durch den für die Verarbeitung Verantwortlichen durchgeführte, angemessene Risikobewertung folglich Voraussetzung. Dabei sind auch die Standorte der Server zu berücksichtigen, auf denen die

Daten verarbeitet werden. Außerdem sollte anhand der nachfolgend dargelegten Kriterien eine Abwägung der Vor- und Nachteile aus Sicht des Datenschutzes durchgeführt werden.

Die Stellungnahme bestimmt sowohl für die für die Verarbeitung Verantwortlichen als auch für die Auftragsverarbeiter die im Sinne der allgemeinen Datenschutzrichtlinie (95/46/EG) anzuwendenden Grundsätze wie Zweckbestimmung und Zweckbegrenzung, die Löschung von Daten sowie technische und organisatorische Maßnahmen. Die Stellungnahme bietet Anleitung in Bezug auf die Sicherheitsanforderungen, sowohl als strukturelle als auch als verfahrensrechtliche Garantie. Besondere Betonung wird auf die vertraglichen Vereinbarungen gelegt, die die Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter in diesem Zusammenhang regeln sollten. Die klassischen Ziele der Datensicherheit sind Verfügbarkeit, Integrität und Vertraulichkeit. Datenschutz ist jedoch nicht auf Datensicherheit beschränkt, und deshalb werden diese Ziele um die spezifischen Datenschutzziele Transparenz, Isolierung, Intervenierbarkeit und Portabilität ergänzt, um das in Artikel 8 der Charta der Grundrechte der Europäischen Union niedergelegte Recht des Einzelnen auf Datenschutz zu stärken.

In Bezug auf die Übermittlung personenbezogener Daten aus dem EWR werden Instrumente wie die von der Europäischen Kommission angenommenen Standardvertragsklauseln, die Bescheinigung eines angemessenen Schutzniveaus und mögliche zukünftige verbindliche unternehmerische Vorschriften sowie die Datenschutzrisiken, die sich aus Ersuchen internationaler Strafverfolgungsbehörden ergeben, analysiert.

Die vorliegende Stellungnahme schließt mit Empfehlungen für Cloud-Anwender als für die Verarbeitung Verantwortliche, für Cloud-Anbieter als Auftragsverarbeiter und für die Europäische Kommission in Bezug auf zukünftige Änderungen im Europäischen Datenschutzrahmen.

Die Berliner Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat im April 2012 das *Sopot Memorandum*[2] angenommen. In diesem Memorandum werden Fragen der Privatsphäre und des Datenschutzes beim Cloud Computing untersucht. Es wird betont, dass Cloud Computing nicht zu niedrigeren Datenschutzstandards als bei der konventionellen Datenverarbeitung führen darf.

[2] http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

2. Datenschutzrisiken des Cloud Computing

Da sich diese Stellungnahme auf die Verarbeitung personenbezogener Daten unter Verwendung des Cloud Computing konzentriert, werden nur die spezifischen Risiken betrachtet, die in diesem Zusammenhang auftreten.[3] Die Mehrheit dieser Risiken fällt in zwei große Kategorien, nämlich die fehlende Kontrolle über die Daten und unzureichende Informationen über die Verarbeitung selbst (fehlende Transparenz). Spezifische, in dieser Stellungnahme berücksichtigte Risiken des Cloud Computing umfassen:

fehlende Kontrolle

Wenn personenbezogene Daten Systemen überlassen werden, die von einem Cloud-Anbieter verwaltet werden, haben Cloud-Anwender möglicherweise nicht mehr länger die ausschließliche Kontrolle über diese Daten und können die technischen und organisatorischen Maßnahmen nicht ergreifen, die zur Sicherstellung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Isolierung[4], Intervenierbarkeit und Portabilität der Daten erforderlich sind. Diese fehlende Kontrolle kann sich folgendermaßen manifestieren:

- fehlende Verfügbarkeit aufgrund fehlender Interoperabilität (Vendor Lock-in): Wenn der Cloud-Anbieter eine eigene Technologie verwendet, kann es für den Cloud-Anwender schwierig sein, Daten und Dokumente zwischen verschiedenen cloudbasierten Systemen zu verschieben (Datenportabilität) oder Informationen mit Stellen auszutauschen, die von anderen Anbietern verwaltete Cloud-Dienste nutzen (Interoperabilität).
- fehlende Integrität durch die gemeinsame Nutzung von Ressourcen: Eine Cloud setzt sich aus gemeinsam genutzten Systemen und Infrastrukturen zusammen. Cloud-Anbieter verarbeiten personenbezogene Daten, die im Hinblick auf die betroffenen Personen und Organisationen aus einer Vielzahl von Quellen stammen. Dabei kann es zu Interessenkollisionen und/oder unterschiedlichen Zielen kommen.
- fehlende Vertraulichkeit in Bezug auf Ersuchen von Strafverfolgungsbehörden, die direkt an den Cloud-Anbieter gerichtet werden: Personenbezogene Daten, die in der Cloud verarbeitet werden, können Gegenstand von Ersuchen von Strafverfolgungsbehörden aus den EU-Mitgliedstaaten und aus Drittländern sein. Es besteht das Risiko, dass personenbezogene Daten einer (fremden) Strafverfolgungsbehörde offengelegt werden, ohne dass hierfür eine gel-

[3] Zusätzlich zu den ausdrücklich in dieser Stellungnahme genannten Risiken, die sich aus der Verarbeitung personenbezogener Daten „in der Wolke“ ergeben, müssen auch alle Risiken berücksichtigt werden, die mit der Auslagerung der Verarbeitung personenbezogener Daten in Verbindung stehen.

[4] In Deutschland wurde das breitere Konzept der „Unverkettbarkeit“ eingeführt. Vgl. die nachfolgende Fußnote 24.

tende Rechtsgrundlage nach dem EU-Recht vorliegt. Dann würde eine Verletzung des EU-Datenschutzrechts vorliegen.

- fehlende Intervenierbarkeit aufgrund der Komplexität und der Dynamik in der Outsourcing-Kette: Der Cloud-Dienst eines Anbieters kann sich aus einer Kombination von Diensten einer Reihe anderer Anbieter zusammensetzen, die im Laufe der Dauer des Vertrags mit dem Kunden dynamisch hinzugefügt oder entfernt werden.
- fehlende Intervenierbarkeit (Rechte der betroffenen Person): Ein Cloud-Anbieter kann möglicherweise nicht die erforderlichen Maßnahmen und Werkzeuge bereitstellen, die den für die Verarbeitung Verantwortlichen bei der Verwaltung der Daten beispielsweise im Hinblick auf den Zugang zu, die Löschung von oder die Berichtigung von Daten unterstützen.
- fehlende Isolierung: Ein Cloud-Anbieter könnte seine physische Kontrolle über die Daten von verschiedenen Anwendern zur Verknüpfung personenbezogener Daten nutzen. Wenn die Administratoren mit ausreichend privilegierten Zugangsrechten (mit hohen Risiken behaftete Funktionen) ausgestattet sind, könnten sie Informationen verschiedener Anwender miteinander verbinden.

fehlende Informationen zur Verarbeitung (Transparenz)

Unzureichende Informationen über die Verarbeitungsprozesse eines Cloud-Dienstes stellen ein Risiko sowohl für den für die Verarbeitung Verantwortlichen als auch für die betroffenen Personen dar, da ihnen möglicherweise die potenziellen Gefahren und Risiken gar nicht bewusst sind und sie folglich auch keine ihnen angemessen erscheinenden Maßnahmen ergreifen können.

Es können sich potenzielle Bedrohungen ergeben, wenn der für die Verarbeitung Verantwortliche nicht weiß, dass

- eine Kettenverarbeitung stattfindet, die zahlreiche Auftragsverarbeiter und Unterauftragnehmer umfasst.
- personenbezogene Daten an verschiedenen geografischen Standorten im EWR verarbeitet werden. Dies wirkt sich direkt auf das Recht aus, das bei Datenschutzstreitigkeiten anzuwenden ist, die sich möglicherweise zwischen dem Anwender und dem Anbieter ergeben.
- personenbezogene Daten in Drittländer außerhalb des EWR übermittelt werden. Drittländer sind möglicherweise nicht dazu in der Lage, ein angemessenes Datenschutzniveau zu bieten und Übermittlungen werden vielleicht nicht durch geeignete Maßnahmen geschützt (z. B. Standardvertragsklauseln oder verbindliche unternehmensinterne Vorschriften), so dass sie illegal sein könnten.

Betroffene Personen, deren personenbezogene Daten in der Cloud verarbeitet werden, müssen über die Identität des für die Verarbeitung Verantwortlichen und den Zweck der Verarbeitung informiert werden (in der Datenschutzrichtlinie 95/46/EG niedergelegte Anforderung für alle für die Verarbeitung Verantwortlichen). Damit gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben gewährleistet wird (Artikel 10 Richtlinie 95/46/EG) und angesichts der potenziellen Komplexität von Verarbeitungsketten in der Cloud Computing-Umgebung sollten für die Verarbeitung Verantwortliche – auch im Sinne einer angemessenen Vorgehensweise – weitere Informationen bezüglich der (Unter-)Auftragsverarbeiter erteilen, die die Cloud-Dienste bereitstellen.

3. Rechtsrahmen

3.1 Datenschutzrahmen

Die Datenschutzrichtlinie 95/46/EG ist der einschlägige Rechtsrahmen. Diese Richtlinie findet in jedem Fall Anwendung, in dem personenbezogene Daten aufgrund einer Nutzung von Cloud Computing-Diensten verarbeitet werden. Die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung) findet auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich verfügbarer elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzwerken Anwendung (Telekom-Betreiber) und ist folglich die einschlägige Richtlinie, wenn solche Dienste mittels einer Cloud-Lösung angeboten werden[5].

3.2 Anwendbares Recht

Die Kriterien zur Festlegung des anwendbaren Rechts sind in Artikel 4 der Richtlinie 95/46/EG niedergelegt, der sich auf das Recht bezieht, das auf die für die Verarbeitung Verantwortlichen anwendbar ist[6], die eine oder mehr Niederlassungen im EWR besitzen oder die außerhalb des EWR niedergelassen sind, aber für die Verarbeitung personenbezogener Daten Ausrüstung verwenden, die sich innerhalb des EWR befindet. Die Artikel-29-Datenschutzgruppe hat dies in ihrer Stellungnahme 8/2010 zum anwendbaren Recht[7] analysiert.

---

[5] Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung): Die Richtlinie 2002/58/EG zur Privatsphäre in der Telekommunikation findet auf die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste Anwendung und verlangt, dass sie die Einhaltung der Verpflichtungen in Bezug auf die Geheimhaltung von Mitteilungen und auf den Schutz personenbezogener Daten sowie der Rechte und Pflichten in Bezug auf elektronische Kommunikationsnetzwerke und -dienste sicherstellen. In Fällen, in denen der Anbieter des Cloud Computing als Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste auftritt, unterliegt er dieser Richtlinie.

[6] Der Begriff des für die Verarbeitung Verantwortlichen wird in Artikel 2 Buchstabe h der Richtlinie genannt und wurde von der Artikel-29-Datenschutzgruppe in ihre Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ analysiert.

[7] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf

Im ersten Fall wird gemäß Artikel 4 Absatz 1 Buchstabe a der Richtlinie die Anwendung des EU-Rechts auf den für die Verarbeitung Verantwortlichen durch den Standort seiner Niederlassung und durch den Ort der Durchführung seiner Tätigkeit festgelegt, ohne dass hierfür die Art des Cloud-Dienst-Modells von Bedeutung wäre. Es ist das Recht des Landes anwendbar, in dem der für die Verarbeitung Verantwortliche seine Niederlassung hat, der den Vertrag über die Cloud Computing-Dienste geschlossen hat und nicht der Ort, an dem der Anbieter des Cloud Computing seinen Sitz hat.

Sollte der für die Verarbeitung Verantwortliche Niederlassungen in mehreren Mitgliedstaaten haben und die Daten als Teil seiner Tätigkeit in diesen Ländern verarbeiten, ist jeweils das Recht jedes Mitgliedstaats anzuwenden, in dem die Verarbeitung stattfindet.

Artikel 4 Absatz 1 Buchstabe c[8] bezieht sich darauf, wie die Datenschutzbestimmungen auf für die Verarbeitung Verantwortliche anzuwenden sind, die nicht im EWR niedergelassen sind, aber automatisierte oder nicht automatisierte Mittel einsetzen, die sich im Hoheitsgebiet des Mitgliedstaates befinden, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr genutzt werden. Das heißt, dass wenn ein Cloud-Anwender, der außerhalb des EWR niedergelassen ist, aber einen innerhalb des EWR niedergelassenen Cloud-Anbieter beauftragt, dieser Anbieter die Datenschutzbestimmungen zum Anwender exportiert.

3.3 Pflichten und Verantwortlichkeiten der verschiedenen Beteiligten

Wie bereits gesagt, betrifft Cloud Computing eine Reihe verschiedener Beteiligter. Es ist wichtig, die Rolle jedes dieser Beteiligten zu bewerten und zu klären, um so ihre spezifischen Verpflichtungen in Bezug auf die aktuellen Datenschutzbestimmungen festzulegen.

Es sollte daran erinnert werden, dass die WP 29 in ihrer Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ darauf hingewiesen hat, dass *„der Begriff „für die Verarbeitung Verantwortlicher“ in erster Linie dazu dient, zu bestimmen, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und wie die betroffenen Personen ihre Rechte in der Praxis ausüben können. Anders ausgedrückt: Er dient dazu, Verantwortung zuzuweisen.“* Die von der vorliegenden Analyse betroffenen Personen sollten diese beiden allgemeinen Kriterien für die Einhaltung und die Zuweisung von Verantwortung im Hinterkopf behalten.

---

[8] Artikel 4 Absatz 1 Buchstabe c legt fest, dass das Recht eines Mitgliedstaats anwendbar ist, wenn der „für die Verarbeitung Verantwortliche […] nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.“

3.3.1 Cloud-Anwender und Cloud-Anbieter

Der Cloud-Anwender legt den letztendlichen Zweck der Verarbeitung fest und entscheidet über die Auslagerung dieser Verarbeitung und die Delegierung von allen oder Teilen der Verarbeitungstätigkeiten an eine externe Organisation. Folglich fungiert der Cloud-Anwender als für die Datenverarbeitung Verantwortlicher. Die Richtlinie legt fest, dass der für die Verarbeitung Verantwortliche als *„natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, […] allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet."* Der Cloud-Anwender als für die Verarbeitung Verantwortlicher muss die Verantwortung für die Einhaltung der Datenschutzbestimmungen übernehmen. Er ist verantwortlich und unterliegt allen rechtlichen Verpflichtungen, die in der Richtlinie 95/46/EG angesprochen werden. Der Cloud-Anwender kann den Cloud-Anbieter damit beauftragen, die Methoden und die technischen oder organisatorischen Maßnahmen für das Erreichen der Zwecke des für die Verarbeitung Verantwortlichen auszuwählen.

Der Cloud-Anbieter ist die juristische Person, die die Cloud Computing-Dienste in den verschiedenen, vorstehend diskutierten Formen bereitstellt. Wenn der Cloud-Anbieter die Mittel und die Plattform bereitstellt und dabei im Auftrag des Cloud-Anwenders handelt, wird er als Auftragsverarbeiter angesehen, das heißt er ist nach der Richtlinie 95/46/EG *„die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet"*.[9] [10]

Wie in der Stellungnahme 1/2010 festgestellt wurde, können manche Kriterien[11] genutzt werden, um zu bewerten, wer für die Verarbeitung verantwortlich ist. Tatsächlich kann es Situationen geben, in denen ein Anbieter von Cloud-Diensten je nach den jeweiligen Umständen entweder als gemeinsamer oder als eigenständiger für die Verarbeitung Verantwortlicher betrachtet werden kann. Das könnte beispielsweise der Fall sein, wenn der Anbieter Daten für seine eigenen Zwecke verarbeitet.

Es sollte betont werden, dass auch in komplexen Datenverarbeitungsumgebungen, in denen verschiedene für die Verarbeitung Verantwortliche bei der Verarbeitung personenbezogener Daten eine Rolle spielen, die Datenschutzbestimmungen eingehalten werden müssen. Auch die Verantwortung für eine mögliche

---

[9] Diese Stellungnahme konzentriert sich lediglich auf die normale Beziehung „für die Verarbeitung Verantwortlicher – Auftragsverarbeiter".

[10] Die Cloud Computing-Umgebung kann auch von natürlichen Personen (Nutzern) verwendet werden, um ausschließlich persönliche oder heimische Tätigkeiten durchzuführen. In dem Fall muss gründlich analysiert werden, ob die sogenannte Ausnahmeklausel für Privathaushalte Anwendung findet, nach der Nutzer keine für die Verarbeitung Verantwortlichen sein können. Diese Frage geht jedoch über den Zweck dieser Stellungnahme hinaus.

[11] Z. B. Weisungsebene, Überwachung durch den Cloud-Anwender, Kenntnisse der Parteien.

Verletzung dieser Bestimmungen muss klar zugewiesen sein, um zu vermeiden, dass der Schutz personenbezogener Daten reduziert wird oder dass „negative Zuständigkeitskonflikte" und Lücken auftreten und dadurch einige Verpflichtungen und Rechte aus der Richtlinie durch eine der Parteien nicht gewährleistet werden.

Im aktuellen Cloud Computing-Szenario haben die Anwender von Cloud Computing-Diensten vielleicht nicht die Möglichkeit, die Vertragsbedingungen für die Nutzung der Cloud-Dienste auszuhandeln, da diese häufig Gegenstand standardisierter Angebote sind. Dennoch ist es letztendlich der Anwender, der für bestimmte Zwecke über die Zuweisung eines Teils oder aller Verarbeitungsschritte an Cloud-Dienste entscheidet. Die Rolle des Anbieters gegenüber dem Anwender ist die eines Auftragnehmers. In diesem Fall ist das der entscheidende Punkt. Wie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 1/2010[12] zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" festgestellt hat *„darf das Ungleichgewicht in der Vertragsposition zwischen einem kleinen für die Verarbeitung Verantwortlichen und großen Dienstleistern nicht als Rechtfertigung dafür gelten, dass der für die Verarbeitung Verantwortliche Vertragsklauseln und -bedingungen akzeptiert, die gegen das Datenschutzrecht verstoßen."* Aus diesem Grund muss der für die Verarbeitung Verantwortliche einen Cloud-Anbieter auswählen, der die Einhaltung der Datenschutzbestimmungen garantiert. Besondere Betonung muss auf die Bestandteile der anzuwendenden Verträge gerichtet werden. Diese haben einen Satz standardisierter Datenschutzgarantien zu enthalten, die die Garantien umfassen müssen, welche die Datenschutzgruppe in Abschnitt 3.4.3 (Technische und organisatorische Maßnahmen) und in Abschnitt 3.5 (Grenzüberschreitende Datenflüsse) dargelegt hat – sowie etwaige zusätzliche Mechanismen, die sich als eine Vereinfachung in Bezug auf die gebührende Sorgfalt und Rechenschaftspflicht herausstellen können (wie unabhängige Prüfungen durch Dritte und Zertifizierungen der Leistungen des Anbieters – siehe Abschnitt 4.2).

Cloud-Anbieter sind (als Auftragsverarbeiter) zur Sicherstellung der Vertraulichkeit verpflichtet. Richtlinie 95/46 EC stellt Folgendes fest: *„Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen."* Der Zugang des Cloud-Anbieters zu den Daten während der Dienstebereitstellung ist ebenfalls im Wesentlichen durch die Anforderung geregelt, die Bestimmungen von Artikel 17 der Richtlinie einzuhalten – siehe Abschnitt 3.4.2.

[12] Stellungnahme 01/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" – http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

Auftragsverarbeiter müssen die Art der betreffenden Cloud berücksichtigen (Public, Private, Community oder Hybrid / IaaS, SaaS oder PaaS [siehe Anhang a) Rollout-Modelle – b) Modelle der Diensteerbringung]) und die Art Dienst, für den der Anwender einen Vertrag abgeschlossen hat. Die Auftragsverarbeiter sind dafür verantwortlich, Sicherheitsmaßnahmen zu ergreifen, die den EU-Bestimmungen entsprechen, in deren Anwendungsbereich der für die Verarbeitung Verantwortliche und Auftragsverarbeiter fallen. Auftragsverarbeiter müssen den für die Verarbeitung Verantwortlichen auch bei der Einhaltung der (ausgeübten) Rechte der betroffenen Personen unterstützen.

3.3.2 Unterauftragnehmer

Cloud Computing-Dienste können die Beteiligung einer Reihe von Vertragsparteien mit sich bringen, die als Auftragsverarbeiter fungieren. Auftragsverarbeiter schließen häufig Unterverträge mit zusätzlichen Unterauftragsverarbeitern, die dann Zugang zu personenbezogenen Daten erhalten. Wenn ein Auftragsverarbeiter Dienste an Unterauftragsverarbeiter weitervergibt, muss der Anwender darüber informiert werden. Dabei müssen die Art des weitervergebenen Dienstes und die Kenndaten aktueller oder potenzieller Unterauftragnehmer angegeben werden. Außerdem muss garantiert werden, dass diese dem Anbieter der Cloud Computing-Dienste anbieten, die Richtlinie 95/46/EG einzuhalten.

Alle einschlägigen Verpflichtungen müssen folglich durch Verträge zwischen dem Cloud-Anbieter und dem Unterauftragnehmer auch für Unterauftragsverarbeiter gelten. Diese Verträge sollten die vertraglichen Vereinbarungen zwischen dem Cloud-Anwender und dem Cloud-Anbieter widerspiegeln. In ihrer Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ hat die Artikel-29-Datenschutzgruppe auf die Vielzahl von Auftragsverarbeitern hingewiesen, die in einer direkten Beziehung zu dem für die Verarbeitung Verantwortlichen stehen können oder die Unterauftragnehmer sein können, an die die Auftragsverarbeiter einen Teil der ihnen anvertrauten Verarbeitungstätigkeiten ausgelagert haben. *„In der Richtlinie spricht nichts dagegen, dass durch Aufteilung der betreffenden Aufgaben aufgrund organisatorischer Anforderungen mehrere Organisationen zu Auftragsverarbeitern oder (Unter-)Auftragsverarbeitern bestimmt werden. Bei der Durchführung der Verarbeitung müssen jedoch alle diese Auftragsverarbeiter die Weisungen des für die Verarbeitung Verantwortlichen befolgen.“*[13]

Bei solchen Szenarien sollten die sich aus den Datenschutzbestimmungen ergebenden Verpflichtungen und Verantwortlichkeiten klar zugewiesen sein und nicht

[13] Vgl. WP169, S. 29, Stellungnahme 01/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ – http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

entlang der Kette von Auslagerungen oder der Vergabe von Unterverträgen gestreut werden, damit eine wirksame Kontrolle sichergestellt und eine klare Verantwortung für die Verarbeitungstätigkeiten zugewiesen wird.

Ein mögliches Muster der Zusicherungen, das zur Klärung der Pflichten und Verpflichtungen von Auftragsverarbeitern genutzt werden kann, wenn sie die Datenverarbeitung weitervergeben, wurde zuerst im Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern[14] eingeführt. Nach diesem Muster ist eine Vergabe von Unteraufträgen nur mit der vorherigen schriftlichen Einwilligung des für die Verarbeitung Verantwortlichen und mit einer schriftlichen Vereinbarung möglich, welche dem Unterauftragsverarbeiter dieselben Verpflichtungen auferlegt, die der Auftragsverarbeiter hat. Erfüllt der Unterauftragsverarbeiter seine Datenschutzverpflichtungen aus einer solchen schriftlichen Vereinbarung nicht, bleibt der Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters aus einer solchen Vereinbarung uneingeschränkt haftbar. Eine Bestimmung dieser Art könnte in jeder Vertragsklausel zwischen einem für die Verarbeitung Verantwortlichen und einem Cloud-Diensteanbieter verwendet werden, wenn der letztgenannte die Dienste durch die Vergabe von Unteraufträgen bereitstellen möchte. So können die erforderlichen Garantien für die Vergabe von Unteraufträgen sichergestellt werden.

Eine ähnliche Lösung bezüglich der Zusicherungen im Lauf einer Vergabe von Unteraufträgen wurde kürzlich von der Kommission in dem Vorschlag für eine Datenschutz-Grundverordnung[15] gemacht. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem unter anderem insbesondere vorgesehen ist, dass der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch nehmen darf (Artikel 26 Absatz 2 des Vorschlags).

Nach Ansicht der WP29 kann der Auftragsverarbeiter seine Tätigkeiten nur auf der Grundlage der Einwilligung des für die Verarbeitung Verantwortlichen weitervergeben. Diese Einwilligung kann bei Beginn der Bereitstellung der Dienste generell erteilt werden[16]. Der Auftragsverarbeiter ist eindeutig dazu verpflichtet, den für die Verarbeitung Verantwortlichen über beabsichtigte Änderun-

14 Siehe FAQ II.5 in WP176.

15 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 25.1.2012.

16 Siehe FAQ II.1 in WP176, angenommen am 12. Juli 2010.

gen in Bezug auf weitere Unterauftragnehmer oder den Ersatz von Unterauftragnehmern zu informieren. Der für die Verarbeitung Verantwortliche hat jederzeit die Möglichkeit, solchen Änderungen zu widersprechen oder den Vertrag zu beenden. Der Cloud-Anbieter sollte eindeutig dazu verpflichtet sein, alle beauftragten Unterauftragnehmer zu nennen. Darüber hinaus sollte zwischen dem Cloud-Anbieter und dem Unterauftragnehmer ein Vertrag geschlossen werden, der die Vertragsbedingungen zwischen dem Cloud-Anwender und dem Cloud-Anbieter widerspiegelt. Der für die Verarbeitung Verantwortliche sollte im Fall von Vertragsverletzungen durch die Unterauftragsverarbeiter vertragliche Rückgriffsmöglichkeiten in Anspruch nehmen können. Hierzu könnte sichergestellt werden, dass der Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen für alle Vertragsverletzungen direkt haftbar ist, die von einem von ihm beauftragten Unterauftragsverarbeiter begangen werden. Eine weitere Möglichkeit wäre die Schaffung des Rechts als Drittbegünstigter zugunsten des für die Verarbeitung Verantwortlichen in allen Verträgen, die zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter unterzeichnet werden. Eine weitere Möglichkeit stellt auch die Tatsache dar, dass diese Aufträge im Auftrag des für die Datenverarbeitung Verantwortlichen unterzeichnet werden, so dass dieser Vertragspartei wird.

3.4 Datenschutzanforderungen in dem Verhältnis Anwender-Anbieter

3.4.1 Einhaltung der Grundprinzipien

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in der Cloud hängt von der Einhaltung der Grundprinzipien der Datenschutzbestimmungen der EU ab: Gegenüber der betroffenen Person muss Transparenz garantiert sein, der Grundsatz der Zweckbestimmung und Zweckbegrenzung muss eingehalten werden und personenbezogene Daten sind zu löschen, sobald ihre Aufbewahrung nicht mehr länger erforderlich ist. Darüber hinaus müssen geeignete technische und organisatorische Maßnahmen umgesetzt werden, um ein angemessenen Niveau des Datenschutzes und der Datensicherheit zu gewährleisten.

3.4.1.1 Transparenz

Transparenz ist eine grundlegende Voraussetzung dafür, dass personenbezogene Daten nach Treu und Glauben und rechtmäßig verarbeitet werden. Richtlinie 95/46/EG verpflichtet den Cloud-Anwender dazu, der betroffenen Person, bei der die sie betreffenden Daten erhoben werden, seine Identität und die Zweckbestimmung der Verarbeitung mitzuteilen. Der Cloud-Anwender sollte auch weitere Informationen beispielsweise betreffend die Empfänger oder Kategorien der Empfänger der Daten erteilen, die auch Auftragsverarbeiter und Unterauftragsverarbeiter umfassen können, sofern diese Informationen notwendig sind, um gegen-

über der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten (vgl. Artikel 10 der Richtlinie)[17].

Transparenz muss auch in der (den) Beziehung(en) zwischen dem Cloud-Anwender, dem Cloud-Anbieter und den Unterauftragnehmern (sofern vorhanden) sichergestellt werden. Der Cloud-Anwender kann die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in der Cloud nur dann prüfen, wenn ihn der Anbieter über alle einschlägigen Fragen informiert. Ein für die Verarbeitung Verantwortlicher, der in Erwägung zieht, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen, sollte die Geschäftsbedingungen des Cloud-Anbieters sorgfältig prüfen und sie von einem datenschutzrechtlichen Standpunkt aus bewerten.

Transparenz in der Cloud bedeutet, dass es erforderlich ist, den Cloud-Anwender über alle Unterauftragnehmer zu informieren, die zur Bereitstellung der entsprechenden Cloud-Dienste beitragen sowie über alle Standorte der Datenzentren, an denen personenbezogene Daten verarbeitet werden können.[18]

Erfordert die Bereitstellung der Dienste die Installation von Software auf dem System des Cloud-Anwenders (z. B. Browser Plug-ins), sollte der Cloud-Anbieter den Kunden im Rahmen einer angemessenen Vorgehensweise über diesen Umstand informieren und insbesondere über die Konsequenzen aus der Sicht des Datenschutzes und der Datensicherheit. Entsprechend sollte der Cloud-Anwender dieses Thema vorab ansprechen, wenn es von dem Cloud-Anbieter nicht in ausreichendem Maß behandelt wird.

3.4.1.2 Zweckbestimmung und -begrenzung

Der Grundsatz der Zweckbestimmung und -begrenzung sieht vor, dass personenbezogene Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden (vgl. Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG). Der Cloud-Anwender muss den (die) Zweck(e) der Verarbeitung festlegen, bevor er personenbezogene Daten von der betroffenen Person erhebt und diese darüber informieren. Er darf personenbezogene Daten nicht für andere Zwecke verarbeiten, die nicht mit den ursprünglichen Zwecken vereinbar sind.

Außerdem muss sichergestellt werden, dass personenbezogene Daten nicht (ge-

---

17 Eine ähnliche Informationspflicht gegenüber der betroffenen Person besteht, wenn Daten, die nicht bei der betroffenen Person erhoben wurden, sondern aus einer anderen Quelle stammen, aufgezeichnet oder an Dritte weitergegeben werden (vgl. Artikel 11).

18 Nur dann kann er beurteilen, ob personenbezogene Daten an ein sogenanntes Drittland außerhalb des Europäischen Wirtschaftsraums (EWR) übermittelt werden können, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG sicherstellt. Vgl. auch den nachstehenden Abschnitt 3.4.6.

setzeswidrig) für weitere Zwecke von dem Cloud-Anbieter oder von einem seiner Unterauftragnehmer verarbeitet werden. Da ein typisches Cloud-Szenario leicht eine größere Anzahl an Unterauftragnehmern umfassen kann, muss das Risiko einer Verarbeitung personenbezogener Daten für weitere, nicht vereinbarte Zwecke als recht hoch angesehen werden. Zur Minimierung dieses Risikos sollte der Vertrag zwischen dem Cloud-Anbieter und dem Cloud-Anwender technische und organisatorische Maßnahmen zur Eindämmung dieses Risikos umfassen und Sicherungen für das Protokollieren und die Kontrolle der einschlägigen Verarbeitungen personenbezogener Daten enthalten, die von Angestellten des Cloud-Anbieters oder der Unterauftragnehmer durchgeführt werden.[19] Der Vertrag sollte bei einer Verletzung der Datenschutzbestimmungen Vertragsstrafen gegen den Anbieter oder den Unterauftragnehmer vorsehen.

3.4.1.3 Löschung von Daten

Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG sieht vor, dass personenbezogene Daten nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Personenbezogene Daten, die nicht länger benötigt werden, müssen gelöscht oder wirklich anonymisiert werden. Wenn solche Daten aufgrund gesetzlicher Aufbewahrungsbestimmungen (z. B. Steuerbestimmungen) nicht gelöscht werden können, sollte der Zugang zu diesen personenbezogenen Daten gesperrt werden. Es obliegt der Verantwortung des Cloud-Anwenders, sicherzustellen, dass personenbezogene Daten gelöscht werden, sobald sie nicht mehr in dem vorgenannten Sinn erforderlich sind[20].

Der Grundsatz der Löschung der Daten gilt für personenbezogene Daten unabhängig davon, ob sie auf der Festplatte oder auf einem anderen Speichermedium (z. B. Backup-Bänder) gespeichert sind. Da personenbezogene Daten möglicherweise zusätzlich auf verschiedenen Servern an unterschiedlichen Orten gespeichert sind, muss sichergestellt werden, dass alle gespeicherten Daten unwiderruflich gelöscht werden (d. h. es müssen auch vorherige Versionen, temporäre Dateien und selbst Dateifragmente gelöscht werden).

Es muss Cloud-Anwendern bewusst sein, dass Logdaten [21], die die Überprüfbarkeit beispielsweise der Speicherung, einer Änderung oder Löschung von Daten

---

19 Vgl. den nachstehenden Abschnitt 3.4.3.

20 Die Löschung von Daten spielt sowohl während der Laufzeit des Cloud Computing-Vertrags, als auch nach Beendigung des Vertrags eine Rolle. Sie ist auch im Fall des Austauschs oder der Streichung eines Unterauftragnehmers von Bedeutung.

21 Anmerkungen zu den Anforderungen an das Protokollieren folgen unter 4.3.4.2.

vereinfachen, auch als personenbezogene Daten der Person gelten können, die die entsprechende Verarbeitung eingeleitet hat.[22]

Eine sichere Löschung personenbezogener Daten erfordert, dass das Speichermedium entweder zerstört oder entmagnetisiert wird oder dass die personenbezogenen Daten durch Überschreiben wirkungsvoll gelöscht werden. Für das Überschreiben personenbezogener Daten sollte eine spezielle Software verwendet werden, die Daten entsprechend einem anerkannten Verfahren vielfach überschreibt.

Der Cloud-Anwender sollte sicherstellen, dass der Cloud-Anbieter eine sichere Löschung im vorgenannten Sinne garantiert und dass der Vertrag zwischen dem Anbieter und dem Anwender eindeutige Bestimmungen zur Löschung personenbezogener Daten enthält[23]. Das gilt auch für Verträge zwischen Cloud-Anbietern und Unterauftragnehmern.

3.4.2 Vertragliche Absicherungsklauseln der Beziehung(en) „für die Verarbeitung Verantwortlicher" – „Auftragsverarbeiter"

Der für die Verarbeitung Verantwortliche hat im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen (Artikel 17 Absatz 2 der Richtlinie 95/46/EG). Artikel 17 Absatz 3 der Richtlinie 95/46/EG legt außerdem fest, dass sie rechtlich dazu verpflichtet sind, einen förmlichen Vertrag mit dem Cloud-Anbieter zu unterzeichnen. Dieser Artikel legt die Anforderung fest, dass ein Vertrag oder Rechtsakt die Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter regelt. Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags oder Rechtsakts und die Anforderungen in Bezug auf technische Maßnahmen und organisatorische Vorkehrungen schriftlich oder in einer anderen Form zu dokumentieren.

In dem Vertrag muss insbesondere mindestens festgelegt werden, dass der Auftragsverarbeiter auf Weisung des für die Verarbeitung Verantwortlichen handeln muss und dass er technische und organisatorische Maßnahmen für einen angemessenen Schutz der personenbezogenen Daten zu ergreifen hat.

---

22 Das heißt, dass angemessene Aufbewahrungsfirsten für Logdateien festgelegt werden müssen und dass Prozesse vorhanden sein müssen, welche die rechtzeitige Löschung oder Anonymisierung dieser Daten sicherstellen.

23 Vgl. den nachstehenden Abschnitt 3.4.3.

Zur Sicherstellung der Rechtssicherheit sollte der Vertrag Folgendes enthalten:

1. detaillierte Angaben zu den Anweisungen des Anwenders (Ausmaß und Modalitäten), die dem Anbieter zu übermitteln sind, insbesondere bezüglich der anzuwendenden Dienstgütevereinbarungen (die objektiv und messbar sein sollten) und der entsprechenden Strafen (finanzieller oder sonstiger Natur, einschließlich der Möglichkeit, den Anbieter im Fall der Nichteinhaltung verklagen zu können).

2. Darlegung der Sicherheitsmaßnahmen, die der Cloud-Anbieter abhängig von den Risiken einhalten muss, die durch die Verarbeitung und die Natur der zu schützenden Daten bestimmt werden. Es ist sehr wichtig, dass konkrete technische und organisatorische Maßnahmen spezifiziert werden, beispielsweise wie die im nachfolgenden Abschnitt 3.4.3 aufgeführten. Dies gilt unbeschadet der Anwendung möglicherweise strengerer Maßnahmen, die nach dem innerstaatlichen Recht des Anwenders vorgesehen sind.

3. Gegenstand und Zeitrahmen des durch den Cloud-Anbieter zu erbringenden Cloud-Dienstes, Umfang, Art und Zweck der Verarbeitung der personenbezogenen Daten durch den Cloud-Anbieter sowie die Arten der personenbezogenen Daten, die verarbeitet werden.

4. Spezifizierung der Bedingungen für die Rückgabe der (personenbezogenen) Daten oder für die Zerstörung der Daten bei Beendigung der Diensteerbringung. Darüber hinaus muss sichergestellt werden, dass die personenbezogenen Daten auf Antrag des Cloud-Anwenders zuverlässig gelöscht werden.

5. Einschluss einer Vertraulichkeitsklausel, die sowohl für den Cloud-Anbieter als auch für alle seine Angestellten verbindlich ist, die Zugang zu den Daten haben. Ausschließlich autorisierte Personen dürfen Zugang zu den Daten haben.

6. Verpflichtung von Seiten des Anbieters, den Anwender zu unterstützen, so dass die betroffenen Personen ihre Rechte auf Zugang, Berichtigung und Löschung ihrer Daten leichter ausüben können.

7. In dem Vertrag sollte ausdrücklich festgelegt werden, dass der Cloud-Anbieter die Daten keinem Dritten mitteilen darf – auch nicht zu Zwecken der Aufbewahrung – sofern die Hinzuziehung von Unterauftragnehmern nicht vertraglich geregelt ist. Der Vertrag sollte festlegen, dass Unterauftragsverarbeiter ausschließlich auf der Grundlage einer Einwilligung beauftragt werden dürfen, die der für die Verarbeitung Verantwortliche generell erteilen kann. Der Auftragsverarbeiter ist eindeutig dazu verpflichtet, den für die Verarbeitung Verantwortlichen über beabsichtigtediesbezügliche Änderungen zu informieren. Der für die Verarbeitung Verantwortliche hat dabei jederzeit die

Möglichkeit, solchen Änderungen zu widersprechen oder den Vertrag zu beenden. Der Cloud-Anbieter sollte eindeutig dazu verpflichtet sein, alle beauftragten Unterauftragnehmer zu nennen (z. B. in einem öffentlichen digitalen Register). Es muss sichergestellt werden, dass Verträge zwischen dem Cloud-Anbieter und dem Unterauftragnehmer die Bestimmungen des Vertrags zwischen dem Cloud-Anwender und dem Cloud-Anbieter widerspiegeln (d. h., dass Unterauftragsverarbeiter denselben vertraglichen Verpflichtungen unterliegen wie der Cloud-Anbieter). Es muss insbesondere garantiert werden, dass sowohl der Cloud-Anbieter als auch alle Unterauftragnehmer ausschließlich auf Weisung des Cloud-Anwenders handeln. Wie in dem Abschnitt über die Vergabe von Unteraufträgen erklärt wurde, sollte die Haftungskette in dem Vertrag klar festgelegt werden. Der Vertrag sollte den Auftragsverarbeiter verpflichten, internationalen Übermittlungen einen Rahmen zu geben, beispielsweise durch die Unterzeichnung von Verträgen mit den Unterauftragsverarbeitern, die auf den Standardvertragsklauseln aus 2010/87/EU basieren.

8. Klarstellung der Verantwortung des Cloud-Anbieters auf Benachrichtigung des Cloud-Anwenders im Falle einer Datenschutzverletzung, welche die Daten des Cloud-Anwenders betrifft.

9. Verpflichtung des Cloud-Anbieters, eine Liste der Standorte bereitzustellen, an denen die Daten möglicherweise verarbeitet werden.

10. Das Recht des für die Verarbeitung Verantwortlichen auf Überwachung und die entsprechende Pflicht des Cloud-Anbieters zur Zusammenarbeit.

11. Es sollte vertraglich festgelegt werden, dass der Cloud-Anbieter dazu verpflichtet ist, den Anwender über einschlägige Änderungen bei den jeweiligen Cloud-Diensten zu informieren, wie beispielsweise über die Implementierung zusätzlicher Funktionen.

12. Der Vertrag sollte die Protokollierung und Prüfung der relevanten Verarbeitungstätigkeiten an personenbezogenen Daten festlegen, die durch den Cloud-Anbieter oder die Unterauftragnehmer durchgeführt werden.

13. Benachrichtigung des Cloud-Anwenders über alle rechtlich verbindlichen Ersuchen einer Strafverfolgungsbehörde auf Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen.

14. eine generelle Verpflichtung des Anbieters zur Zusicherung, dass seine interne Organisation und seine Maßnahmen zur Datenverarbeitung (und die seiner

Unterauftragsverarbeiter, sofern vorhanden) die anzuwendenden nationalen und internationalen rechtlichen Anforderungen und Standards einhalten.

Im Falle einer Verletzung durch den für die Verarbeitung Verantwortlichen hat jede Person, die aufgrund der unrechtmäßigen Verletzung einen Schaden erlitten hat, das Recht auf Begleichung der verursachten Schäden durch den für die Verarbeitung Verantwortlichen. Sollte der Auftragsverarbeiter die Daten für einen anderen Zweck nutzen oder sie verbreiten oder auf eine vertragsverletzende Weise nutzen, wird er auch als für die Verarbeitung Verantwortlicher angesehen und ist für die Vertragsverletzungen haftbar, in die er persönlich verwickelt war.

Es sollte angemerkt werden, dass Anbieter von Cloud-Diensten in vielen Fällen Standarddienste und von den für die Verarbeitung Verantwortlichen zu unterzeichnende Standardverträge anbieten, die ein Standardformat für die Verarbeitung personenbezogener Daten festlegen. Das Ungleichgewicht in der Vertragsposition zwischen einem kleinen für die Verarbeitung Verantwortlichen und großen Dienstleistern darf nicht als Rechtfertigung dafür gelten, dass für die Verarbeitung Verantwortliche Vertragsklauseln und -bedingungen akzeptieren, die gegen das Datenschutzrecht verstoßen.

3.4.3 Technische und organisatorische Maßnahmen des Datenschutzes und der Datensicherheit

Artikel 17 Absatz 2 der Richtlinie 95/46/EG macht den Cloud-Anwender (der als für die Datenverarbeitung Verantwortlicher handelt) allein verantwortlich für die Wahl von Cloud-Anbietern, die hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bieten und Rechenschaft ablegen können.

Zusätzlich zu den wichtigsten Sicherheitszielen der Verfügbarkeit, Vertraulichkeit und Integrität muss die Aufmerksamkeit auch auf die zusätzlichen Datenschutzziele der Transparenz (siehe vorstehenden Punkt 3.4.1.1) Isolierung[24], Intervenierbarkeit, Rechenschaft und Portabilität gerichtet werden. Dieser Abschnitt richtet das Augenmerk unbeschadet zusätzlicher sicherheitsorientierter Risikoanalysen[25] auf diese zentralen Datenschutzziele.

3.4.3.1 Verfügbarkeit

Die Bereitstellung von Verfügbarkeit bedeutet, den zeitnahen und zuverlässigen Zugang zu personenbezogenen Daten sicherzustellen.

---

[24] In Deutschland wurde der breitere Begriff der „Unverkettbarkeit“ in das Recht eingeführt und wird von der Konferenz der Datenschutzbeauftragten unterstützt.

[25] Vgl. z. B. ENISA unter http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

Eine große Gefahr für die Verfügbarkeit in der Cloud ist der versehentliche Verlust der Netzwerkverbindung zwischen dem Kunden und dem Anbieter der Serverleistung durch böswillige Handlungen wie (Distributed) Denial of Service (DoS)[26]-Angriffe. Zu den weiteren Verfügbarkeitsrisiken zählen versehentliche Hardware-Ausfälle sowohl im Netzwerk als auch in den Verarbeitungs- und Speichersystemen der Cloud, Stromausfälle und sonstige Infrastrukturprobleme.

Für die Datenverarbeitung Verantwortliche sollten prüfen, ob der Cloud-Anbieter angemessene Maßnahmen ergriffen hat, um dem Risiko der Störungen zu begegnen. Zu diesen Maßnahmen zählen unter anderem Backup-Internet-Netzwerkverbindungen, redundante Speicherung und wirksame Mechanismen zum Daten-Backup.

3.4.3.2 Integrität

Integrität kann definiert werden als Eigenschaft, dass die Daten authentisch sind und nicht böswillig oder versehentlich während der Verarbeitung, Aufbewahrung oder Übermittlung geändert wurden. Der Begriff der Integrität kann auf IT-Systeme ausgeweitet werden und erfordert, dass die Verarbeitung personenbezogener Daten auf diesen Systemen unverändert bleibt.

Änderungen an personenbezogenen Daten können durch Mechanismen der kryptografischen Authentifizierung wie Message Authentication Codes oder Signaturen entdeckt werden.

Störungen der Integrität von IT-Systemen in der Cloud können mit Hilfe von Intrusion Detection und Intrusion Prevention Systemen (IDS / IPS) entdeckt bzw. verhindert werden. Das ist besonders bei der Art offener Netzwerkumgebung erforderlich, in der Clouds normalerweise betrieben werden.

3.4.3.3 Vertraulichkeit

Korrekt ausgeführt kann die Verschlüsselung in der Cloud-Umgebung maßgeblich zur Vertraulichkeit personenbezogener Daten beitragen, auch wenn sie personenbezogene Daten nicht unwiderruflich anonymisiert[27]. Personenbezogene Daten sollten während des „Transits“ immer verschlüsselt sein und „ruhende

---

[26] Ein DoS-Angriff ist ein koordinierter Versuch, die Verfügbarkeit eines Computers oder einer Netzwerkressource für die autorisierten Nutzer entweder vorübergehend oder dauerhaft zu unterbinden (z. B. mittels einer großen Anzahl von angreifenden Systemen, die ihr Ziel mit einer Vielzahl von externen Kommunikationsanforderungen blockieren).

[27] Richtlinie 95/46/EG – Erwägungsgrund 26: „(…) Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. (…)“ Gleichermaßen führen die technischen Datenfragmentierungsprozesse, die im Rahmen der Bestimmungen von Cloud Computing-Diensten genutzt werden können, nicht zu einer unwiderbringlichen Anonymisierung der Daten und implizieren folglich nicht, dass die Datenschutzvorschriften keine Anwendung finden.

Daten“ sofern möglich.[28] In einigen Fällen (z. B. in einem IaaS Speicherdienst) kann sich ein Cloud-Anwender möglicherweise nicht auf die Verschlüsselungslösung verlassen, die der Cloud-Anbieter anbietet, sondern wird sich eventuell entscheiden, personenbezogene Daten zu verschlüsseln, bevor er sie in die Cloud sendet. Werden ruhende Daten verschlüsselt, muss besondere Aufmerksamkeit auf die Verwaltung der kryptografischen Schlüssel gerichtet werden, da die Datensicherheit dann letztendlich von der Vertraulichkeit der Schlüssel für die Verschlüsselung abhängt.

Mitteilungen zwischen dem Cloud-Anbieter und dem Anwender sowie zwischen den Datenzentren sollten verschlüsselt werden. Die Fernverwaltung der Cloud-Plattform sollte nur über sichere Kommunikationskanäle erfolgen. Wenn ein Anwender nicht nur die Aufbewahrung, sondern auch die weitere Verarbeitung personenbezogener Daten in der Cloud plant (z. B. Suchdatenbanken für Datensätze), muss er daran denken, dass die Verschlüsselung während der Verarbeitung der Daten nicht aufrecht erhalten werden kann (mit Ausnahme sehr spezieller Berechnungsmethoden).

Weitere technische Maßnahmen zur Sicherstellung der Vertraulichkeit umfassen Autorisierungsmechanismen und die sichere Authentifizierung (z. B. Zwei-Faktor-Authentifizierung). Die Vertragsklauseln sollten auch den Angestellten von Cloud-Anwendern, Cloud-Anbietern und Unterauftragnehmern die Verpflichtung zur Vertraulichkeit auferlegen.

3.4.3.4 Transparenz

Die technischen und organisatorischen Maßnahmen müssen die Transparenz unterstützen, so dass eine Überprüfung möglich ist. Vgl. 3.4.1.1.

3.4.3.5 Isolierung (Zweckbegrenzung)

In Cloud-Infrastrukturen teilen sich viele Mieter Ressourcen wie Aufbewahrung, Speicher und Netzwerke. Das schafft neue Risiken in Bezug auf die Offenlegung oder Weiterverarbeitung der Daten für illegale Zwecke. Das Schutzziel „Isolierung“ soll dieses Problem angehen und dazu beitragen, dass Daten nicht über ihren ursprünglichen Zweck hinaus verwendet werden (Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG) und dass die Vertraulichkeit und Integrität gewahrt bleiben.[29]

---

[28] Das gilt insbesondere für die Datenverarbeitung Verantwortliche, die eine Übermittlung sensibler Daten im Sinne von Artikel 8 der Richtlinie 95/46/EG (z. B. Gesundheitsdaten) oder von dem Berufsgeheimnis unterliegenden Daten in die Cloud planen.

[29] Vgl. 3.4.1.2.

Damit eine Isolierung erreicht werden kann, ist zuerst eine adäquate Kontrolle der Rechte und Rollen für den Zugang zu den personenbezogenen Daten erforderlich. Es ist eine regelmäßigeÜberprüfung durchzuführen. Die Einführung von Funktionen mit sehr großen Privilegien sollte vermieden werden (so sollte kein Anwender oder Administrator für die gesamte Cloud zugangsberechtigt sein). Allgemeiner gesagt: Administratoren und Anwender dürfen nur Zugang zu den Informationen haben, die sie für die rechtmäßige Zweckerfüllung benötigen (Least Privilege Prinzip).

Zweitens hängt die Isolierung auch von technischen Maßnahmen wie dem Verstärken der Hypervisoren und einer richtigen Verwaltung gemeinsam genutzter Ressourcen ab, wenn virtuelle Maschinen genutzt werden, um physische Ressourcen gemeinsam mit verschiedenen Cloud-Anwendern zu nutzen.

3.4.3.5 Intervenierbarkeit

Richtlinie 95/46/EG gibt der betroffenen Person das Recht auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch (vgl. Artikel 12 und 14). Der Cloud-Anwender muss überprüfen, dass der Cloud-Anbieter diesen Anforderungen keine technischen und organisatorischen Hürden auferlegt. Dies gilt auch für die Fälle, in denen die Daten von Unterauftragnehmern weiterverarbeitet werden.

Der Vertrag zwischen dem Anwender und dem Anbieter sollte festlegen, dass der Cloud-Anbieter dazu verpflichtet ist, den Anwender dahingehend zu unterstützen, dass die Ausübung der Rechte der betroffenen Person vereinfacht wird. So muss auch sichergestellt werden, dass dies auch für seine Beziehung zu jedem Unterauftragnehmer gilt.[30]

3.4.3.6 Portabilität

Derzeit nutzen die wenigsten Cloud-Anbieter Standard-Datenformate und Service-Schnittstellen, die die Interoperabilität und Portabilität zwischen verschiedenen Cloud-Anbietern vereinfachen. Wenn ein Cloud-Anwender entscheidet, von einem Cloud-Anbieter zu einem anderen zu migrieren, kann dieser Mangel an Interoperabilität dazu führen, dass der Transfer der (personenbezogenen) Daten des Anwenders zu einem neuen Cloud-Anbieter unmöglich oder zumindest schwierig ist (sogenanntes Vendor Lock-in). Das gilt auch für Dienste, die der Anwender auf einer Plattform entwickelt hat, die von dem ursprünglichen Cloud-

[30] Vgl. den vorstehenden Abschnitt 3.4.2 Nr. 6. Der Anbieter kann sogar dazu instruiert werden, Anfragen im Namen des Anwenders zu beantworten.

Anbieter angeboten wurden (PaaS). Der Cloud-Anwender sollte vor Buchen eines Cloud-Dienstes prüfen, ob und wie der Anbieter die Portabilität der Daten und Leistungen garantiert.[31]

3.4.4.7 Rechenschaftspflicht

Im IT-Bereich kann Rechenschaft als die Fähigkeit definiert werden, festzustellen, was eine Entität zu einem bestimmten Zeitpunkt in der Vergangenheit gemacht hat und wie sie es getan hat. Im Bereich des Datenschutzes ist die Bedeutung meist weiter gefasst und beschreibt die Fähigkeit der Parteien, nachzuweisen, dass sie angemessene Schritte zur Umsetzung der Datenschutzgrundsätze unternommen haben.

Rechenschaft in der Informationstechnik ist besonders wichtig für die Ermittlung von Datenschutzverletzungen im Bereich personenbezogener Daten, wo der Cloud-Anwender, der Anbieter und der Unterauftragsverarbeiter je einen Teil der operativen Verantwortung tragen können. Diesbezüglich ist die Fähigkeit der Cloud-Plattform, eine verlässliche Überwachung und verständliche Protokollierungs-Mechanismen zu bieten, von größter Bedeutung.

Darüber hinaus sollten die Cloud-Anbieter durch die Vorlage von entsprechenden Schriftstücken nachweisen, dass sie die in den vorstehenden Abschnitten aufgeführten Datenschutzgrundsätze mittels angemessener und effektiver Maßnahmen umgesetzt haben. Beispiele für solche Maßnahmen sind Verfahren zur Sicherstellung der Identifizierung aller Datenverarbeitungsschritte, die Beantwortung von Auskunftsersuchen, die Zuweisung von Ressourcen einschließlich der Ernennung von Datenschutzbeauftragten, die für die Organisation der Einhaltung der Datenschutzbestimmungen zuständig sind oder unabhängige Zertifizierungsverfahren. Darüber hinaus sollten die für die DatenverarbeitungVerantwortlichen sicherstellen, dass sie gegenüber der zuständigen Überwachungsbehörde jederzeit auf Anfrage die notwendigen Maßnahmen nachweisen können.[32]

3.5 Internationale Übermittlungen

Artikel 25 und 26 der Richtlinie 95/46/EG sehen den freien Verkehr personenbezogener Daten in Länder außerhalb des EWR nur dann vor, wenn das Land

---

31 Der Anbieter sollte vorzugsweise standardisierte oder offene Datenformate und Schnittstellen nutzen. Es sollten auf jeden Fall Vertragsklauseln vereinbart werden, die gesicherte Formate, die Erhaltung logischer Beziehungen und die Kosten der Migration zu einem anderen Cloud-Anbieter festlegen.

32 Die Arbeitsgruppe hat in ihrer Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht detaillierte Ausführungen zur Rechenschaftspflicht vorgelegt
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_de.pdf.

oder der Empfänger ein angemessenes Datenschutzniveau bietet. Andernfalls sind von dem für die Verarbeitung Verantwortlichen und seinen für die Verarbeitung Mitverantwortlichen und/oder den Auftragsverarbeitern besondere Garantien einzurichten. Cloud Computing basiert jedoch meistens auf dem vollständigen Fehlen eines festen Standorts, an dem sich die Daten innerhalb des Netzwerks des Cloud-Anbieters befinden. Die Daten können um 14.00 Uhr in dem einen Datenzentrum sein und um 16.00 Uhr in einem anderen Datenzentrum am anderen Ende der Welt. Der Cloud-Anwender kann deshalb nur selten in Echtzeit wissen, wo sich die Daten befinden, wo sie gespeichert oder übermittelt werden. In diesem Zusammenhang sind die traditionellen Rechtsinstrumente zur Bereitstellung eines Rahmens zur Regulierung der Datenübermittlungen in Drittländer außerhalb der EU, die keinen angemessenen Schutz bieten, eingeschränkt.

3.5.1 Safe Harbor und angemessene Länder

Die Angemessenheit des Schutzniveaus, einschließlich Safe Harbor sind in Bezug auf den geografischen Anwendungsbereich eingeschränkt und decken folglich nicht alle Übermittlungen in der Cloud ab. Übermittlungen an US-amerikanische Organisationen, die sich an die Grundsätze halten, können rechtmäßig unter EU-Recht stattfinden, da davon ausgegangen wird, dass die Empfängerorganisationen ein angemessenes Schutzniveau für die übermittelten Daten bieten.

Die Arbeitsgruppe vertritt jedoch die Ansicht, dass allein die Selbstzertifizierung nach dem Safe Harbor Abkommen bei einem gleichzeitigen Fehlen der tatsächlichen Durchsetzung der Datenschutzgrundsätze in der Cloud-Umgebung nicht als ausreichend angesehen werden kann. Darüber hinaus verlangt Artikel 17 der EU-Richtlinie, dass zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter für die Verarbeitungszwecke ein Vertrag unterzeichnet wird. Dies wird in FAQ 10 der EU-US Safe Harbor Rahmendokumente bestätigt. Dieser Vertrag unterliegt nicht der vorherigen Genehmigung durch die europäischen Datenschutzbehörden. Ein solcher Vertrag spezifiziert die durchzuführende Verarbeitung und alle Maßnahmen, die erforderlich sind, damit die sichere Aufbewahrung der Daten sichergestellt ist. Einige nationale Bestimmungen und Datenschutzbehörden können zusätzliche Anforderungen stellen.

Die Arbeitsgruppe ist der Ansicht, das sich Daten exportierende Unternehmen nicht nur auf die Erklärung des Datenimporteurs verlassen sollten, dass er eine Safe-Harbor-Zertifizierung hat. Stattdessen sollte das Daten exportierende Unternehmen einen Nachweis erhalten, dass die Safe Harbor Selbstzertifizierung vorliegt und einen Nachweis fordern, dass die Grundsätze wirklich befolgt wer-

den. Das ist besonders wichtig in Bezug auf die Informationen, die den von der Datenverarbeitung betroffenen Personen erteilt werden[33] [34].

Die Arbeitsgruppe ist auch der Ansicht, dass der Cloud-Anwender überprüfen muss, ob die von Cloud-Anbietern aufgesetzten Standardverträge den nationalen Anforderungen im Hinblick auf die vertragliche Datenverarbeitung entsprechen. Die nationalen Anforderungen können möglicherweise verlangen, dass die Vergabe von Unteraufträgen im Vertrag definiert wird. Dazu gehören die Standorte und andere Daten zu den Unterauftragsverarbeitern sowie die Nachverfolgbarkeit der Daten. Normalerweise bieten die Cloud-Anbieter den Anwendern diese Informationen nicht – ihre Verpflichtung zu den Safe-Harbor-Grundsätzen kann das Fehlen der vorgenannten Garantien nicht ersetzen, wenn diese in den nationalen Rechtsvorschriften gefordert werden. In solchen Fällen wird der Exporteur dazu aufgefordert, andere verfügbare Rechtsinstrumente zu nutzen, wie beispielsweise Standardsvertragsklauseln oder verbindliche unternehmensinterne Vorschriften.

Schließlich vertritt die Arbeitsgruppe die Ansicht, dass die Safe-Harbor-Grundsätze an sich dem Daten-Exporteur nicht die erforderlichen Mittel garantieren, um sicherstellen zu können, dass von dem Cloud-Anbieter in den USA angemessene Sicherheitsmaßnahmen angewendet wurden, wie es möglicherweise von den nationalen Rechtsvorschriften basierend auf Richtlinie 95/46/EC[35] gefordert wird. Im Hinblick auf die Datensicherheit führt Cloud Computing zu einigen Cloud-spezifischen Sicherheitsrisiken, wie den Verlust der Kontrolle, ein unsicheres oder unvollständiges Löschen der Daten, unzureichende Prüfpfade oder Fehler bei der Isolierung[36], die durch die bestehenden Safe Harbor Grundsätze zum Datenschutz nicht ausreichend behandelt werden[37]. Es können also zusätzliche Garantien zur Datensicherheit eingesetzt werden, wie durch die Einbindung des Fachwissens und der Ressourcen von Dritten, die dazu befähigt sind, die Angemessenheit des Cloud-Anbieters durch verschiedene Prüfungs-, Standardisierungs- und Zertifizierungssysteme zu bewerten[38]. Aus diesen Gründen könnte es empfehlenswert sein, die Verpflichtung des Datenimporteurs zu den Safe Harbor Grundsätzen mit zusätzlichen Garantien zu vervollständigen, die die besondere Natur der Cloud berücksichtigen.

---

33 Siehe die deutsche Datenschutzbehörde.
http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

34 Für die Anforderungen in Bezug auf Verträge mit Unterauftragsverarbeitern siehe 3.3.2.

35 Siehe die Stellungnahme der dänischen Datenschutzbehörde.
http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Detailliert in dem ENISA-Papier zum Cloud Computing beschrieben: Vorteile, Risiken und Empfehlungen der Informationssicherheit unter:
https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 „Organisationen müssen angemessene Vorkehrungen treffen, um personenbezogene Informationen vor Verlust, Missbrauch und unautorisiertem Zugriff, vor Offenlegung, Änderung und Zerstörung zu schützen."

38 Siehe nachfolgenden Abschnitt 4.2.

3.5.2 Ausnahmen

Die Ausnahmen gemäß Artikel 26 der Richtlinie 95/46/EG ermöglichen Datenexporteuren dieÜbermittlung von Daten aus der EU ohne dass sie zusätzliche Garantien bereitstellen. Die WP29 hat jedoch eine Stellungnahme angenommen, in welcher sie die Ansicht vertritt, dass Ausnahmen nur dann anwendbar sein sollten, wenn die Übermittlungen weder wiederkehrend noch in großem Umfang oder strukturell sind.[39]

Basierend auf solchen Auslegungen ist es fast unmöglich, sich im Zusammenhang mit Cloud Computing auf Ausnahmen zu verlassen.

3.5.3 Standardvertragsklauseln

Standardvertragsklauseln wie die von der EU-Kommission angenommenen, mit denen internationalen Datenübermittlungen zwischen zwei für die Verarbeitung Verantwortlichen oder einem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter ein Rahmen gegeben werden soll, basieren auf einem bilateralen Ansatz. Wenn der Cloud-Anbieter als Auftragsverarbeiter angesehen wird, sind Standardklauseln nach dem Kommissionsbeschluss 2010/87/EG ein Instrument, das zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen als eine Grundlage in der Cloud Computing-Umgebung herangezogen werden kann, um angemessene Garantien im Zusammenhang mit internationalen Übermittlungen zu bieten.

Die Arbeitsgruppe vertritt die Ansicht, dass der Cloud-Anbieter den Kunden zusätzlich zu den Standardvertragsklauseln Bestimmungen anbieten könnte, die auf ihren pragmatischen Erfahrungen basieren, solange diese nicht direkt oder indirekt den von der Kommission bewilligten Standardvertragsklauseln widersprechen oder Grundrechte oder -freiheiten der betroffenen Personen beeinträchtigen[40]. Dennoch können Unternehmen die Standardvertragsklauseln nicht ergänzen oder ändern, ohne dass dies bedeutet, dass die Bestimmungen nicht mehr länger „Standard“[41] sind.

Wenn der als Auftragsverarbeiter agierende Cloud-Anbieter in der EU niedergelassen ist, könnte die Situation noch komplexer sein, da die Musterklauseln im

---

39 Arbeitsunterlage 12/1998: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU. Von der Arbeitsgruppe am 24. Juli 1998 angenommen (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf).

40 Siehe FAQ IV Bl.9 9, Can companies include the standard contractual clauses in a wider contract and add specific clauses? veröffentlicht von der EG unter http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 Siehe FAQ IV B1.10, Can Companies amend and change the standard contractual clauses approved by the Commission?

Allgemeinen nur auf Datenübermittlungen von einem für die Verarbeitung Verantwortlichen in der EU an einen Auftragsverarbeiter außerhalb der EU Anwendung finden (siehe Erwägungsgrund 23 des Kommissionsbeschlusses 2010/87/EU über Standardvertragsklauseln und WP 176).

Bezüglich der vertraglichen Beziehungen zwischen einem nicht in der EU ansässigen Auftragsverarbeiter und den Unterauftragsverarbeitern sollte eine schriftliche Vereinbarung getroffen werden, die dem Unterauftragsverarbeiter dieselben Verpflichtungen auferlegt, die dem Auftragsverarbeiter auferlegt würden, fänden die Musterklauseln Anwendung.

3.5.4 Verbindliche unternehmensinterne Vorschriften: in Richtung eines globalen Ansatzes

Verbindliche unternehmensinterne Vorschriften sind ein Verhaltenskodex für Unternehmen, die Daten innerhalb ihrer Gruppe übermitteln. Ist der Anbieter ein Auftragsverarbeiter, werden solche Lösungen auch im Kontext des Cloud Computing bereitgestellt. Derzeit arbeitet die WP 29 an verbindlichen unternehmensinternen Vorschriften für Auftragsverarbeiter, die die Übermittlung innerhalb der Gruppe zugunsten der für die Verarbeitung Verantwortlichen ermöglichen, ohne dass für jeden Anwender ein Vertrag zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter unterzeichnet werden muss.[42]

Solche verbindlichen unternehmensinternen Vorschriften für Auftragsverarbeiter würden es dem Kunden des Anbieters ermöglichen, dem Auftragsverarbeiter seine personenbezogenen Daten anzuvertrauen und dabei sicher zu sein, dass für die innerhalb des Geschäftsbereichs des Anbieters übermittelten Daten ein angemessenes Schutzniveau besteht.

4. Schlussfolgerungen und Empfehlungen

Unternehmen und Verwaltungen, die Cloud Computing nutzen wollen, sollten als ersten Schritt eine umfassende und gründliche Risikoanalyse durchführen. Diese Analyse muss unter Berücksichtigung der Art der in der Cloud verarbeiteten Daten die Risiken untersuchen, die mit der Verarbeitung der Daten in der Cloud einhergehen (fehlende Kontrolle und unzureichende Informationen – siehe Abschnitt 2 oben).[43] Es sollte besondere Aufmerksamkeit auf die Bewer-

[42] Siehe Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, angenommen am 6. Juni 2012: http://ec.europa.eu/justice/data protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

[43] Die ENISA stellt eine Liste der Risiken bereit, die berücksichtigt werden müssen http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

tung der rechtlichen Risiken in Bezug auf den Datenschutz gelegt werden, die in erster Linie Sicherheitsvorschriften und internationale Übermittlungen betreffen. Die Verarbeitung sensibler Daten mittels Cloud Computing weckt zusätzliche Bedenken. Unbeschadet nationaler Rechtsvorschriften erfordern solche Verarbeitungen folglich zusätzliche Garantien.[44] Die nachstehenden Schlussfolgerungen sollen eine Checkliste für die Einhaltung des Datenschutzes durch Cloud-Anwender und Cloud-Anbieter bieten. Sie basieren auf dem aktuellen Rechtsrahmen. Einige Empfehlungen werden auch angesichts zukünftiger Entwicklungen in den Rechtsvorschriften auf EU-Ebene und darüber hinaus erteilt.

4.1 Leitlinien für Anwender und Anbieter von Cloud Computing-Diensten

– Beziehung „für die Verarbeitung Verantwortlicher – Auftragsverarbeiter“: Diese Stellungnahme konzentriert sich auf die Anwender-Anbieter-Beziehung als Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter (siehe Abschnitt 3.3.1). Basierend auf konkreten Umständen kann es jedoch Situationen geben, in denen der Cloud-Anbieter auch als für die Verarbeitung Verantwortlicher fungiert, beispielsweise, wenn der Anbieter einige personenbezogene Daten für seine eigenen Zwecke erneut verarbeitet. In einem solchen Fall trägt der Cloud-Anbieter die vollständige (gemeinsame) Verantwortung für die Verarbeitung und muss alle rechtlichen Verpflichtungen erfüllen, die in den Richtlinien 95/46/EG und 2002/58/EG niedergelegt sind (sofern anwendbar).

– Die Verantwortung des Cloud-Anwenders als für die Verarbeitung Verantwortlicher: Der Kunde als der für die Verarbeitung Verantwortliche muss die Verantwortung für die Einhaltung der Datenschutzvorschriften übernehmen und unterliegt allen rechtlichen Verpflichtungen, die in den Richtlinien 95/46/EG und 2002/58/EG niedergelegt sind (sofern anwendbar). Dies gilt insbesondere gegenüber den betroffenen Personen (siehe 3.3.1). Der Anwender sollte sich für einen Cloud-Anbieter entscheiden, der die Einhaltung der EU-Datenschutzvorschriften garantiert, wie sie in den nachfolgend zusammengefassten vertraglichen Garantien wiedergegeben werden.

– Garantien bei der Untervergabe: In jedem Vertrag zwischen dem Cloud-Anbieter und dem Cloud-Anwender sollten Bestimmungen für Unterauftragnehmer enthalten sein. Der Vertrag sollte festlegen, dass Unterauftragsverarbeiter ausschließlich auf der Grundlage einer Einwilligung beauftragt werden dürfen, die der für die Verarbeitung Verantwortliche generell erteilen kann.

[44] Siehe Sopot-Memorandum, vgl. Fußnote 2 oben.

Gleichzeitig ist der Auftragsverarbeiter eindeutig dazu verpflichtet, den für die Verarbeitung Verantwortlichen über diesbezügliche beabsichtigte Änderungen zu informieren. Der für die Verarbeitung Verantwortliche hat jederzeit die Möglichkeit, solchen Änderungen zu widersprechen oder den Vertrag zu beenden. Der Cloud-Anbieter sollte eindeutig dazu verpflichtet sein, alle beauftragten Unterauftragnehmer zu nennen. Der Cloud-Anbieter sollte mit jedem Unterauftragnehmer einen Vertrag unterzeichnen, der die Vereinbarungen mit dem Cloud-Anwender wiedergibt. Der Anwender sollte sicherstellen, dass er im Fall von Vertragsverletzungen durch die Unterauftragnehmer des Anbieters Regress nehmen kann (siehe 3.3.2).

– Einhaltung der grundlegenden Datenschutzgrundsätze:

  • Transparenz (siehe 3.4.1.1): Cloud-Anbieter sollten die Cloud-Anwender während der Vertragsverhandlungen über alle (datenschutzrechtlich) relevanten Aspekte ihrer Dienste informieren. Die Anwender sollten insbesondere über alle Unterauftragnehmer informiert sein, die zur Bereitstellung des jeweiligen Cloud-Dienstes beitragen und über alle Orte, an denen Daten vom Cloud-Anbieter und/oder seinen Unterauftragnehmern aufbewahrt oder verarbeitet werden können (insbesondere, wenn sich einige oder alle der Orte außerhalb des Europäischen Wirtschaftsraums (EWR) befinden). Der Anwender sollte aussagekräftige Informationen über technische und organisatorische Maßnahmen erhalten, die von dem Anbieter umgesetzt wurden. Der Anwender sollte die betroffenen Personen im Sinne einer angemessenen Vorgehensweise über den Cloud-Anbieter und alle Unterauftragnehmer (sofern vorhanden) informieren sowie über die Orte, an denen die Daten von dem Cloud-Anbieter und/oder seinen Unterauftragnehmern möglicherweise aufbewahrt oder verarbeitet werden.

  • Zweckbestimmung und -begrenzung (3.4.1.2): Der Anwender sollte die Einhaltung der Grundsätze der Zweckbestimmung und -begrenzung sicherstellen und garantieren, dass keine Daten von dem Anbieter oder von Unterauftragnehmern für weitere Zwecke verarbeitet werden. Entsprechende Verpflichtungen sollten in angemessenen vertraglichen Maßnahmen (einschließlich technischer und organisatorischer Garantien) festgehalten werden.

  • Datenspeicherung (3.4.1.3): Der Anwender muss sicherstellen, dass personenbezogene Daten (durch den Anbieter und jeden Unterauftragnehmer) von jedem Speicherort gelöscht werden, sobald sie nicht mehr für den bestimmten Zweck benötigt werden. Sichere Mechanismen zur Löschung (Zerstörung, Entmagnetisierung, Überschreiben) sollten vertraglich festgelegt werden.

– Vertragliche Garantien (siehe 3.4.2, 3.4.3 und 3.4.5):

  • Generell sollten der Vertrag mit dem Anbieter (und die Verträge, die zwischen dem Anbieter und den Unterauftragnehmern geschlossen werden) ausreichende Garantien in Bezug auf die technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen (gemäß Artikel 17 Absatz 2 der Richtlinie) enthalten und schriftlich oder in einer anderen angemessenen Form vorliegen. Der Vertrag sollte die Anweisungen des Anwenders an den Anbieter genau beschreiben, einschließlich des Gegenstands und Zeitrahmens des Dienstes, des Ziels und der messbaren Servicelevel und der entsprechenden Strafen (finanzieller oder sonstiger Natur). Er sollte die Sicherheitsmaßnahmen aufführen, die abhängig von den Risiken der Verarbeitung und der Natur der Daten und gemäß den nachfolgenden Anforderungen und vorbehaltlich strengerer Maßnahmen durchzuführen sind, die im nationalen Recht des Kunden vorgesehen sind. Wenn Cloud-Anbieter Standardvertragsklauseln nutzen wollen, sollten sie sicherstellen, dass die Bestimmungen die Datenschutzvorschriften einhalten (siehe 3.4.2). In den entsprechenden Vertragsbedingungen sollten insbesondere die technischen und organisatorischen Maßnahmen genau dargelegt werden, die vom Anbieter umgesetzt wurden.

  • Zugang zu den Daten: Nur autorisierte Personen sollten Zugang zu den Daten haben. Der Vertrag sollte in Bezug auf den Anbieter und seine Angestellten eine Vertraulichkeitsvereinbarung enthalten.

  • Offenlegung der Daten gegenüber Dritten: Dies sollte vertraglich geregelt sein. Der Anbieter sollte in dem Vertrag dazu verpflichtet werden, alle seine Unterauftragnehmer zu nennen – beispielsweise in einem öffentlichen digitalen Register – und sicherzustellen, dass der Anwender jederzeit Zugang zu den die Änderungen betreffenden Informationen hat, so dass er diesen Änderungen widersprechen oder den Vertrag beenden kann. Der Vertrag sollte den Anbieter auch dazu verpflichten, jede rechtlich verbindliche Anfrage auf Offenlegung personenbezogener Daten durch eine Strafverfolgungsbehörde zu melden, sofern eine solche Offenlegung nicht anderweitig verboten ist. Der Anwender sollte gewährleisten, dass der Anbieter jede Anfrage auf Offenlegung ablehnt, die nicht rechtlich verbindlich ist.

  • Verpflichtung zur Kooperation: Der Anwender sollte sicherstellen, dass der Anbieter zur Kooperation in den folgenden Bereichen verpflichtet ist: Recht des Anwenders auf Überwachung der Verarbeitung, Vereinfachung der Ausübung des Rechts der betroffenen Personen auf Zugang/Berichtigung/Löschung ihrer Daten und (sofern anwendbar) Benachrichtigung des Cloud-Anwender über alle Datenschutzverletzungen, die die Daten des Anwenders betreffen.

- Grenzüberschreitende Datenübermittlungen: Der Cloud-Anwender sollte überprüfen, ob der Cloud-Anbieter die Rechtmäßigkeit grenzüberschreitender Datenübermittlungen garantieren und die Übermittlungen, wenn möglich, auf Länder beschränken kann, die der Anwender ausgewählt hat. Übermittlungen in nicht angemessene Drittländer erfordern spezielle Garantien durch die Anwendung von Safe Harbor Vereinbarungen, Standardvertragsklauseln oder verbindlicher unternehmensinterner Vorschriften -je nach Fall. Die Anwendung von Standardvertragsklauseln für Anbieter (gemäß Beschluss der Kommission 2010/87/EG) erfordert gewisse Anpassungen an die Cloud-Umgebung (um zu verhindern, dass für die jeweiligen Anwender getrennte Verträge zwischen einem Anbieter und seinen Unterauftragsverarbeitern bestehen), die möglicherweise vorher durch die zuständige Datenschutzbehörde genehmigt werden müssen. Es sollte eine Liste der Orte zur Verfügung gestellt werden, in welchen die Dienste möglicherweise bereitgestellt werden.

- Protokollieren und Überprüfung der Verarbeitung: Der Anwender sollte verlangen, dass die Verarbeitungsschritte durch den Anbieter und seine Unterauftragnehmer protokolliert werden. Der Anwender sollte dazu befugt sein, diese Verarbeitungsschritte zu überprüfen. Eine Kontrolle und die Zertifizierung durch Dritte, die der für die Verarbeitung Verantwortliche ausgewählt hat, sollten jedoch auch möglich sein, sofern eine vollständige Transparenz garantiert wird (beispielsweise durch Erhalt einer Kopie der Prüfbescheinigung oder des Prüfberichts zur Überprüfung der Zertifizierung).

- Technische und organisatorische Maßnahmen: Diese sollten zur Beseitigung der Risiken dienen, die der in der Cloud-Computing-Umgebung sehr weit verbreitete Mangel an Kontrolle und Informationen nach sich zieht. Die Erstgenannten umfassen Maßnahmen, mit denen die Verfügbarkeit, Integrität, Vertraulichkeit, Isolierung, Intervenierbarkeit und Portabilität in den in der Stellungnahme niedergelegten Definitionen sichergestellt werden sollen während sich die Letztgenannten auf die Transparenz konzentrieren (siehe 3.4.3 für alle Einzelheiten).

4.2 Datenschutz-Zertifizierung durch Dritte

- Eine unabhängige Überprüfung oder Zertifizierung durch einen anerkannten Dritten kann für Cloud-Anbieter ein glaubwürdiges Mittel sein, um ihre Einhaltung der in dieser Stellungnahme niedergelegten Verpflichtungen nachzuweisen. Eine solche Zertifizierung würde mindestens angeben, dass eine anerkannte dritte Organisation anhand anerkannter Standards die Überwachung des Datenschutzes überprüft hat und dass die in dieser Stellungnahme nieder-

gelegten Anforderungen erfüllt werden.[45] Im Bereich des Cloud Computing sollten potenzielle Kunden prüfen, ob die Anbieter der Cloud-Dienste eine Kopie dieser Prüfbescheinigung durch eine dritte Partei oder des Prüfberichts, der die Zertifizierung in Bezug auf die in dieser Stellungnahme niedergelegten Anforderungen überprüft, vorlegen kann.

- Individuelle Prüfungen von Daten, die in einer virtualisierten Serverumgebung mit vielen Parteien gehostet sind, könnten sich als technisch unpraktisch herausstellen und unter bestimmten Umständen die Risiken für die bereits stattfindenden physischen und logischen Netzwerk-Sicherheitskontrollen erhöhen. In solchen Fällen könnte eine entsprechende Prüfung durch einen von dem für die Verarbeitung Verantwortlichen ausgewählten Dritten anstelle des Rechts auf Prüfung durch einen individuellen für die Verarbeitung Verantwortlichen ausreichen.

- Die Annahme von privatsphärenspezifischen Standards und Zertifizierungen ist für den Aufbau eines Vertrauensverhältnisses zwischen Cloud-Anbietern, für die Verarbeitung Verantwortlichen und betroffenen Personen von großer Bedeutung.

- Diese Standards und Zertifizierungen sollten technische Maßnahmen betreffen (wie die Lokalisierung oder Verschlüsselung von Daten) sowie die Prozesse innerhalb der Organisation des Anbieters, die den Datenschutz sicherstellen (wie Vorgehensweisen zur Zugangskontrolle, die Zugangskontrolle oder Backups).

4.3 Empfehlungen: zukünftige Entwicklungen

Der Arbeitsgruppe ist es vollkommen bewusst, dass die in dieser Stellungnahme dargelegten Garantien und Lösungen keine allumfassende Lösung für die Komplexität des Cloud Computing sind. Sie stellen jedoch eine tragfähige Grundlage dar, um die Verarbeitung personenbezogener Daten abzusichern, die im EWR niedergelassene Anwender an Cloud-Anbieter übergeben. Dieser Abschnitt konzentriert sich auf einige Fragen, die kurz- oder mittelfristig angegangen werden müssen, um die bestehenden Garantien zu stärken, die Cloud-Industrie bezüglich der dargelegten Fragen zu unterstützen und gleichzeitig die Achtung der Grundrechte auf Privatsphäre und Datenschutz sicherzustellen.

– Mehr Ausgewogenheit zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter in Bezug auf die Verantwortung: Die Arbeits-

[45] Zu diesen Standards würden unter anderem die der Internationalen Normenorganisationen, des International Auditing and Assurance Standards Board und des Auditing Standards Board of the American Institute of Certified Public Accountants zählen, insoweit diese Organisationen Standards bereitstellen, die die in dieser Stellungnahme niedergelegten Anforderungen erfüllen.

gruppe begrüßt die Bestimmungen in Artikel 26 des Vorschlags der Kommission (Entwurf einer EUDatenschutz-Grundverordnung), mit denen die Rechenschaftspflicht des Auftragsverarbeiters gegenüber dem für die Verarbeitung Verantwortlichen hervorgehoben wird, indem er diesem helfen muss, die Einhaltung insbesondere der Sicherheits- und ähnlicher Verpflichtungen sicherzustellen. Artikel 30 dieses Vorschlags führt die Pflicht für den Auftragsverarbeiter ein, geeignete technische und organisatorische Maßnahmen einzuführen. Der Vorschlagsentwurf stellt klar, dass ein Auftragsverarbeiter, der die Anweisungen des für die Verarbeitung Verantwortlichen nicht befolgt, als für die Verarbeitung Verantwortlicher gilt und spezifischen Bestimmungen unterworfen ist, da er für die Verarbeitung mitverantwortlich ist. Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass dieser Vorschlag in die richtige Richtung geht, um das Ungleichgewicht auszugleichen, das häufig in der Cloud Computing-Umgebung besteht, in welcher der Anwender (insbesondere wenn es sich um ein KMU handelt) Schwierigkeiten haben könnte, die in den Datenschutzvorschriften geforderte Kontrolle darüber auszuüben, wie der Anbieter die geforderten Dienste ausführt. Darüber hinaus wird angesichts der asymmetrischen Rechtsposition von betroffenen Personen und kleinen Unternehmen gegenüber großen Cloud Computing-Anbietern eine proaktivere Rolle für Verbraucher- und Unternehmensschutzorganisationen empfohlen, um ausgewogenere allgemeine Geschäftsbedingungen solcher Anbieter auszuhandeln.

– Zugang zu personenbezogenen Daten für nationale Sicherheits-und Strafverfolgungszwecke: Es ist von größter Bedeutung, der zukünftigen Verordnung hinzuzufügen, dass es den in der EU tätigen für die Verarbeitung Verantwortlichen untersagt sein muss, personenbezogene Daten an Drittländer offenzulegen, wenn dies von einer Gerichts- oder Verwaltungsbehörde eines Drittlandes gefordert wird, es sei denn, dies wird ausdrücklich in einer internationalen Vereinbarung oder einem Rechtshilfeabkommen gestattet oder von einer Überwachungsbehörde genehmigt. Die Verordnung (EG) Nr. 2271/96 des Rates ist ein angemessenes Beispiel einer Rechtsgrundlage hierfür.[46] Die Arbeitsgruppe ist besorgt über diese Lücke in dem Vorschlag der Kommission, da dies einen beträchtlichen Verlust an Rechtssicherheit für die betroffenen Personen bedeutet, deren personenbezogenen Daten in Datenzentren in der ganzen Welt gespeichert werden. Aus diesem Grund möchte die Arbeitsgruppe betonen[47], dass es wichtig ist, in der Verordnung festzuhalten, dass im Fall von Offenlegungen, die nicht durch das Recht der Union oder der Mitgliedstaaten berechtigt sind, Rechtshilfeabkommen zu nutzen sind.

---

46 Verordnung (EG) Nr. 2271/96 des Rates vom 22. November 1996 zum Schutz vor den Auswirkungen der extraterritorialen Anwendung von einem Drittland erlassener Rechtsakte sowie von darauf beruhenden oder sich daraus ergebenden Maßnahmen, Amtsblatt L 309, 29.11.1996 S. 0001–0006,
URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:DE:HTML

47 Vgl. WP 191 – Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, S. 23.

– Besondere Vorkehrungen durch den öffentlichen Sektor: Ein besonderer Vorbehalt ist in Bezug auf die Notwendigkeit hinzuzufügen, dass eine öffentliche Behörde erst prüfen muss, ob die Kommunikation, Verarbeitung und Speicherung der Daten außerhalb des innerstaatlichen Hoheitsgebiets die Sicherheit und Privatsphäre der Bürger sowie die nationale Sicherheit und Wirtschaft unannehmbaren Risiken aussetzen würde. Dies gilt insbesondere, wenn sensible Datenbanken (z. B. Zensusdaten) und Leistungen (z. B. Gesundheitsfürsorge) betroffen sind.[48] Dies sollte unbedingt jedes Mal in Erwägung gezogen werden, wenn sensible Daten in der Cloud-Umgebung verarbeitet werden. Ausgehend davon könnten nationale Regierungen und Organe der Europäischen Union über eine weitere Prüfung des Konzepts einer Europäischen Regierungs-Cloud als einen supranationalen virtuellen Raum nachdenken, in dem einheitliche und harmonisierte Vorschriften angewendet werden könnten.

– Europäische Cloud-Partnerschaft: Die Arbeitsgruppe unterstützt die Strategie für eine Europäische Cloud-Partnerschaft (ECP), die Frau Kroes, Vizepräsidentin der Europäischen Kommission, im Januar 2012 in Davos vorgestellt hat.[49] Diese Strategie umfasst die öffentliche IT-Beschaffung zur Anregung eines Europäischen Cloud-Marktes.Die Übermittlung personenbezogener Daten an einen europäischen Cloud-Anbieter, der sich an europäische Datenschutzvorschriften zu halten hat, könnte für die Kunden mit großen datenschutzrechtlichen Vorteilen verbunden sein, insbesondere durch die Förderung der Annahme allgemeiner Standards (vor allem in Bezug auf die Interoperabilität und die Datenportabilität) und könnte ihnen Rechtssicherheit geben.

---

48 Diesbezüglich macht die ENISA in ihrem Papier zur Sicherheit und Belastbarkeit von Regierungs-Clouds folgende Empfehlung (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): „In Bezug auf den Aufbau scheinen Private und Community Clouds derzeit die beste Lösung für den Bedarf von staatlichen Verwaltungsbehörden in Bezug auf sensible Anwendungen zu sein, da sie das höchste Maß an Governance, Kontrolle und Sichtbarkeit bieten, auch wenn beim Planen einer Private oder Community Cloud besonderes Augenmerk auf die Größe der Infrastruktur gerichtet werden sollte."

49 Neelie Kroes, Vizepräsidentin der Europäischen Kommission, verantwortlich für die Digitale Agenda, Setting up the European Cloud Partnership World Economic Forum Davos, Schweiz, 26. Januar 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ANHANG

a) Rollout-Modelle

Private Cloud[50] beschreibt eine IT-Infrastruktur, die einer einzigen Organisation gewidmet ist. Sie befindet sich entweder in den Geschäftsräumen der Organisation oder ihre Verwaltung ist an einen Dritten ausgelagert (üblicherweise über Server-Hosting), der der strikten Anweisungsbefugnis des für die Verarbeitung Verantwortlichen unterliegt. Eine Private Cloud kann mit einem herkömmlichen Datenzentrum verglichen werden. Der Unterschied liegt darin, dass technische Maßnahmen umgesetzt werden, um die verfügbaren Ressourcen zu optimieren und diese Ressourcen über kleine Investitionen zu stärken, die schrittweise im Laufe der Zeit gemacht werden.

Die **Public Cloud** dagegen ist eine Infrastruktur, die sich im Eigentum eines Anbieters befindet, der sich auf die Bereitstellung von Diensten spezialisiert hat und der seine Systeme Nutzern, Unternehmen und/oder öffentlichen Verwaltungsbehörden zur Verfügung stellt und folglich unter ihnen teilt. Auf die Dienste kann über das Internet Zugriff genommen werden, was die Datenverarbeitung und/oder Übermittlung der Daten an die Systeme des Diensteanbieters nach sich zieht. Deshalb hat der Diensteanbieter eine Schlüsselrolle in Bezug auf den wirksamen Schutz der an sein System übergebenen Daten. Zusammen mit den Daten gibt der Nutzer einen großen Teil seiner Kontrolle über diese Daten ab.

Neben „Public" und „Private" Clouds gibt es noch sogenannte „intermediäre" oder „hybride" Clouds, bei denen die Dienste sowohl von privaten Infrastrukturen bereitgestellt werden, als auch von Public Clouds gekauft werden. Es sollte auch auf die „Community Cloud" hingewiesen werden, bei der sich verschiedene Organisationen die IT-Infrastruktur zum Nutzen einer bestimmten Nutzergemeinschaft teilen.

Flexibilität und Einfachheit bei der Konfigurierung von Cloud-Systemen ermöglichen ihre „elastischen" Dimensionen, d. h. diese Systeme können gemäß einem nutzerbasierten Ansatz an die besonderen Ansprüche angepasst werden. Die Nutzer müssen nicht selbst IT-Systeme verwalten, auf die auf der Grundlage von Auslagerungs-Vereinbarungen Zugriff genommen wird und die deshalb vollstän-

[50] Das NIST (National Institute of Standards and Technology) in den USA, das seit einiger Zeit an der Standardisierung cloudbasierter Technologien arbeitet und auf dessen Definitionen auch in dem ENISA-Papier hingewiesen wird.
Private Cloud.
Die Cloud-Infrastruktur wird nur für eine Organisation betrieben. Sie kann von der Organisation selbst oder von einem Dritten verwaltet werden und muss sich nicht unbedingt in den Geschäftsräumen befinden. Es sollte darauf hingewiesen werden, dass sich eine „Private Cloud" zumindest auf manche Technologien stützt, die auch für „Public Clouds" üblich sind – einschließlich insbesondere der Virtualisierungs-Technologien, die – wie oben erklärt – eine Re-Organisation (oder Überarbeitung) der Datenverarbeitungsorganisation fördern.
Public Cloud.
Die Cloud-Infrastruktur wird der Allgemeinheit oder einer großen Industriegruppe zur Verfügung gestellt. Sie ist das Eigentum einer Organisation, die Cloud-Dienste verkauft.

dig von dem Dritten verwaltet werden, in dessen Cloud die Daten aufbewahrt werden. Häufig kommen große Anbieter mit komplexen Infrastrukturen ins Spiel. Deshalb kann sich die Cloud über mehrere Standorte erstrecken. Die Anwender wissen nicht unbedingt genau, wo ihre Daten aufbewahrt werden.

b) Servicemodelle

Abhängig von den Anforderungen des Nutzers gibt es verschiedene Cloud Computing-Lösungen auf dem Markt, die in drei Hauptkategorien oder „Servicemodelle" zusammengefasst werden können. Diese Modelle finden normalerweise sowohl auf Private als auch auf Public Clouds Anwendung:

– **IaaS (Cloud Infrastructure as a Service):** Ein Anbieter vermietet eine technische Infrastruktur, d. h. virtuelle Remote-Server, auf die sich der End-Nutzer gemäß den Mechanismen und Vereinbarungen stützen kann. Dadurch wird es einfach, wirksam und vorteilhaft, die IT-Systeme des Unternehmens in den Geschäftsräumen des Unternehmens zu ersetzen und/oder die gemietete Infrastruktur zusammen mit dem unternehmensinternen System zu nutzen. Solche Anbieter sind normalerweise spezialisierte Marktteilnehmer, die sich auf eine physische, komplexe Infrastruktur stützen können, die sich häufig über mehrere geografische Gebiete erstreckt.

– **SaaS (Cloud Software as a Service):** Ein Anbieter liefert verschiedene Anwendungsdienste über das Web und macht sie für den End-Nutzer verfügbar. Mit diesen Diensten sollen häufig konventionelle Anwendungen ersetzt werden, die von den Nutzern auf ihren lokalen Systemen installiert werden müssen. Entsprechend wird von den Nutzern letztendlich erwartet, dass sie ihre Daten an den individuellen Anbieter auslagern. Das ist beispielsweise bei den typischen webbasierten Office-Anwendungen wie Tabellen, Textverarbeitungstools, computergestützten Verzeichnissen und Agenden, gemeinsam genutzten Kalendern usw. der Fall. Die betreffenden Dienste umfassen jedoch auch cloudbasierte E-Mail-Anwendungen.

– **PaaS (Cloud Platform as a Service):** Ein Anbieter bietet Lösungen für die fortgeschrittene Entwicklung und das Hosting von Anwendungen. Diese Dienste werden üblicherweise an Marktteilnehmer gerichtet, die sie nutzen, um eigene, anwendungsbasierte Lösungen zu entwickeln und zu hosten, mit denen betriebsinterne Anforderungen erfüllt und/oder Leistungen an Dritte erbracht werden sollen. Auch hier machen es die von einem PaaS-Anbieter bereitgestellten Dienste unnötig, dass der Anwender sich auf zusätzliche und/oder spezifische Hardware oder Software auf interner Ebene stützt.

Der vollständige Übergang zu einem vollkommen öffentlichen Cloud-System scheint kurzfristig aus verschiedenen Gründen nicht durchführbar zu sein; insbesondere in Bezug auf große Institutionen wie wichtige Unternehmen oder Orga-

nisationen, die bestimmte Verpflichtungen zu erfüllen haben wie z. B. große Banken, Regierungsbehörden, große Stadtverwaltungen usw. Das kann hauptsächlich anhand von zwei Gründen erklärt werden: Erstens gibt es einen Faktor mit Eigendynamik, der mit den Investitionen zusammenhängt, die für einen solchen Übergang erforderlich wären, und zweitens müssen die besonders wertvollen und/oder sensiblen Informationen berücksichtigt werden, die in diesen spezifischen Fällen zu verarbeiten sind.

Ein weiterer Faktor, der für die Verwendung von Private Clouds spricht (zumindest in den vorgenannten Fällen), hängt damit zusammen, dass häufig kein öffentlicher Cloud-Anbieter eine Qualität des Dienstes (basierend auf einer Dienstgütevereinbarung) sicherstellen kann, die mit der kritischen Natur des von dem für die Verarbeitung Verantwortlichen bereitzustellenden Dienstes Schritt halten kann – möglicherweise weil die Bandbreite und Verlässlichkeit des Netzes in einem bestimmten Gebiet nicht ausreicht oder nicht angemessen ist oder in Bezug auf spezifische Nutzer-Anbieter-Verbindungen. Andererseits kann man davon ausgehen, dass in einigen der vorgenannten Fällen Private Clouds geleast oder gemietet werden können (da sich dies als kostenwirksamer herausstellen könnte) oder dass hybride Cloud-Modelle (die sowohl Komponenten der Public als auch der Private Cloud umfassen) genutzt werden können. Die entsprechenden Auswirkungen müssten in allen Fällen sorgfältig abgewogen werden.

Wenn international vereinbarte Standards fehlen, besteht die Gefahr von „do-it-yourself"-Cloud-Lösungen oder zusammengeschlossenen Cloud-Lösungen, die erhöhte Gefahren des Lock-in mit sich brächten (und sogenannter „Privatsphären-Monokulturen")[51] . Eine vollständige Kontrolle über die Daten würde verhindert, ohne dass die Interoperabilität sichergestellt wäre. Tatsächlich sind sowohl die Interoperabilität als auch die Datenportabilität Schlüsselfaktoren für die Entwicklung cloudbasierter Technologien und für die Sicherstellung einer vollständigen Ausübung der Datenschutzrechte, die den betroffenen Personen übertragen wurden (wie das Recht auf Zugang und Berichtigung).

Unter diesem Aspekt gibt die aktuelle Debatte über Cloud-Technologien ein signifikantes Beispiel der Spannung, die zwischen dem kostenorientierten und dem rechteorientierten Ansatz besteht, die kurz im vorstehenden Abschnitt 2 dargelegt wurden. Während es unter Berücksichtigung der spezifischen Umstände der Verarbeitung datenschutzrechtlich gesehen machbar und tatsächlich empfehlenswert sein könnte, sich auf Private Clouds zu stützen, ist dies auf lange Sicht einfach aus Kostengründen für Organisationen vermutlich nicht möglich. Eine sorgfältige Abwägung der auf dem Spiel stehenden Interessen ist erforderlich, da in diesem Bereich derzeit keine Lösung vorgelegt werden kann, die auf alle Situationen passt.

[51] Siehe die Studie des Europäischen Parlaments „Nützlich oder hinderlich? Die Förderung von Innovationen im Internet und das Recht der Bürger auf Schutz der Privatsphäre", veröffentlicht im Dezember 2011.

IV. Internationale Konferenz der Datenschutzbeauftragten

34. Konferenz am 25./26. Oktober 2012 in Punta del Este, Uruguay

Entschließung über die Zukunft des Datenschutzes

Unter Berücksichtigung der Diskussionen in der Europäischen Union über die Vorschläge für einen überarbeiteten Rechtsrahmen zum Datenschutz und der laufenden Arbeiten im Europarat und der OECD;

unter Berücksichtigung der in den USA laufenden Prozesse zur Verbesserung des Datenschutzes und insbesondere des Vorhaben, eine „Bill of Rights“ zum Datenschutz einzuführen;

unter Berücksichtigung der jüngsten, von der APEC ergriffenen Initiative die Zusammenarbeit zwischen Datenschutzbehörden zu stärken und ein System einfacher und überprüfbarer Datentransfers innerhalb der APEC und über ihre Grenzen hinaus durch die Regelungen grenzüberschreitender Datentransfers einzuführen;

unter Berücksichtigung des immer größer werdenden multilateralen Netzwerks und seiner Initiativen zur Förderung der Zusammenarbeit der internationalen Datenschutzbehörden bei der Durchsetzung des Datenschutzes;

unter Begrüßung der Tatsache, dass viele Länder in den letzten Jahren neue Datenschutzbehörden geschaffen haben;

mit Bezug auf zunehmende Globalisierung und rasante technologischen Entwicklungen hat die 34. Internationale Datenschutzkonferenz beschlossen, dass Ihre Mitglieder folgende Schritte unternehmen sollen:

1. ihre Zusammenarbeit verstärken, um die mit den grenzüberschreitenden Datenübermittlungen verbunden Risiken koordiniert in Angriff zu nehmen, z. B. durch Zusammenarbeit in multilateralen Netzwerken zur Durchsetzung des Datenschutzes, und

2. Informationen und Fachwissen im größtmöglichen Umfang austauschen, um sicherzustellen, dass aus den knappen Ressourcen der Behörden maximaler Nutzen gezogen wird,

3. Möglichkeiten größerer Interoperabilität zwischen unterschiedlichen Rechtssystemen und Datenschutzregimen erkennen und nutzen.

Erläuterungen

Immer mehr Unternehmen sind in mehr als einem Land tätig und auch Regierungen kooperieren zunehmend miteinander, um gemeinsame Bedrohungen und Besorgnisse zu überwinden. Technologien wurden entwickelt, die die grenzüberschreitende Kommunikation und den Datenaustausch erleichtern. Dadurch werden täglich große Mengen personenbezogener Daten über Grenzen hinweg übermittelt.

Verschiedene dieser Technologien weisen auch selbst Risiken für den Datenschutz und die Privatsphäre auf. Vor allem das Internet stellt den Schutz der personenbezogenen Daten und der Privatsphäre der Menschen vor großen Herausforderungen, insbesondere in Verbindung mit der zunehmenden Nutzung mobiler Geräte.

Gesetzgeber auf der ganzen Welt sind deshalb überzeugt, dass die Vorschriften und Gesetze zum Datenschutz und zum Schutz der Privatsphäre überprüft werden müssen. Außerdem sind die Datenschutzbehörden angesichts der gestiegenen Anforderungen aufgefordert, enger zusammenzuarbeiten und zu versuchen, ihre Handlungen soweit wie möglich zu koordinieren. Wegen der derzeitigen schwierigen wirtschaftlichen Lage weltweit ist es von entscheidender Bedeutung, Informationen und Fachwissen auszutauschen und den besten Nutzen aus knappen Ressourcen zu ziehen.

Derzeit werden in allen Teilen der Welt die datenschutzrechtlichen Regelungen überprüft. Es wird die große Chance geboten, zu versuchen, die verschiedenen Systeme miteinander in Einklang zu bringen. Wir müssen diese Chance ergreifen, um allen Menschen auf der ganzen Welt einen besseren Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten zu bieten.

Entschließung zu Cloud Computing

Cloud Computing (CC) gewinnt zunehmend an Interesse, weil es eine größere Wirtschaftlichkeit, weniger Belastung für die Umwelt, einfachere Handhabung, mehr Benutzerfreundlichkeit und viele andere Vorteile verspricht. Aufgrund folgender Tatsachen wirft die Entwicklung von CC viele wichtigen Themen auf, wie z. B. in folgender Hinsicht: Die Technologie befindet sich noch im Entwicklungsstadium, die Datenverarbeitung findet jetzt weltweit statt, und aufgrund der fehlenden Transparenz wird die Durchsetzung von Regelungen zum Schutz der Privatsphäre und der Daten sogar noch erschwert. Dadurch könnten die Risiken, die bei der Datenverarbeitung auftreten, noch erhöht werden, wie Verstöße gegen die Datensicherheit, Verstöße gegen Gesetze und Grundsätze für den Schutz der

Privatsphäre und der Daten, und der Missbrauch der in der Cloud gespeicherten Daten.

Die Mitglieder der Internationalen Konferenz und andere Interessengruppen, wie zum Beispiel die International Working Group on Data Protection in Telecommunications (IWGDPT, auch bekannt als „Berlin Group“[1]), hat die mit CC verbundenen datenschutzrechtlichen Probleme untersucht.

Ohne dabei eine von einer bestimmten Gruppe vorgenommene Analyse zu unterstützen, begrüßt die Internationale Konferenz derartige Bemühungen. Um einen Beitrag für die Förderung solcher Bemühungen und zur Vermeidung der mit der Nutzung der Cloud Computing Dienste verbundenen Risiken und zur Förderung der Verantwortlichkeit und der ordnungsgemäßen Geschäftsführung zu leisten, empfiehlt die **Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre** deshalb:

- Im Vergleich mit anderen Arten der Datenverarbeitung darf Cloud Computing nicht zur Absenkung der Datenschutzstandards führen;

- die verantwortlichen Stellen sollen vor der Aufnahme von CC-Projekten die notwendigen Prüfungen der Auswirkungen und Risiken für den Datenschutz durchführen (ggf. durch vertrauenswürdige Dritte)

- Die Anbieter von Cloud-Diensten sollen angemessene Transparenz, Sicherheit, Verantwortlichkeit und Vertrauen in CC-Lösungen gewährleisten, insbesondere in Bezug auf Informationen über die Verletzung des Schutzes personenbezogener Daten und in Bezug auf Vertragsklauseln, die gegebenenfalls die Datenportabilität und Datenkontrolle durch Cloud-Nutzer unterstützen. Wenn sie als verantwortliche Stellen handeln, sollen Cloud-Diensteanbieter den Nutzern gegebenenfalls wichtige Informationen über mögliche Auswirkungen auf den Datenschutz und über mit deren Dienste verbundene Risiken zur Verfügung stellen.

- Es sollen weitere Bemühungen im Bereich der Forschung, der Zertifizierung durch Dritte, Standardisierung, „Privacy by Design“-Technologien und anderen, damit verbundenen Systemen unternommen werden, um das gewünschte Maß an Vertrauen in CC zu erreichen. Um den Datenschutz gründlich und wirksam in Cloud Computing einzubauen, sollten schon im Anfangsstadium angemessene Maßnahmen in die Architektur von IT-Systemen und Geschäftsabläufen einbezogen werden (Privacy by Design).

[1] Siehe z. B. das Arbeitspapier der Gruppe „Cloud Computing – Privacy and data protection issues (Sopot Memorandum)“, Sopot (Polen), 23./24. April 2012;
http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.l2.6.l2.pdf

- Die Gesetzgeber sollen die Angemessenheit und Interoperabilität der bestehenden Rechtsrahmen zur Erleichterung grenzüberschreitender Datenübermittlungen überprüfen, und sie sollten zusätzliche notwendige Maßnahmen zum Datenschutz im Bereich CC in Erwägung ziehen.

- Die Datenschutzbehörden sollen den verantwortlichen Stellen, Anbietern von Cloud- Diensten und Gesetzgebern weiterhin mit Informationen zu Fragen hinsichtlich des Schutzes der Privatsphäre und personenbezogener Daten zur Verfügung stehen.

Alle Interessengruppen – Anbieter, Kunden von CC und auch Regulierungsbehörden – sollten zusammenarbeiten, um ein hohes Datenschutzniveau und eine hohe IT-Sicherheit zu gewährleisten.

V. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

51. Sitzung am 23./24. April in Sopot, Polen

Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes – „Sopot Memorandum " –

– Übersetzung –

Anwendungsbereich

In diesem Arbeitspapier wird insbesondere die Verarbeitung personenbezogener Daten beim Cloud Computing untersucht.

Nicht betrachtet werden Szenarien, in denen alle Endnutzer, der für die Verarbeitung Verantwortliche, der Auftragsdatenverarbeiter und alle Unterauftragnehmer denselben Datenschutzregeln unterliegen, physisch im selben Hoheitsgebiet angesiedelt sind und jegliche Datenverarbeitung und -speicherung in diesem Hoheitsgebiet erfolgt. Das Arbeitspapier ist ebenfalls weniger relevenat, wenn der Cloud-Dienst unter der vollständigen Kontrolle des Nutzers dieses Dienstes ist.

Schließlich befasst sich das Arbeitspapier nur mit der Nutzung von Cloud-Diensten durch Unternehmen und Behörden, die bestehende Verfahren „in die Cloud" verlagern, und nicht mit der Nutzung dieser Dienste durch Privatpersonen.

Allgemeiner Hintergrund

„Cloud Computing ist ein sich entwickelndes Paradigma."[1]

Cloud Computing (CC) stößt auf wachsendes Interesse, da es eine höhere Wirtschaftlichkeit, geringere Umweltbelastung, einen einfacheren Betrieb, höhere Benutzerfreundlichkeit und eine Reihe weiterer Vorteile verspricht.

Im September 2011 erschien die Sonderveröffentlichung SP 800-145 des National Institute of Standards and Technology (NIST), in der Cloud Computing wie folgt definiert wird:

[1] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Seite 2.

„Cloud Computing ist ein Modell zur Ermöglichung eines ubiquitären, komfortablen, auf Abruf verfügbaren Netzzugriffs auf einen gemeinsamen Pool aus konfigurierbaren Rechenressourcen (z. B. Netze, Server, Speicher, Anwendungen und Dienste), der schnell und mit geringfügigem Verwaltungsaufwand bzw. minimaler Interaktion mit dem Dienstanbieter bereitgestellt und öffentlich verfügbar gemacht werden kann. Das Cloud-Modell besteht aus fünf wesentlichen Charakteristika, drei Service- und vier Nutzungsmodellen.“ [2]

Unter anderem soll die Definition

„als Ausgangspunkt für eine Diskussion darüber dienen, was Cloud Computing ist und wie es am besten genutzt werden kann.“[3]

Die Definition trägt zu einem besseren Verständnis davon bei, was CC eigentlich ist. Dieses Verständnis entwickelt sich derzeit rasant. Die Definition des NIST ist ein hervorragender Ausgangspunkt für die weitere Untersuchung des CC und seiner Nutzung.

Allerdings gibt es auch immer noch Unklarheiten im Zusammenhang mit CC, insbesondere hinsichtlich des Datenschutzes und anderer rechtlicher Fragen. Die Empfehlungen in diesem Arbeitspapier sollen helfen, diese Unklarheiten zu verringern.

Im ersten Teil werden zunächst die Empfehlungen vorgestellt. Der zweite Teil enthält weitere Hintergrundinformationen über Cloud Computing und Begründungen für die Empfehlungen. Wer sich näher mit dem Thema auseinandersetzen möchte, sollte diesen Teil zuerst lesen.

Für die Zwecke dieses Arbeitspapiers ist der für die Verarbeitung Verantwortliche der Kunde und der Auftragsverarbeiter der Cloud-Anbieter.[4]

Die Entwicklung des CC har eine Reihe wichtiger Themen hervorgehoben, z. B.:

a. Es gibt noch keine internationale Einigung auf eine einheitliche Terminologie;

b. Die Technologie befindet sich noch in der Entwicklung;

c. Riesige Datenmengen werden zusammengetragen und gebündelt;

---

[2] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Seite 3.

[3] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Seite 2.

[4] Vgl. Nr. 39 und 40 unten. Die Unterauftragnehmer des Cloud-Anbieters gelten im Zusammenhang mit der Verarbeitung personenbezogener Daten ebenfalls als Auftragsverarbeiter.

d. Die Technologie ist grenzenlos und grenzüberschreitend[5];

e. Daten werden weltweit verarbeitet;

f. Die Prozesse, Verfahren und Methoden der Cloud-Anbieter sind nicht ausreichend transparent, z. B. ob Cloud-Anbieter Unteraufträge für die Verarbeitung vergeben und wenn ja, welche Prozesse, Verfahren und Methoden diese verwenden;

g. Dieser Mangel an Transparenz erschwert eine angemessene Risikobewertung.

h. Aufgrund dieses Mangels an Transparenzist es auch schwerer, Datenschutzregeln durchzusetzen.

i. Die Cloud-Anbieter stehen unter einem großen Druck, möglichst schnell Kapital aus den hohen Investitionskosten zu schlagen.

j. Die Kunden stehen unter einem zunehmenden, teilweise der weltweiten Finanzkrise geschuldeten Druck, die Kosten auch für ihre Datenverarbeitung zu senken.

k. Um die Preise niedrig zu halten, sind Cloud-Anbieter eher bereit, allgemeine Geschäftsbedingungen anzubieten.

Daraus können sich folgende **Risiken** ergeben:

A. Verletzungen der Informationssicherheit, wie die Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von (personenbezogenen) Daten werden vom Verantwortlichen für die Verarbeitung nicht erkannt.

B. Daten werden in Hoheitsgebiete übertragen, die keinen angemessenen Datenschutz gewährleisten.

C. Verstöße gegen Gesetze und Grundsätze des Schutzes der Privatsphäre und des Datenschutzes.

D. Der für die Verarbeitung Verantwortliche akzeptiert allgemeine Geschäftsbedingungen, die dem Cloud-Anbieter zu viel Spielraum lassen, u. a. die Möglichkeit, Daten entgegen den Anweisungen des für die Verarbeitung Verantwortlichen zu verarbeiten.

E. Verwendung von Daten des für die Verarbeitung Verantwortlichen für eigene Zwecke ohne Wissen oder Erlaubnis des für die Verarbeitung Verantwortlichen durch Cloud-Anbieter oder ihre Unterauftragnehmer.

F. Die Rechenschaftspflicht und Verantwortung wird in einer Kette von Unterauftragnehmern scheinbar ausgehöhlt oder verschwindet.

[5] Vgl. Nr. 38

G. Der für die Verarbeitung Verantwortliche verliert die Kontrolle über die Daten und die Datenverarbeitung.

H. Der für die Verarbeitung Verantwortliche oder ein vertrauenswürdiger Dritter (z. B. Prüfer) ist nicht in der Lage, den Cloud-Anbieter angemessen zu kontrollieren.

I. Datenschutzbehörden werden davon abgehalten, die Verarbeitung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen und den Cloud-Anbieter angemessen zu überwachen.

J. Der für die Verarbeitung Verantwortliche verlässt sich aufgrund mangelnder Informationen und Überwachung auf ungerechtfertigtes Vertrauen und verstößt dadurch möglicherweise gegen geltendes Datenschutzrecht im Niederlassungsland.

Die **folgenden Empfehlungen** sollen zur **Verringerung der Risiken bei der Nutzung von Cloud-Diensten beitragen und verantwortungsvolles Handeln fördern**[6], so dass die Vorteile der Verwendung von CC genutzt werden können, jedoch nicht auf Kosten der Rechte des Einzelnen.

Empfehlungen[7]

Allgemeine Empfehlungen

Die Arbeitsgruppe empfiehlt, dass:

- durch Cloud Computing Datenschutzstandards im Vergleich zur herkömmlichen Datenverarbeitung nicht abgesenkt werden **dürfen**;

- die für die Verarbeitung Verantwortlichen vor dem Einstieg in CC-Projekte eine Abschätzung der Folgen für den Datenschutz und eine Risikoabschätzung vornehmen (ggf. mithilfe vertrauenswürdiger Dritter).

- Anbieter von Cloud-Diensten ihre Verfahren weiterentwickeln, um mehr Transparenz, Sicherheit, Nachprüfbarkeit und Vertrauen in CC-Lösungen zu schaffen, insbesondere im Hinblick auf Informationen über mögliche Verstöße

6 Auf den Seiten 9 und 10 ihres Berichts *Cloud Computing – Benefits, risks and recommendations for information security* [Cloud Computing: Nutzen, Risiken und Empfehlungen zur Informationssicherheit] vom November 2009 nennt die ENISA die häufigsten Sicherheitsrisiken. Dazu zählen in zufälliger Reihenfolge: Kontrollverlust, Abhängigkeit von einem Anbieter (Lock-in-Effekt), fehlende Isolation, Datenschutz, unsichere oder unvollständige Löschung von Daten, interne Angreifer. Weitere Einzelheiten können dem Bericht entnommen werden. Hier wird der Kontrollverlust betont.

7 Die Liste der Empfehlungen ist nicht abschließend.

gegen den Datenschutz und ausgewogenere Vertragsbedingungen zur Förderung der Portabilität von Daten und der Kontrolle über die Datendurch die Cloud-Nutzer.

- Weitere Bemühungen in der Forschung, der Zertifizierung durch Dritte, der Standardisierung, von „Privacy by Design"-Technologien und anderen damit verbundenen Bereichen unternommen werden, um das gewünschte Vertrauen in CC zu erreichen.

- Gesetzgeber überprüfen, ob das bestehende Recht zur grenzüberschreitenden Datenübertragung weiterhin angemessen ist, und zusätzliche Datenschutzvorkehrungen im Bereich des CC in Erwägung ziehen[8].

- Datenschutzbehörden die für die Verarbeitung Verantwortlichen, Cloud-Anbieter und Gesetzgeber weiterhin über Fragen des Schutzes der Privatsphäre und des Datenschutzes informieren.

Weitere Hinweise zu bewährten Verfahren („best practices")

1. CC sollte in sorgfältigen, maßvollen Schritten umgesetzt werden, beginnend mit nicht-sensiblen und nicht-vertraulichen Daten.

2. Die Verarbeitung sensitiver[9] Daten über CC stößt auf zusätzliche Bedenken. Unbeschadet nationaler Gesetze erfordert diese Art der Verarbeitung zusätzliche Schutzmaßnahmen.

3. Für die Verarbeitung Verantwortliche und Datenschutzbehörden sollten Zugang zu **standortbezogenen Audit Trails** haben. Der Audit Trail sollte automatisch aufgezeichnet werden und anzeigen, an welchen physischen Standorten personenbezogene Daten zu welchen Zeitpunkten gespeichert oder verarbeitet wurden[10].

4. Ein **automatisch aufgezeichneter Audit Trail über Kopier- und Löschvorgänge sollte** eingerichtet werden, anhand dessen eindeutig erkennbar ist,

---

8 Vgl. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre: Entschließung über Internationale Standards zum Schutz der Privatsphäre („Entschließung von Madrid"), 5. November 2009; http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

9 Der Begriff der sensitiven Daten ist in verschiedenen Rechtskulturen unterschiedlich besetzt: vgl. Art. 8 der Richtlinie 95/46/EG, Art. 9 des Entwurfs der Datenschutzverordnung sowie den FTC-Bericht „Protecting Comsumer Privacy in an Era of Rapid Change" (2012).

10 Der standortbezogene Audit Trail könnte beispielsweise eine klare Übersicht darüber geben, wann die einzelnen personenbezogenen Daten an bestimmten Standorten ein- und ausgetragen wurden und wann sie zu welchen Standort übertragen werden.

welche Kopien personenbezogener Daten der Auftragsverarbeiter oder seine Unterauftragnehmer angelegt und gelöscht haben.

5. Die Audit Trails zur Protokollierung des Standorts sowie der Kopier- und Löschvorgänge sollten auch die Datensicherung umfassen.

6. Wirksame technische Maßnahmen sollten entwickelt werden, um eine rechtswidrige Übertragung personenbezogener Daten in Hoheitsgebiete ohne ausreichenden Datenschutz zu verhindern.

7. Es sollte sichergestellt werden, dass personenbezogene Daten wirksam von Laufwerken und anderen Speichermedien **gelöscht** werden, z. B. durch **sofortiges Überschreiben mit Zufallsdaten**[11].

8. Es sollte sichergestellt sein, dass ruhende Daten und die Datenübertragung[12] mithilfe anerkannter Standardalgorithmen und aktueller Schlüssellängen **verschlüsselt** werden. Die Schlüssel sollten von keinem anderen als dem für die Verarbeitung Verantwortlichen und den Cloud-Anbieter verwendet werden und nur diesen zugänglich sein. Die Schlüssel sollten nicht von anderen Kunden als denen des Cloud-Anbieters verwendet werden oder diesen zugänglich sein. Daten sollten nicht länger und in größerem Umfang in unverschlüsselter Form zugänglich sein als für die jeweilige Datenverarbeitung unbedingt nötig. Methoden, mit deren Hilfe Daten für CC-Anbieter zu jeder Zeit **unlesbar** gemacht werden können, sollten weiter untersucht werden[13]. Es könnte nützlich sein, Möglichkeiten zu erkunden, wie der für die Verarbeitung Verantwortliche die Entschlüsselung von Daten durch den Cloud-Anbieter und seine Unterauftragnehmer wirksam und schnell unterbinden kann (Notbremse).

9. Alle Verwendungen personenbezogener Daten durch Cloud-Anbieter und ihre Unterauftragnehmer sollten automatisch **protokolliert** werden. Das Protokoll sollte für den für die Verarbeitung Verantwortlichen leicht zugänglich sowie einfach und leicht verständlich gestaltet sein. Der Cloud-Anbieter und seine Unterauftragnehmer sollten die Integrität der Protokolle gewährleisten.

---

[11] Eine Löschung durch Dereferenzierung der Daten und späteres Überschreiben durch Wiederverwendung der Speicherbereiche reicht in der Regel nicht aus, da weiterhin die Möglichkeit besteht, dass Daten vor oder während der Wiederverwendung der Speicherbereiche durch erneute Referenzierung wieder zugänglich werden.

[12] Während der Datenübertragung sollte eine Ende-zu-Ende-Verschlüsselung erfolgen. Es muss sichergestellt sein, dass personenbezogene Daten während der Übertragung gegen aktive (z. B. Replays, Traffic Injection) und passive Angriffe (z. B. Belauschen) geschützt sind. Ferner muss der Datenzugriff durch unbefugte Dritte mithilfe entsprechender technischer und organisatorischer Verfahren verhindert werden (z. B. Zugangskontrolle, Datenverschlüsselung).

[13] Ein Forschungsbeispiel in diesem Bereich ist die Sealed Cloud, welche im Preprint des Artikels von Hubert A. Jäger und Arnold Monitzer „Sealed Cloud – a novel approach to defend insider attacks“ beschrieben ist. Der Preprint kann unter der folgenden Adresse aufgerufen werden http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf.

Verantwortliche für die Verarbeitung

10. Der für die Verarbeitung Verantwortliche sollte in die Vereinbarung mit dem Cloud-Anbieter eine vollständige Liste mit Informationen über alle physischen Standorte aufnehmen, an denen über die Laufzeit der Vereinbarung Daten durch den Cloud-Anbieter und/oder seine Unterauftragnehmer gespeichert oder verarbeitet werden, einschließlich zur Datensicherung (**Grundsatz der Standorttransparenz**).

11. Der für die Verarbeitung Verantwortliche sollte in der Vereinbarung sicherstellen, dass weder der Cloud-Anbieter noch seine Unterauftragnehmer, ungeachtet ihrer Gründe und ob die Daten verschlüsselt werden, Daten an andere Standorte als die im Vertrag aufgelisteten übertragen. Dies sollte von technischen Maßnahmen begleitet werden, deren Vorhandensein und Zuverlässigkeit der für die Verarbeitung Verantwortliche tatsächlich prüfen kann.

12. Der für die Verarbeitung Verantwortliche sollte dafür sorgen, dass die Vereinbarung mit dem Cloud-Anbieter unmissverständlich ist und keine Auslegungen zulässt, die den Grundsatz untergräbt, dass der Cloud-Anbieter personenbezogene Daten nur entsprechend den Weisungen des für die Verarbeitung Verantwortlichen verarbeitet. Können Cloud-Anbieter die Vereinbarung einseitig ändern, sollte der für die Verarbeitung Verantwortliche das Recht haben, den Vertrag zu kündigen und die Daten an einen anderen Cloud-Anbieter zu übertragen.

13. Die Vereinbarung sollte ausdrücklich regeln, dass der Cloud-Anbieter die Daten des für die Verarbeitung Verantwortlichen nicht für seine eigenen Zwecke nutzen darf.

14. Der für die Verarbeitung Verantwortliche sollte die Möglichkeit haben, alle Standorte, an denen personenbezogene Daten ganz oder teilweise verarbeitet werden, in der Vergangenheit verarbeitet wurden oder gemäß der Vereinbarung in Zukunft verarbeitet werden, zu prüfen oder prüfen zu lassen. Die Vereinbarung sollte festlegen, dass der für die Verarbeitung Verantwortliche das Recht hat, vollständige Informationen über alle Aspekte des Cloud-Anbieters und seiner Unterauftragnehmer zu erhalten, die der für die Verarbeitung Verantwortliche als notwendig erachtet, um die Einhaltung der Vereinbarung zu gewährleisten, d. h. zu gewährleisten, dass die Verarbeitung personenbezogener Daten in Einklang mit den Weisungen und geltendem Recht sowie auf angemessen sichere Art und Weise erfolgt.

15. Der für die Verarbeitung Verantwortliche sollte sich in der Vereinbarung das Recht sichern, die Verarbeitung personenbezogener Daten durch den Cloud-Anbieter und ggf. seine Unterauftragnehmer durch einen vertrauenswürdigen

Dritten (z. B. ein anerkanntes Prüfunternehmen)[14] vollständig oder teilweise überwachen zu lassen.

16. Vor dem Einsatz von CC sollte der für die Verarbeitung Verantwortliche auf der Grundlage seiner Informationen über die Bedingungen und Umstände, unter denen personenbezogene Daten vom Cloud-Anbieter und ggf. seinen Unterauftragnehmern verarbeitet werden, eine **Risikoabschätzung** vornehmen. Die Risikoabschätzung sollte alle Standorte umfassen, an denen personenbezogene Daten verarbeitet oder gespeichert werden. Setzt der Cloud-Anbieter für Teile der Verarbeitung Unterauftragnehmer ein, sollte die Risikoabschätzung auch alle Standorte der Unterauftragnehmer umfassen.

17. Der für die Verarbeitung Verantwortliche sollte die Risikoabschätzung regelmäßig überprüfen und aktualisieren, solange personenbezogene Daten vom Cloud-Anbieter verarbeitet werden.

18. Vor dem Einsatz von CC sollte der für die Verarbeitung Verantwortliche versuchen sicherzustellen, dass ein Ausstieg aus dem Cloud-Dienst tatsächlich möglich ist, wozu auch eine aktive Rolle des Cloud-Anbieters beim Transfer der Daten zählt, um nicht von einem Cloud-Anbieter abhängig zu werden (Lock-in-Effekt).

19. Der für die Verarbeitung Verantwortliche sollte prüfen, ob es notwendig ist, sich den Zugriff auf mindestens eine nutzbare Kopie der Daten außerhalb der Kontrolle, des Zugriffs oder des Einflusses des Cloud-Anbieters (und seiner Unterauftragnehmer) zu sichern. Falls ja, sollte die Kopie unabhängig von der Mitwirkung des Cloud-Anbieters und seiner Unterauftragnehmer für den Verantwortlichen für die Verarbeitung zugänglich und nutzbar sein.

20. Der für die Verarbeitung Verantwortliche sollte im Falle eines **Verletzung der Datensicherheit** seine Verpflichtungen gegenüber den Betroffenen und den Datenschutzbehörden vollständig erfüllen und geeignete Maßnahmen ergreifen können. Von daher sollte der für die Verarbeitung Verantwortliche klare Vereinbarungen mit dem Cloud-Anbieter über die umgehende und umfassende Benachrichtigung des für die Verarbeitung Verantwortlichen und/oder der Datenschutzbehörde im Falle einer solchen Verletzung treffen.

21. Der für die Verarbeitung Verantwortliche sollte den Cloud-Anbieter vertraglich dazu verpflichten, wirksame und schnelle Verfahren umzusetzen, damit die Betroffenen ihr Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten wahrnehmen können.

---

[14] Das Thema vertrauenswürdige Dritte ist in Nr. 44 näher beschrieben.

Cloud-Anbieter

22. Der Cloud-Anbieter sollte gegenüber dem für die Verarbeitung Verantwortlichen vollständige Transparenz bezüglich der von ihm und ggf. seinen Unterauftragnehmern verwendeten Standorte für die Verarbeitung und Speicherung personenbezogener Daten gewährleisten.

23. Der Cloud-Anbieter sollte vollständige Transparenz bezüglich seiner Unterauftragnehmer und der von ihnen durchgeführten Verarbeitungsprozesse gewährleisten.

24. Der Cloud-Anbieter sollte Transparenz in Vertragsfragen gewährleisten und CC nicht mit allgemeinen Geschäftsbedingungen anbieten, die einseitige Vertragsänderungen ermöglichen.

25. Cloud-Anbieter und ggf. ihre Unterauftragnehmer werden ermutigt, sich nach bewährten Verfahren zu richten und es einem unparteiischen Dritten zu erlauben, sie zu vergleichen und zu bewerten (Benchmarking).

26. Allgemeine Geschäftsbedingungen für bestimmte Marktsegmente, z. B. kleine und mittelständische Unternehmen, sollten so gestaltet sein, dass die Achtung der Privatsphäre und angemessene Schutzmaßnahmen berücksichtigt werden.

Prüfungen

27. Da ein Cloud-Anbieter sehr große Mengen an personenbezogenen Daten ansammeln kann, sollte der Cloud-Anbieter im Interesse des für die Verarbeitung Verantwortlichen zusätzlich zu dessen Prüfungen auch von einer dritten Stelle überprüft werden. Der Prüfer sollte vollkommen unabhängig vom Cloud-Anbieter sein und der Sicherheit der Verarbeitung personenbezogener Daten besondere Aufmerksamkeit schenken. Der Prüfer sollte insbesondere prüfen, ob Maßnahmen in den folgenden Bereichen ergriffen wurden und ordnungsgemäß funktionieren: standortbezogener Audit Trail (vgl. Nr. 3), Audit Trails für das Kopieren und Löschen (vgl. Nr. 4), Löschung (vgl. Nr. 7) und Protokollierung (vgl. Nr. 9). Ferner sollte der Prüfer prüfen, ob folgende Maßnahmen ergriffen wurden und ordnungsgemäß funktionieren: Maßnahmen zur Verhütung der rechtswidrigen Datenübertragung in Hoheitsgebiete ohne ausreichenden Datenschutz (vgl. Nr. 6) und Maßnahmen zur Verhütung der Datenübertragung an andere Standorte als die ausdrücklich mit dem Kunden vereinbarten (vgl. Nr. 10 und 11). Schließlich sollte der Prüfer sicherstellen, dass es dem Cloud-Anbieter oder ggf. seinen Unterauftragnehmern nicht möglich ist, diese Maßnahmen unentdeckt zu umgehen.

Hintergrundinformationen zu den Empfehlungen

28. CC ist eine recht **neue Form** der Datenverarbeitung, die sich aus der mangels einer besseren Benennung **traditionelle Datenverarbeitung** genannten Form der Datenverarbeitung entwickelt hat. Es hat sich eine langjährige, solide Erfahrung mit der traditionellen Datenverarbeitung angesammelt, doch gibt es keine derartige solide Erfahrung mit CC.

29. Die Folge dieses **Paradigmenwechsels** ist, dass Grundannahmen, Erfahrungen, Ideen, Theorien und Modelle für die Datenverarbeitung nicht mehr mit der Praxis übereinstimmen und daher einer kritischen Prüfung, Neubewertung und ggf. Überarbeitung unterzogen werden müssen. Dies trifft auch auf den Schutz der Privatsphäre und den Schutz personenbezogener Daten sowie die Art und Weise zu, wie **Risiken** analysiert, bewertet und beurteilt werden können. Die bewährten Verfahren von gestern sind nicht unbedingt die bewährten Verfahren von heute.

30. Die **neue Situation** muss untersucht und in **sorgfältig gewählten Schritten** umgesetzt werden, insbesondere hinsichtlich des Datenschutzes und des Schutzes der Rechte der Betroffenen im weiteren Sinne.

31. Die **technische Grundlage** des CC ist eine ausgereifte Netzwerktechnik und Server-Virtualisierung. Dies ermöglicht eine schnelle und dynamische Verlagerung von Daten und deren Verarbeitung lokal zwischen Servern im jeweiligen Rechenzentrum und global zwischen Servern in weltweiten Rechenzentren. Die Technologie ist hochgradig skalierbar, ohne einschränkende Engpässe zu erzeugen. Das Internet ermöglicht es dem Endnutzer, unabhängig vom Standort der Rechenzentren auf die Daten zuzugreifen.

32. Die **wirtschaftliche Antriebskraft** hinter CC sind **Skaleneffekte**. Die Zusammenfassung der Datenverarbeitung in großen Zentren verbessert die Nutzung teurer Ressourcen, wie z. B. menschlichem Wissen, Sachwerten (Hardware, Software, Gebäude), von Kommunikationsbandbreite und Energie. Aufgrund ihrer Größe und ihres Volumens haben Cloud-Anbieter zudem eine besonders starke Verhandlungsposition beim Erwerb von Ressourcen. Somit können Cloud-Anbieter Stückkosten reduzieren und den Kunden attraktive Preise anbieten. Um Skaleneffekte erzielen zu können, müssen möglichst viele Kunden den Dienst nutzen. Um ein ausreichendes **Volumen** zu erreichen, werden Cloud-Dienste weltweit über das Internet angeboten.

33. CC gilt als große Chance für kleine und mittelständische Unternehmen, Zugang zu bezahlbaren und skalierbaren Rechenressourcen zu erhalten. Aufgrund der großen Anzahl relativ kleiner Organisationen wird erwartet, dass

Cloud-Anbieter allgemeine Geschäftsbedingungen für dieses Marktsegment entwickeln.

34. CC ist viel dynamischer als die traditionelle Datenverarbeitung. Der Standort, an dem Daten verarbeitet werden, kann sich stark verändern. Der aktuelle Standort von Daten und ihrer Verarbeitung kann von verschiedenen Faktoren abhängen, über die sich Endnutzer und für die Verarbeitung Verantwortliche bisher wenig Gedanken gemacht haben und über die sie unter Umständen wenig wissen und wenig Kontrolle haben. Beispielsweise siedeln Cloud-Anbieter ihre Datenzentren häufig in verschiedenen Ländern und auf mehreren Kontinenten an, u. a. aufgrund einer günstigen Stromversorgung, eines kühlen Klimas und unterschiedlicher Zeitzonen. Unvorhersehbare Umstände, z. B. Ausfälle in einem Rechenzentrum oder ein Kapazitätsmangel bei Spitzenlasten (Überlauf), können auch Einfluss auf den aktuellen Standort von Daten haben. Kopien von Daten können an andere Datenzentren übertragen werden, um die Online-Verfügbarkeit im Falle von Störungen in einem Datenzentrum zu gewährleisten oder Sicherungskopien zu erstellen (Redundanz).

35. CC beruht auf vielen Kunden, die dynamisch einen gemeinsamen Pool an Ressourcen des Cloud-Anbieters nutzen. Dies sollte jedoch nur geschehen, wenn eine **klare Trennung** der verschiedenen Kundendaten und ihrer Verarbeitung aufrechterhalten werden kann. Die gemeinsame Nutzung von Ressourcen birgt ein höheres Risiko für umfangreiche Verluste oder die unbefugte Offenlegung von Daten.[15] Das Risiko erhöht sich auch dadurch, dass CC von der Kostenoptimierung durch ein großes Datenvolumen angetrieben wird (Skaleneffekt). Cloud-Kunden stellen ein Risiko für einander dar. Je mehr Kunden auf dieselben Ressourcen zugreifen, desto größer wird das Risiko für jeden einzelnen Kunden und somit für alle Cloud-Kunden zusammen.

36. Das Wissen über CC und Informationen über seine Risiken konzentrieren sich derzeit auf einige wenige große Cloud-Anbieter, die anscheinend aus wirtschaftlichen oder wettbewerblichen Gründen nur zögerlich Informationen über bestimmte Bedingungen und Umstände an die Öffentlichkeit weitergeben. Die ungleiche Verteilung von Wissen und Informationen zwischen Cloud-Anbietern und Kunden versetzt letztere in eine schwächere Po-

[15] Auf den Seiten 9 und 10 ihres Berichts *Cloud Computing – Benefits, risks and recommendations for information security* [Cloud Computing: Nutzen, Risiken und Empfehlungen zur Informationssicherheit] vom November 2009 nennt die ENISA die häufigsten Sicherheitsrisiken. Dazu zählen in zufälliger Reihenfolge: Kontrollverlust, Abhängigkeit von einem Anbieter (Lock-in-Effekt), fehlende Isolation, Datenschutz, unsichere oder unvollständige Löschung von Daten, interne Angreifer. Weitere Einzelheiten können dem Bericht entnommen werden. An dieser Stelle sei darauf hingewiesen, dass fehlende Isolation als eines der größten Risiken angesehen wird.

sition beim Abschluss von Vereinbarungen und erschwert es ihnen, die Risiken der beabsichtigten Nutzung von CC angemessen zu bewerten.

37. Eine gründliche **Risikoabschätzung** muss auf **dem Verständnis des** konkreten Aufbaus und der konkreten Umstände des Cloud-Dienstes an allen Standorten beruhen, an denen Daten verarbeitet werden.

38. Die CC-Technologie ist **grenzenlos** und **grenzüberschreitend**. Der weltweite Kundenstamm, gepaart mit der weltweiten Verteilung von Rechenzentren und dem dynamischen Strom von Daten (und von Datenverarbeitung) kann dazu führen, dass Daten nationale Grenzen überschreiten und Hoheitsgebiete mit einem damit einhergehenden Mangel an Transparenz wechseln. Personenbezogene Daten können in Datenzentren in Hoheitsgebieten ohne angemessenen Datenschutz gelangen oder kommerziell missbraucht werden, oder ausländische Mächte greifen ohne Berechtigung darauf zu.[16]

39. Im Sinne des Datenschutzes muss zwischen den einander ausschließenden Rollen des für die Verarbeitung Verantwortlichen und des Auftragsdatenverarbeiters unterschieden werden. Der **für die Verarbeitung Verantwortliche** legt den Zweck und die Mittel für einen bestimmten Vorgang der Datenverarbeitung fest.

40. Allgemein anerkannt ist auch, dass ein für die Verarbeitung Verantwortlicher die Verarbeitung personenbezogener Daten durch einen **Auftragsdatenverarbeiter** erlauben kann, dies jedoch nur in Einklang mit den ausdrücklichen **Weisungen** des für die Verarbeitung Verantwortlichen.

41. Ein allgemein anerkannter Grundsatz des Datenschutzes ist, dass der Auftragsdatenverarbeiter personenbezogene Daten nicht in größerem Umfang verarbeiten darf, als sich aus den ausdrücklichen Weisungen des für die Verarbeitung Verantwortlichen ableiten lässt[17]. Für das CC bedeutet dies, dass ein Cloud-Anbieter keine einseitige Entscheidung treffen oder die mehr oder weniger automatische Übertragung personenbezogener Daten (und ihrer Verarbeitung) an unbekannte Rechenzentren veranlassen kann. Dies gilt unabhängig davon, ob der Cloud-Anbieter eine solche Übertragung mit der Verringerung der Betriebskosten, der Bewältigung von Spitzenlasten (Überlauf), der Lastenverteilung, der Erstellung von Sicherungskopien usw. begründet.

---

16 Zwar können personenbezogene Daten in einem Hoheitsgebiet verarbeitet werden, doch kann der Cloud-Anbieter oder das Mutterunternehmen in einem anderen Hoheitsgebiet angesiedelt sein, was es ausländischen Strafverfolgungsbehörden ermöglichen würde, auf die Daten im Cloud-Dienst zuzugreifen, auch wenn die Daten physisch außerhalb der geografischen Grenzen dieses Landes gespeichert sind. Hierzu könnte der Abschluss eines internationalen Abkommens notwendig sein.

17 Oder durch Gesetz.

Noch darf der Cloud-Anbieter personenbezogene Daten für seine eigenen Zwecke nutzen[18].

42. Ein weiterer allgemein anerkannter Grundsatz des Datenschutzes erfordert, dass der für die Verarbeitung Verantwortliche geeignete **technische und organisatorische Sicherheitsmaßnahmen** ergreift, um Daten vor versehentlicher oder rechtswidriger Zerstörung, Verlust oder Schädigung, sowie vor unbefugter Offenlegung, Missbrauch oder anderen Arten der Verarbeitung, die gegen gesetzliche Bestimmungen verstoßen, zu schützen. Dasselbe gilt für Auftragsdatenverarbeiter.

43. Um seiner Verantwortung gerecht zu werden, muss der für die Verarbeitung Verantwortliche die Verarbeitung durch den Auftragsdatenverarbeiter **überwachen**, um sicherzustellen, dass sie entsprechend seiner Anweisungen erfolgt und dabei angemessene Sicherheitsmaßstäbe eingehalten werden.

44. Ohne seine Verantwortung abzutreten kann der für die Verarbeitung Verantwortliche ausdrückliche Anweisungen geben, dass die Überwachung der Verarbeitung durch den Auftragsverarbeiter teilweise von einem **vertrauenswürdigen Dritten** (z. B. einem Prüfer) übernommen wird. Bedingung ist, dass der Dritte über die notwendigen Qualifikationen verfügt, unabhängig vom Auftragsverarbeiter ist, vollen Zugang zu und vollständigen Einblick in die Bedingungen und Umstände der Verarbeitung durch den Auftragsverarbeiter hat und dem für die Verarbeitung Verantwortlichen zuverlässig über seine Beobachtungen, Bewertungen und Schlussfolgerungen berichten kann.

Die Arbeitsgruppe wird die Entwicklungen im Bereich des Cloud Computing weiter verfolgen und das vorliegende Arbeitspapier ggf. aktualisieren.

[18] Verarbeiten Cloud-Anbieter Daten ohne Wissen des für die Verarbeitung Verantwortlichen, sollte der Cloud-Anbieter als Mitverantwortlicher für die Verarbeitung angesehen und als solcher für die unbefugte, unabhängige Datenverarbeitung zur Rechenschaft gezogen werden.

B. Dokumente zur Informationsfreiheit

I. Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließungen der 24. Konferenz am 12. Juni 2012 in Mainz

Informationsfreiheit auf europäischer Ebene ausbauen, nicht einschränken!

Mit Besorgnis nehmen die Informationsfreiheitsbeauftragten in Deutschland zur Kenntnis, dass der freie Zugang zu Dokumenten der Europäischen Union gemäß Verordnung 1049/2001 erneut in Frage gestellt wird. Bereits im Jahre 2008 hatte die Europäische Kommission mannigfaltige Vorschläge zu einer drastischen Einschränkung des Zugangs zu europäischen Dokumenten vorgelegt, deren Folge eine massive Reduzierung der gebotenen Transparenz des Handelns europäischer Institutionen gewesen wäre (vgl. Entschließung der Informationsfreiheitsbeauftragten in Deutschland vom 30. Juni 2008). Das Europäische Parlament forderte daraufhin zwar eine Stärkung der Informationsfreiheit, doch arbeiten die Mitgliedstaaten derzeit daran, genau das zu verhindern. Ein „Kompromisspapier" der dänischen Ratspräsidentschaft sah zuletzt vor, das Zugangsrecht zu Akten der Institutionen der Europäischen Union deutlich einzuschränken.

Während bislang alle Arten von Inhalten der Informationsfreiheit unterfallen, sollen zukünftig nur „formell übermittelte" Dossiers öffentlich einzusehen sein. Damit würden der Öffentlichkeit sämtliche Entwürfe oder Diskussionspapiere des Rats, der Kommission und des Parlaments vorenthalten. Dies würde auch Vertragsverletzungsverfahren, Wettbewerbs- und Kartellverfahren betreffen, die von hohem öffentlichem Interesse sind.

Die Konferenz lehnt die Ausnahme einzelner europäischer Institutionen von der Transparenzpflicht ab. Sie tritt dafür ein, dass insbesondere die Europäische Zentralbank und die Europäische Investitionsbank nicht nur hinsichtlich ihrer Verwaltungstätigkeiten auf mehr Transparenz verpflichtet werden.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an die Bundesregierung, sich im Europäischen Rat für mehr Transparenz einzusetzen. Verwaltung und Politik auf der Ebene der Europäischen Union dürfen nicht in bürokratische Geheimniskrämerei zurückfallen. Die Forderungen des

Europäischen Parlaments müssen endlich erfüllt werden. Gerade angesichts der zunehmenden Verantwortung, die den europäischen Institutionen von der gemeinsamen Außenpolitik bis zur Bewältigung der Finanzkrise zukommt, gilt es, alle Institutionen der Europäischen Union noch weiter zu öffnen. Denn: Vertrauen basiert auf Transparenz!

Mehr Transparenz bei der Wissenschaft – Offenlegung von Kooperationsverträgen –

Die Kooperation zwischen Wissenschaft und Wirtschaft hat eine lange Tradition. Dies gilt für gemeinsame Institute ebenso wie für Stiftungsprofessuren und sonstige Formen der Zusammenarbeit.

Unternehmensfinanzierte Forschung nimmt einen immer größeren Anteil an der Wissenschaft ein. Deutschlandweit sollen inzwischen 660 Lehrstühle direkt oder indirekt von Unternehmen finanziert sein. Oft sind Motivation und Umfang der Förderung für Außenstehende nicht erkennbar. Für eine Beurteilung der Forschungsergebnisse und deren Bewertung ist die Kenntnis dieser Hintergründe jedoch Voraussetzung. Die Freiheit von Forschung und Wissenschaft lebt von einer offenen Diskussion; Geheimhaltung engt diese Freiheiten ein.

Einer verborgenen Einflussnahme auf Forschungsgegenstände, Forschungsergebnisse und auf deren Veröffentlichung kann nur durch eine konsequente Politik der Offenheit begegnet werden. Kooperationsverträge zwischen Wissenschaft und Unternehmen sind grundsätzlich offenzulegen. Eine solche Veröffentlichungspflicht sollte mindestens die Identität der Drittmittelgeber, die Laufzeit der Projekte, den Förderumfang und die Einflussmöglichkeiten der Drittmittelgeber auf Forschungsziele und -ergebnisse umfassen. Die Pflicht zur Veröffentlichung der Verträge darf nur zurücktreten, soweit und solange die Bekanntgabe gesetzlich geschützte Interessen beeinträchtigt.

Die regelmäßige Offenlegung der Finanzierung von Forschungsprojekten ist nach Auffassung der Informationsfreiheitsbeauftragten ein geeignetes Instrument, um die Freiheit der Forschung zu schützen, indem einseitige Abhängigkeiten oder auch nur deren Anschein vermieden wird. Eine reine Selbstverpflichtung der Universitäten und Forschungseinrichtungen ist hierfür nicht ausreichend. Es bedarf vielmehr konsequenter Regelungen in den Informationsfreiheitsgesetzen des Bundes und der Länder.

2. Entschließungen der 25. Konferenz am 27. November 2012 in Mainz

Parlamente sollen in eigener Sache für mehr Transparenz sorgen!

Die Informationsfreiheitsgesetze von Bund und Ländern nehmen die Parlamente von den für sonstige öffentliche Stellen bestehenden Transparenzpflichten aus. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland sieht, dass der Kernbereich der Abgeordnetentätigkeit in der unabhängigen Wahrnehmung ihres Mandats nicht dem umfassenden Zugangsanspruch der Öffentlichkeit unterliegen kann. Defizite bei der Transparenz führen aber zu einem Verlust an öffentlicher Glaubwürdigkeit. Die Parlamente von Bund und Ländern sollten deshalb Vorreiter in Sachen Transparenz werden und Ausnahmen vom Informationszugang soweit wie möglich zurücknehmen.

In welchem Umfange Transparenz herzustellen ist, ist eine Frage des verfassungsrechtlich gebundenen, gesetzgeberischen Ermessens. Dieses verpflichtet die Parlamente dazu, die bereits vorhandenen Transparenzregelungen regelmäßig daraufhin zu überprüfen, ob sie sich bewährt haben oder ggf. zu konkretisieren und zu ergänzen sind.

Dabei sollten – soweit noch nicht geschehen – folgende Punkte berücksichtigt werden:

a. ein möglichst hohes Maß an Transparenz bei den weiteren Tätigkeiten und Einkünften von Abgeordneten unter Berücksichtigung von Berufsgeheimnissen. Den möglichen Besonderheiten des Mandats, insbesondere bei „Teilzeit"-Parlamenten, sollte Rechnung getragen werden,

b. Veröffentlichung von Tagesordnungen von Plena und Ausschüssen, ebenso Stellungnahmen, Protokolle und weitere Unterlagen, die Gegenstand der Beratungen sind,

c. Öffentlichkeit von Sitzungen der Fachausschüsse,

d. grundsätzliche Veröffentlichung von wissenschaftlichen Ausarbeitungen der Parlamentsdienste und sonstiger Gutachten,

e. Zugang zu Informationen über Beschaffungen, Reisen, Sachausgaben und sonstige kostenträchtige Vorhaben der Parlamente und ihrer Ausschüsse.

Mehr Transparenz bei Krankenhaushygienedaten

Das Vertrauen der Bevölkerung in das deutsche Gesundheitssystem, insbesondere in unsere Krankenhäuser, hat im Laufe der letzten Jahre abgenommen. Dies ist auch auf eine verbreitete Intransparenz zurückzuführen.

Zwar wurden in einem von einer Tageszeitung herausgegebenen Klinikführer Berlin-Brandenburg erstmals auch Hygienedaten veröffentlicht, jedoch nahmen nicht alle Krankenhäuser an der dieser Publikation zugrunde liegenden freiwilligen Datenerhebung teil. Das wurde unter anderem damit begründet, dass die nur zu internen Zwecken erhobenen Daten falsch interpretiert werden könnten und dass Patientinnen und Patienten möglicherweise andere Krankenhäuser wählen würden, wenn sie über entsprechende Vergleichsdaten verfügten.

Die Entscheidung für oder gegen ein bestimmtes Krankenhaus können die Patientinnen und Patienten aber nur dann verantwortlich treffen, wenn ihnen alle relevanten Parameter zur Verfügung stehen; dazu gehören auch die jeweiligen Hygienedaten und ihre Umsetzung in den einzelnen Kliniken. Nur eine standardisierte Melde- und Veröffentlichungspflicht für alle Hygienedaten ermöglicht es jedem Patienten und jeder Patientin, die jeweiligen Hygienestandards der Krankenhäuser zu bewerten und zu vergleichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher alle Verantwortlichen, insbesondere den Bundes- und die Landesgesetzgeber auf, für Transparenz bei Krankenhaushygienedaten zu sorgen. Dazu gehören auch standardisierte und weit reichende Melde- und Veröffentlichungspflichten und die Erweiterung der Qualitätsberichte der Krankenhäuser. Dies wäre ein wichtiger Schritt, um durch mehr Transparenz das Vertrauen der Bevölkerung in die Gesundheitsversorgung durch Krankenhäuser zu fördern.