

Denkschrift zu dem Protokoll vom 10. Oktober 2018 zur Änderung des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

A. Allgemeines

I. Entstehungsgeschichte

Die Konvention 108 des Europarats stammt aus dem Jahr 1981 und war das erste rechtsverbindliche zwischenstaatliche Übereinkommen zum Datenschutz. Die Konvention 108 enthält die wichtigsten Grundsätze des Datenschutzrechts. Neben den 47 Mitgliedstaaten des Europarats, zu denen alle EU-Mitgliedstaaten sowie eine Reihe weiterer Staaten wie etwa die Russische Föderation, die Türkei, die Schweiz und Norwegen gehören, haben bereits Mexiko, Uruguay, Mauritius, Senegal, Tunesien und Kap Verde die Konvention 108 ratifiziert. Die Konvention 108 hat damit – weit über Europa hinaus – Bedeutung für die globale Entwicklung des Datenschutzrechts.

Angesichts der gewaltigen technologischen Entwicklungen seit den 1980er Jahren war eine Modernisierung der Konvention 108 einschließlich ihres Zusatzprotokolls aus dem Jahr 2001 erforderlich. Nach mehrjährigen Verhandlungen haben sich die Konventionsstaaten auf ein Änderungsprotokoll geeinigt, das die Konvention 108 zukunftsfähig macht. Die Verhandlungen erstreckten sich auch deshalb über mehrere Jahre, da sichergestellt werden sollte, dass das Änderungsprotokoll vollständig kohärent mit dem aktuellen EU-Datenschutzrecht ist, welches 2016 in Kraft trat (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) und Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

II. Würdigung des Protokolls

Ziel des Änderungsprotokolls ist die Modernisierung und Verbesserung des Übereinkommens (SEV Nr. 108) unter Berücksichtigung der seit seiner Verabschiedung im Jahr 1980 zutage getretenen neuen Herausforderungen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Gegenstand der Aktualisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, dem einzigen völkerrechtlich bindenden Vertrag mit weltweiter Bedeutung auf diesem Gebiet, sind die Herausforderungen, welche die Verwendung neuer Informations- und Kommunikationstechnologien für den Schutz der Privatsphäre darstellen, sowie die Stärkung des Konventionsmechanismus zur Gewährleistung ihrer wirksamen Umsetzung.

Das Protokoll schafft einen soliden und flexiblen multilateralen Rechtsrahmen, der den grenzüberschreitenden Datenverkehr erleichtern und dabei wirksame Schutzmechanismen bei der Verwendung personenbezogener Daten garantieren soll. Es bildet eine Brücke zwischen verschiedenen Regionen der Welt und ein Bindeglied zwischen unterschiedlichen normativen Rahmen, darunter der neuen Gesetzgebung der Europäischen Union, die seit dem 25. Mai 2018 verbindlich anzuwenden ist und im Zusammenhang mit grenzüberschreitendem Datenverkehr auf die Konvention 108 Bezug nimmt.

Das Protokoll enthält u. a. folgende Neuerungen:

- höhere Anforderungen hinsichtlich der Grundsätze der Verhältnismäßigkeit und der Datenminimierung sowie der Rechtmäßigkeit der Verarbeitung;
- Erweiterung der Kategorien sensibler Daten, welche nunmehr auch genetische und biometrische Daten sowie Daten bezüglich Gewerkschaftsmitgliedschaft und ethnischer Herkunft umfassen;
- Verpflichtung, Datenschutzverstöße zu melden;
- größere Transparenz bei der Datenverarbeitung;
- neue Rechte für Personen im Zusammenhang mit algorithmischen Entscheidungsprozessen, was besonders im Rahmen der Entwicklung künstlicher Intelligenz von Bedeutung ist;
- Stärkung der Rechenschaftspflicht der für die Datenverarbeitung Verantwortlichen;
- verbindliche Anwendung des Grundsatzes des „eingebauten Datenschutzes“;
- Anwendung der Datenschutzgrundsätze auf alle Datenverarbeitungstätigkeiten, einschließlich jener aus Gründen der nationalen Sicherheit, für die Ausnahmen und Einschränkungen gemäß den im Übereinkommen festgelegten Bedingungen möglich sind

und die in jedem Fall einer unabhängigen und wirksamen Prüfung und Überwachung unterliegen sollten;

- klares Regelwerk für grenzüberschreitenden Datenverkehr;
- Stärkung der Befugnisse und der Unabhängigkeit der Datenschutzbehörden und Weiterentwicklung der Rechtsgrundlage für die internationale Zusammenarbeit;
- auch die Europäische Union kann die Konvention 108 unterzeichnen.

B. Besonderes

Zu den Bestimmungen der Konvention 108 in der Fassung des Protokolls im Einzelnen:

Zur Präambel

Die Präambel bekräftigt das Bekenntnis der Unterzeichnerstaaten zu den Menschenrechten und Grundfreiheiten.

Ein wesentliches Ziel des Übereinkommens ist es, jeden Menschen in die Lage zu versetzen, über die Verarbeitung seiner personenbezogenen Daten durch Dritte Kenntnis zu erlangen und diese bestimmen zu können. Dementsprechend enthält die Präambel einen ausdrücklichen Verweis auf die Entscheidungsfreiheit und das Recht jedes Menschen, selbst über seine personenbezogenen Daten zu bestimmen, was sich insbesondere aus dem Recht auf Privatsphäre und die Würde des Menschen ableitet. Für die Würde des Menschen sind bei der Verarbeitung personenbezogener Daten Sicherheitsvorkehrungen erforderlich, damit Menschen nicht als bloße Objekte behandelt werden.

Angesichts der Bedeutung des Rechts auf Schutz personenbezogener Daten in Bezug auf dessen gesellschaftliche Rolle wird in der Präambel hervorgehoben, dass die Interessen, Rechte und Grundfreiheiten der Menschen miteinander in Einklang zu bringen sind. Um die verschiedenen Interessen, Rechte und Grundfreiheiten vorsichtig in ein Gleichgewicht zu bringen, sind in dem Übereinkommen bestimmte Bedingungen und Beschränkungen für die Verarbeitung von Informationen und den Schutz personenbezogener Daten festgelegt. So ist beispielsweise das Recht auf Datenschutz im Zusammenhang mit dem Recht der freien Meinungsäußerung zu betrachten, das in Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte (SEV Nr. 5) festgelegt ist und die Meinungsfreiheit und die Freiheit, Informationen zu empfangen und weiterzugeben, einschließt. Im Übrigen bestätigt das Übereinkommen, dass die Wahrnehmung des Rechts auf Datenschutz, das nicht absolut ist, nicht allgemein herangezogen werden sollte, um den öffentlichen Zugang zu amtlichen Dokumenten zu verhindern.¹

Durch die im Übereinkommen Nr. 108 festgelegten Grundsätze und Werte wird der Einzelne geschützt und gleichzeitig ein Rahmen für den internationalen Datenverkehr geschaffen. Dies ist angesichts der wachsenden Bedeutung globaler Informationsflüsse in der modernen Gesellschaft besonders wichtig, um die Ausübung der Grundrechte und Grundfreiheiten zu ermöglichen und gleichzeitig Innovationen anzuregen und gesellschaftlichen und wirtschaftlichen Fortschritt zu fördern und dabei die öffentliche Sicherheit zu gewährleisten. Bei dem Verkehr von personenbezogenen Daten in einer Informations- und Kommunikationsgesellschaft

¹ Siehe Konvention des Europarates über den Zugang zu amtlichen Dokumenten (SEV-Nr. 205).

müssen die Grundrechte und Grundfreiheiten des Einzelnen gewahrt bleiben. Auch bei der Entwicklung und Nutzung innovativer Technologien sollten diese Rechte beachtet werden. Dies wird dazu beitragen, Vertrauen in Innovationen und neue Technologien zu schaffen und deren Weiterentwicklung zu fördern.

Da die internationale Zusammenarbeit zwischen Aufsichtsbehörden ein Schlüssel für den wirksamen Schutz des Einzelnen ist, zielt das Übereinkommen darauf ab, diese Zusammenarbeit zu stärken, insbesondere, indem die Parteien zu gegenseitiger Hilfeleistung aufgefordert werden und indem es eine geeignete Rechtsgrundlage bietet für die Zusammenarbeit und den Austausch von Informationen für Ermittlungen und Strafverfolgung.

Zu Kapitel I

Allgemeine Bestimmungen

Zu Artikel 1 – Ziel und Zweck

In Artikel 1 werden das Ziel und der Zweck des Übereinkommens beschrieben. Der Schwerpunkt liegt dabei auf dem Schutzaspekt: Jedermann muss geschützt werden, wenn seine personenbezogenen Daten verarbeitet werden.² Kürzlich wurde der Datenschutz als ein Grundrecht in Artikel 8 der Charta der Grundrechte der Europäischen Union und in die Verfassungen einiger Unterzeichner des Übereinkommens aufgenommen.

Die in dem Übereinkommen festgelegten Garantien werden auf jeden Menschen, unabhängig von seiner Nationalität oder seinem Wohnsitz, ausgedehnt. Bei der Anwendung dieser Garantien darf nicht zwischen Staatsangehörigen und Drittausländern unterschieden werden.³ Klauseln, die den Datenschutz auf eigene Staatsangehörige oder rechtmäßig aufhältige ausländische Staatsangehörige beschränken, wären mit dem Übereinkommen unvereinbar.

Zu Artikel 2 – Begriffsbestimmungen

Mit den Begriffsbestimmungen in dem Übereinkommen soll die einheitliche Verwendung von Begriffen zur Beschreibung bestimmter Grundkonzepte in einzelstaatlichen Rechtsvorschriften sichergestellt werden.

Buchstabe a – „personenbezogene Daten“

„Bestimmbare natürliche Person“ bedeutet eine Person, die unmittelbar oder mittelbar identifiziert werden kann. Eine Person gilt als nicht bestimmbar, wenn für ihre Identifizierung ein unverhältnismäßig hoher Aufwand an Zeit, Mühe und sonstigen Ressourcen nötig ist. Dies ist der Fall, wenn beispielsweise für die Identifizierung eines Betroffenen übermäßig komplexe, langwierige und kostenintensive Tätigkeiten nötig wären. Die Frage, was einen „unverhältnismäßig hohen Aufwand an Zeit, Mühe und sonstigen Ressourcen“ darstellt, sollte im Einzelfall bewertet werden. In Erwägung gezogen werden könnten beispielsweise der Zweck der Datenverarbeitung sowie objektive Kriterien wie die Kosten, der Nutzen einer solchen Identifizierung, die Art des Verantwortlichen, die verwendete Technologie usw. Durch technische und sonstige

² „Der Schutz personenbezogener Daten ist von grundlegender Bedeutung für die Ausübung des Rechts jedes Einzelnen auf Privat- und Familienleben, wie es in Artikel 8 garantiert ist“ - EGMR MS v. Schweden, (Anwendung Nr. 20837(92), 1997, Rdnr. 41.

³ Siehe Menschenrechtskommissar des Europarats, Die Rechtsstaatlichkeit im Internet und in der weiteren digitalen Welt (The rule of law on the Internet and in the wider digital world), Thesenpapier, [CommDH/IssuePaper\(2014\)1](#), 8. Dezember 2014, S. 48, Ziffer 3.3 Jedermann frei von Diskriminierung ('Everyone' without discrimination).

Entwicklungen können sich im Übrigen Änderungen hinsichtlich der Auslegung der Formulierung „unverhältnismäßig hoher Aufwand an Zeit, Mühe und sonstigen Ressourcen“ ergeben.

Der Begriff „bestimmbar“ bezieht sich nicht nur auf die zivile oder rechtliche Identität einer Person, sondern auch auf Merkmale, anhand derer eine „Individualisierung“ oder eine Unterscheidung (und damit eine unterschiedliche Behandlung) einer Person möglich ist. Diese „Individualisierung“ kann beispielsweise erfolgen, indem konkret auf ihn oder sie Bezug genommen wird oder auf ein Gerät oder eine Kombination von Geräten (Computer, Mobiltelefon, Kamera, Spielgeräte usw.) auf der Grundlage einer Identifikationsnummer, eines Pseudonyms, biometrischer oder genetischer Daten, Standortdaten, einer IP-Adresse oder sonstiger Merkmale. Die Verwendung eines Pseudonyms oder eines digitalen Merkmals / einer digitalen Identität führt nicht zur Anonymisierung der Daten, da die betroffene Person nach wie vor identifiziert oder individuell betrachtet werden kann. Pseudonyme Daten gelten daher als personenbezogene Daten und fallen unter die Bestimmungen des Übereinkommens. Bei der Bewertung, ob die getroffenen Sicherheitsvorkehrungen zur Minderung der Risiken für betroffene Personen geeignet sind, sollte die Qualität der Pseudonymisierungstechniken hinreichend Berücksichtigung finden.

Daten gelten nur dann als anonym, solange es nicht möglich ist, den Personenbezug wiederherstellen zu können oder solange diese erneute Identifizierung einen unverhältnismäßigen Aufwand an Zeit, Mühe oder Ressourcen erfordern würde, unter Berücksichtigung der zum Zeitpunkt der Verarbeitung verfügbaren Technologie und der technischen Entwicklungen. Auch bei Daten, die anonym zu sein scheinen, weil sie kein offensichtliches Identifizierungsmerkmal enthalten, lässt sich in bestimmten Fällen (ohne unzumutbaren Aufwand an Zeit, Mühe oder Ressourcen) der Personenbezug herstellen. Dies ist beispielsweise dann der Fall, wenn der Datenverarbeiter oder eine andere Person die Person identifizieren kann, indem unterschiedliche Arten von Daten miteinander kombiniert werden, wie physische, physiologische, genetische, ökonomische oder soziale Daten (Kombination von Daten zu Alter, Geschlecht, Beschäftigung, Geolokalisierung, Familienstand usw.). Dann können Daten nicht als anonym gelten und fallen demnach unter die Bestimmungen des Übereinkommens.

Bei der Anonymisierung von Daten sollten durch den Einsatz vor allem sämtlicher technischer Möglichkeiten geeignete Vorkehrungen getroffen werden, um sicherzustellen, dass der Personenbezug nicht mehr herstellbar ist. Angesichts der rasanten technologischen Entwicklungen sollten diese Vorkehrungen regelmäßig überprüft und evaluiert werden.

Buchstaben b und c – „Datenverarbeitung“

„Datenverarbeitung“ beginnt mit der Erhebung von personenbezogenen Daten und umfasst alle Vorgänge, die im Zusammenhang mit personenbezogenen Daten ausgeführt werden, ganz gleich, ob teilweise oder vollständig automatisiert. Sofern keine automatische Verarbeitung stattfindet, bedeutet ‚Datenverarbeitung‘ einen Vorgang oder eine Vorgangsreihe im Zusammenhang mit personenbezogenen Daten innerhalb einer strukturierten Reihe solcher Daten, auf die nach spezifischen Kriterien zugegriffen oder die nach spezifischen Kriterien ausgelesen werden können, wodurch es für den Datenverarbeiter oder eine andere Person möglich ist, die mit einer betroffenen Person in Bezug stehenden Daten zu durchsuchen, zu kombinieren oder miteinander in Beziehung zu setzen.

Buchstabe d – „der für die Verarbeitung Verantwortliche“

„Der für die Verarbeitung Verantwortliche“ bezeichnet die Person oder Stelle, die befugt ist, über die Zwecke und Mittel der Verarbeitung zu entscheiden, wobei diese Befugnis aus einer gesetzlichen Benennung oder tatsächlichen Umständen, die im Einzelfall zu bewerten sind, abgeleitet sein kann. In einigen Fällen kann es mehrere Verantwortliche oder Ko-Verantwortliche für die Datenverarbeitung geben (die gemeinsam für die Verarbeitung zuständig sind und möglicherweise für verschiedene Aspekte dieser Datenverarbeitung zuständig sind). Bei der Beurteilung, ob eine Person oder Stelle für die Datenverarbeitung verantwortlich ist, sollte vor allem geprüft werden, ob diese Person oder Stelle die Gründe bestimmt, die eine Verarbeitung rechtfertigen, beziehungsweise die Zwecke der Datenverarbeitung und die dafür verwendeten Mittel. Ebenfalls relevant für diese Beurteilung ist es, ob die Person oder Stelle über die Verarbeitungsmethoden, die Auswahl der zu verarbeitenden Daten und die Regelung des Zugangs dazu bestimmen kann. Diejenigen, die nicht unmittelbar der für die Datenverarbeitung verantwortlichen Person oder Stelle unterstehen und die Verarbeitung im Auftrag und ausschließlich entsprechend den Anweisungen dieser verantwortlichen Person oder Stelle durchführen, gelten als Auftragsverarbeiter. Auch in diesem Fall, wenn ein Auftragsverarbeiter die Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, behält der für die Verarbeitung Verantwortliche die Verantwortung für die Datenverarbeitung.

Buchstabe e – „Empfänger“

Der „Empfänger“ ist eine Person oder Stelle, die personenbezogene Daten empfängt oder der personenbezogene Daten zur Verfügung gestellt werden. Je nach den Umständen kann es sich dabei um einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter handeln. Beispielsweise kann ein Unternehmen bestimmte Daten von Beschäftigten an eine staatliche Stelle übermitteln, die diese Daten als eine für die Verarbeitung verantwortliche Stelle für steuerliche Zwecke verarbeitet. Es kann die Daten aber auch an ein Unternehmen übermitteln, das Dienstleistungen für die Datenspeicherung anbietet oder das als ein Auftragsverarbeiter fungiert. Handelt es sich bei dem Empfänger jedoch um eine Behörde oder eine Stelle, der das Recht zur Wahrnehmung öffentlicher Aufgaben eingeräumt wurde, bei der die empfangenen Daten jedoch im Rahmen eines bestimmten Untersuchungsauftrags nach geltendem Recht verarbeitet werden, gilt diese Behörde oder Stelle nicht als Empfänger. Anträge auf Offenlegung, die von Behörden ausgehen, sollten immer schriftlich erfolgen, mit Gründen versehen sein und gelegentlichen Charakter haben, und sie sollten nicht vollständige Dateisysteme betreffen oder zur Verknüpfung von Dateisystemen führen. Die Verarbeitung personenbezogener Daten durch die genannten Behörden sollte für die Zwecke der Verarbeitung geltenden Datenschutzvorschriften entsprechen.

Buchstabe f – „Auftragsverarbeiter“

Ein „Auftragsverarbeiter“ ist eine natürliche oder juristische Person (bei der es sich nicht um einen Beschäftigten des für die Verarbeitung Verantwortlichen handelt), die im Auftrag und entsprechend den Anweisungen der für die Verarbeitung verantwortlichen Person / Stelle Daten verarbeitet. Was der Auftragsverarbeiter mit den personenbezogenen Daten machen darf, richtet sich nach den Anweisungen des für die Verarbeitung Verantwortlichen.

Zu Artikel 3 – Anwendungsbereich

Nach Absatz 1 soll jede Vertragspartei das Übereinkommen auf die unter ihrer Hoheitsgewalt im öffentlichen und privaten Bereich erfolgende Datenverarbeitung anwenden.

Das Bestreben nach Beständigkeit über einen längeren Zeitraum und unter Berücksichtigung des technologischen Fortschritts rechtfertigt den Hinweis auf die Hoheitsgewalt der Vertragsparteien.

Nach Absatz 2 ist die Datenverarbeitung, die zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird, vom Geltungsbereich des Übereinkommens ausgenommen. Mit diesem Ausschluss soll vermieden werden, dass Einzelpersonen für die Datenverarbeitung in ihrer Privatsphäre für die Ausübung von Tätigkeiten, die mit der Gestaltung ihres Privatlebens zusammenhängen, unverhältnismäßige Verpflichtungen auferlegt werden. Persönliche oder familiäre Tätigkeiten sind solche, die eng und objektiv an das Privatleben einer Einzelperson gekoppelt sind und die Privatsphäre anderer nicht wesentlich beeinträchtigen. Diese Tätigkeiten haben keinen beruflichen oder kommerziellen Hintergrund und beziehen sich lediglich auf persönliche oder familiäre Tätigkeiten, wie das Speichern von Familienfotos oder privaten Fotos auf einem Computer, das Erstellen einer Liste mit Kontaktdaten von Freunden und Angehörigen, Korrespondenz usw. Der Austausch von Daten im privaten Bereich umfasst vor allem den Austausch innerhalb der Familie, innerhalb eines begrenzten Freundeskreises oder eines begrenzten Kreises auf der Grundlage einer persönlichen Beziehung oder eines bestimmten Vertrauensverhältnisses.

Ob Tätigkeiten „rein persönliche oder familiäre Tätigkeiten“ sind, hängt von den Umständen ab. Der Ausschluss gilt jedoch nicht, wenn personenbezogene Daten einer großen Zahl von Personen oder Personen, die offensichtlich außerhalb der Privatsphäre stehen, wie beispielsweise auf einer Website im Internet, zugänglich gemacht werden. Ähnlich verhält es sich mit dem Betrieb einer Kameraanlage, mit deren Hilfe Videoaufnahmen von Menschen auf einem Dauerspeichermedium, wie beispielsweise eine Festplatte, gespeichert werden, die von einer Einzelperson in ihrem Haus zum Zweck des Schutzes des Eigentums, der Gesundheit oder des Lebens der Hauseigentümer installiert wurde, die jedoch – wenn auch nur teilweise – einen Bereich des öffentlichen Raums erfasst und vom Privatbereich der die Daten auf diese Weise verarbeitenden Person nach außen gerichtet ist: Dies kann nicht als eine „rein persönliche oder familiäre Tätigkeit“ angesehen werden.⁴

Das Übereinkommen gilt jedoch für die Datenverarbeitung, die von Anbietern durchgeführt wird, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.

Während das Übereinkommen die Datenverarbeitung im Zusammenhang mit Einzelpersonen betrifft, können die Vertragsparteien des Übereinkommens ihr innerstaatliches Recht erweitern und auch auf den Schutz der rechtmäßigen Interessen von juristischen Personen ausdehnen. Das Übereinkommen gilt für lebende Menschen: Es soll nicht für personenbezogene Daten Verstorbener gelten. Das nimmt den Vertragsparteien jedoch nicht die Möglichkeit, den Schutz auch auf Verstorbene auszudehnen.

Zu Kapitel II

Grundsätze für den Schutz personenbezogener Daten

Zu Artikel 4 – Pflichten der Vertragsparteien

⁴ Siehe Europäischer Gerichtshof, Frantisek Rynes v. Urad, 11. Dezember 2014, C-212/13k.

Nach diesem Artikel sind die Vertragsparteien verpflichtet, die Bestimmungen des Übereinkommens in ihr Recht aufzunehmen und ihnen in der Praxis Wirksamkeit zu verleihen. Wie dies getan wird, hängt von der geltenden Rechtsordnung und dem für die Einbindung völkerrechtlicher Übereinkünfte gewählten Ansatz ab.

Der Begriff „Recht der Vertragsparteien“ bezeichnet, je nach der Rechts- und Verfassungsordnung des jeweiligen Landes, alle durchsetzbaren Regeln sowohl des geschriebenen Rechts als auch des Fallrechts. Dabei müssen die qualitativen Anforderungen an die Zugänglichkeit und Vorhersehbarkeit erfüllt sein. Das schließt ein, dass das Recht hinreichend klar sein muss, damit alle Personen und sonstigen Stellen die Möglichkeit haben, ihr eigenes Verhalten im Lichte der erwarteten Rechtsfolgen zu steuern und damit die Personen, die wahrscheinlich von dem Recht betroffen sein werden, Zugriff darauf haben. Dies umfasst Regeln, durch die Personen (sowohl natürlichen als auch juristischen Personen) Pflichten auferlegt und Rechte verliehen werden oder mit denen die Organisation, die Befugnisse und Zuständigkeiten von Behörden bestimmt oder Verfahren festgelegt werden. Dazu gehören insbesondere die Verfassungen von Staaten und sämtliche geschriebenen Gesetze (Gesetze im formalen Sinne) sowie Regulationsmaßnahmen (Erlasse, Verordnungen, Anordnungen und Verwaltungsvorschriften) auf der Grundlage dieser Gesetze. Abgedeckt sind ebenfalls internationale Übereinkommen, die in innerstaatliches Recht umgesetzt werden müssen, einschließlich EU-Recht. Außerdem umfasst es alle sonstigen Gesetze allgemeiner Natur, ob öffentliches Recht oder Privatrecht (einschließlich Vertragsrecht), sowie in Ländern mit Gewohnheitsrecht die Rechtsprechung und in allen Ländern die ständige Rechtsprechung über die Auslegung des kodifizierten Rechts. Es umfasst jedes Gesetz eines professionellen Gremiums mit delegierten Rechtsetzungsbefugnissen und in Übereinstimmung mit dessen unabhängigen Gesetzgebungskompetenzen.

Dieses „Recht der Vertragsparteien“ kann auf nützliche Weise durch freiwillige Regulationsmaßnahmen im Bereich des Datenschutzes gestärkt werden, wie durch Verhaltenskodizes oder berufssübliche Verhaltensregeln. Solche freiwilligen Maßnahmen sind jedoch selbst nicht ausreichend, um die vollständige Einhaltung des Übereinkommens sicherzustellen.

Wenn internationale Organisationen betroffen sind⁵, so kann das Recht dieser internationalen Organisationen auch unmittelbar auf nationaler Ebene der Mitgliedstaaten dieser Organisationen angewendet werden, je nach der jeweiligen nationalen Rechtsordnung.

Die Effektivität der Anwendung der Maßnahmen, mit denen den Bestimmungen des Übereinkommens Wirksamkeit verliehen wird, ist von entscheidender Bedeutung. Bei der Gesamtbeurteilung der Effektivität der Umsetzung der Bestimmungen des Übereinkommens durch eine Vertragspartei sollten sowohl die Rolle der Aufsichtsbehörde (oder Behörden) als auch die den Rechtssubjekten zur Verfügung stehenden Rechtsbehelfe betrachtet werden. Nach Absatz 2 müssen die Maßnahmen, mit denen dem Übereinkommen Wirksamkeit verliehen wird, von jeder Vertragspartei getroffen werden und bis zum Zeitpunkt der Ratifikation dieses Übereinkommens oder des Beitritts dazu, d. h. wenn das Übereinkommen für eine Vertragspartei verbindlich wird, in Kraft getreten sein. Mit dieser Bestimmung soll der Übereinkommensausschuss in die Lage versetzt werden zu bewerten, ob alle „notwendigen Maßnahmen“ getroffen wurden, um sicherzustellen, dass die Vertragsparteien des Übereinkommens

⁵ Internationale Organisationen sind definiert als Organisationen, die dem Völkerrecht unterliegen.

ihre Verpflichtungen einhalten und in ihrem innerstaatlichen Recht das erwartete Datenschutzniveau sicherstellen. Das Verfahren für diese Verifizierung und die dabei verwendeten Kriterien müssen in der Verfahrensordnung des Übereinkommensausschusses klar definiert sein.

In Absatz 3 verpflichten sich die Vertragsparteien, die Bewertung der Erfüllung ihrer Verpflichtungen aktiv zu unterstützen mit dem Ziel, eine regelmäßige Bewertung der Umsetzung der Grundsätze des Übereinkommens (einschließlich seiner Wirksamkeit) sicherzustellen. Die Vorlage von Berichten durch die Vertragsparteien über die Anwendung ihres Datenschutzrechts könnte ein mögliches Element dieser aktiven Unterstützung sein.

Bei der Ausübung seiner Befugnisse nach Absatz 3 soll der Übereinkommensausschuss nicht bewerten, ob eine Vertragspartei wirksame Maßnahmen insoweit ergriffen hat, als sie von Ausnahmen und Beschränkungen gemäß den Bestimmungen des Übereinkommens Gebrauch gemacht hat. Aus Artikel 11 Absatz 3 folgt, dass von einer Vertragspartei nicht verlangt werden kann, dass sie dem Übereinkommensausschuss eingestufte Informationen zur Verfügung stellt.

Die Bewertung, ob eine Vertragspartei das Übereinkommen erfüllt, erfolgt durch den Übereinkommensausschuss auf der Grundlage eines objektiven, fairen und transparenten Verfahrens, das der Übereinkommensausschuss festlegt und in seiner Verfahrensordnung umfassend erläutert.

Zu Artikel 5 – Rechtmäßigkeit der Datenverarbeitung und Qualität der Daten

Nach Absatz 1 muss die Datenverarbeitung verhältnismäßig sein, d. h. angemessen im Verhältnis zu dem verfolgten rechtmäßigen Zweck und unter Berücksichtigung der Interessen, Rechte und Freiheiten der betroffenen Person oder öffentlicher Interessen. Durch die Datenverarbeitung soll es nicht zu unverhältnismäßigen Eingriffen in diese Interessen, Rechte und Freiheiten kommen. Der Grundsatz der Verhältnismäßigkeit ist in allen Stufen der Verarbeitung zu wahren, einschließlich der Vorstufe, d. h. zum Zeitpunkt der Entscheidung über die Durchführung der Datenverarbeitung.

Nach Absatz 2 müssen zwei wesentliche Voraussetzungen für eine rechtmäßige Verarbeitung vorliegen: die Einwilligung der betroffenen Person oder eine rechtmäßige, gesetzlich geregelte Grundlage. Die Absätze 1, 2, 3 und 4 des Artikels 5 sind kumulativ und müssen zur Wahrung der Rechtmäßigkeit der Datenverarbeitung gewahrt werden.

Die Einwilligung der betroffenen Person muss freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich erfolgen. Bei dieser Einwilligung muss es sich um die freie Äußerung einer bewussten Wahl handeln, die entweder durch Erklärung (schriftlich, auch auf elektronischem Wege, oder mündlich) abgegeben wird oder durch eine eindeutige bestätigende Handlung, die in diesem konkreten Zusammenhang eindeutig das Einverständnis mit der vorgeschlagenen Verarbeitung von personenbezogenen Daten anzeigt. Bloßes Schweigen, Inaktivität oder vorab validierte Formulare sollten daher nicht als Einwilligung gelten. Die Einwilligung sollte sich auf sämtliche Verarbeitungstätigkeiten beziehen, die für denselben Zweck oder dieselben Zwecke durchgeführt werden (im Falle mehrerer Zwecke sollte die Einwilligung für jeden Zweck einzeln gegeben werden). Es kann vorkommen, dass die betroffene Person unterschiedliche Entscheidungen hinsichtlich ihrer Einwilligung trifft (z. B. wenn sich die Art der Daten unterscheidet, obwohl der Zweck derselbe ist, wie beispielsweise bei Gesundheitsdaten und Aufenthaltsdaten: In solch einem Fall kann die betroffene Person der Ver-

arbeitung von ihren Aufenthaltsdaten zustimmen, nicht jedoch der Verarbeitung ihrer Gesundheitsdaten). Die betroffene Person muss über die Auswirkungen ihrer Entscheidung aufgeklärt werden (über die Folgen der Einwilligung und den Umfang der Einwilligung). Auf die betroffene Person darf weder direkt noch indirekt Einfluss genommen oder Druck (wirtschaftlicher oder sonstiger Art) ausgeübt werden, und Einverständniserklärungen, bei denen die betroffene Person keine echte oder freie Wahl hatte oder ihr Einverständnis nicht unbeschadet ablehnen oder widerrufen konnte, sollten nicht als freiwillig abgegeben gelten.

Im Rahmen wissenschaftlicher Forschung kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten oftmals nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.

Eine Einwilligung bedeutet keinen Verzicht auf die Wahrung der Grundsätze für den Schutz von personenbezogenen Daten nach Kapitel II des Übereinkommens, und die Verhältnismäßigkeit der Verarbeitung muss trotzdem berücksichtigt werden.

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zurückzunehmen (was zu unterscheiden ist von dem gesonderten Recht, die Verarbeitung abzulehnen). Die Rechtmäßigkeit der Datenverarbeitung, die erfolgt ist, bevor der für die Verarbeitung Verantwortliche die Erklärung über die Zurücknahme der Einwilligung erhalten hat, bleibt von der Zurücknahme der Einwilligung unberührt. Die Fortsetzung der Datenverarbeitung ist jedoch nicht gestattet, sofern sie nicht auf einer anderen rechtmäßigen, gesetzlich geregelten Grundlage durchgeführt werden kann.

Der in Absatz 2 enthaltene Begriff der „rechtmäßigen, gesetzlich geregelten Grundlage“ umfasst u. a. die Verarbeitung zum Zweck der Erfüllung eines Vertrags (oder vorvertraglicher Maßnahmen auf Ersuchen der betroffenen Person), dessen Vertragspartei die betroffene Person ist, die Datenverarbeitung, die zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen Person oder zur Erfüllung der rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist, oder die Datenverarbeitung, die aus Gründen des öffentlichen Interesses oder auf der Grundlage überwiegender rechtmäßiger Interessen des Verantwortlichen oder eines Dritten erfolgt.

Die Datenverarbeitung aus Gründen des öffentlichen Interesses sollte gesetzlich geregelt sein, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit, für Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Straftaten, der Strafvollstreckung, der nationalen Sicherheit, Verteidigung, für Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe, für Zwecke der Durchsetzung zivilrechtlicher Ansprüche sowie zum Schutz der richterlichen Unabhängigkeit und gerichtlicher Verfahren. Die Datenverarbeitung kann sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen, beispielsweise bei der Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen. Dies kann insbesondere bei Naturkatastrophen der Fall sein, wenn die Verarbeitung personenbezogener Daten von vermissten Personen für eine

begrenzte Zeit im Rahmen der Katastrophenbewältigung notwendig sein kann, was im Einzelfall zu entscheiden ist. Auch in bewaffneten Konflikten oder anderen Gewaltlagen kann dies zutreffen.⁶ Auch im Hinblick auf die Verarbeitung personenbezogener Daten durch staatliche Stellen zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften kann gelten, dass sie aus Gründen des öffentlichen Interesses durchgeführt wird.

Die Voraussetzungen für eine rechtmäßige Verarbeitung sind in den Absätzen 3 und 4 festgelegt. Personenbezogene Daten sollen auf rechtmäßige Weise, nach Treu und Glauben und in einer transparenten Weise verarbeitet werden. Personenbezogene Daten müssen außerdem für eindeutige, festgelegte und rechtmäßige Zwecke erhoben werden und die Verarbeitung muss diesen Zwecken dienen beziehungsweise darf mit diesen nicht unvereinbar sein. Der Verweis auf eindeutige „Zwecke“ zeigt an, dass es nicht gestattet ist, Daten für undefinierte, unbestimmte oder vage Zwecke zu verarbeiten. Was als rechtmäßiger Zweck angesehen wird, hängt von den Umständen ab, denn es soll ein ausgewogenes Verhältnis zwischen allen jeweils betroffenen Rechten, Freiheiten und Interessen sichergestellt werden; das Recht auf Schutz von personenbezogenen Daten einerseits und Schutz von anderen Rechten andererseits, wie beispielsweise zwischen den Interessen der betroffenen Person und den Interessen des Verantwortlichen oder der Gesellschaft.

Durch das Konzept der Vereinbarkeit der Nutzung sollten die Transparenz, die Rechtssicherheit, die Vorhersehbarkeit oder Nachvollziehbarkeit der Verarbeitung nicht beeinträchtigt werden. Es sollte keine Weiterverarbeitung von personenbezogenen Daten stattfinden, die von der betroffenen Person als unerwartet oder unangemessen oder aus sonstigen Gründen als zu beanstanden angesehen werden kann. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.

Die in Absatz 4 Buchstabe b genannte Weiterverarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt a priori als mit solchen Zwecken vereinbar, sofern andere Garantien bestehen (wie beispielsweise die Anonymisierung oder Pseudonymisierung von Daten, sofern nicht die Speicherung der identifizierbaren Form erforderlich ist; Regelung zum Berufsgeheimnis; Zugangsbeschränkungen und Regeln für die Übermittlung der Daten für die vorgenannten Zwecke, insbesondere Statistik- und Archivzwecke; sonstige technische und organisatorische Datenschutzmaßnahmen) und sofern die Verarbeitungsvorgänge grundsätzlich jede Nutzung der gewonnenen Informationen für Entscheidungen oder

⁶ Wenn die vier Genfer Abkommen von 1949, die dazugehörigen Zusatzprotokolle von 1977 und die Satzungen des Internationalen Roten Kreuzes und des Roten Halbmondes gelten.

Maßnahmen hinsichtlich einer bestimmten Person ausschließen. „Statistische Zwecke“ bezieht sich auf statistische Erhebungen oder die Erzeugung von statistischen, aggregierten Ergebnissen. Statistiken dienen der Analyse und Charakterisierung von massenhaften oder kollektiven Phänomenen in einer zu untersuchenden Bevölkerungsgruppe.⁷ Statistische Zwecke können sowohl vom öffentlichen oder privaten Sektor verfolgt werden. Die Verarbeitung von Daten für „wissenschaftliche Forschungszwecke“ dient dazu, Forscher mit Informationen zu versorgen, die zum Verständnis von Phänomenen in verschiedenen wissenschaftlichen Bereichen beitragen (Epidemiologie, Psychologie, Ökonomie, Soziologie, Sprachwissenschaft, Politische Wissenschaften, Kriminologie usw.). Dabei geht es darum, dauerhafte Grundsätze, gesetzmäßige Verhaltensweisen oder Kausalitätsmuster zu erkennen, die über die Personen hinausgehen, für die sie gelten.⁸ „Historische Forschungszwecke“ umfasst auch Forschung im Bereich der Genealogie. „Im öffentlichen Interesse liegende Archivzwecke“ kann auch ursprünglich private Archive umfassen, sofern ein öffentliches Interesse vorliegt.

Personenbezogene Daten, die verarbeitet werden, sollten den Zwecken, für die sie verarbeitet werden, entsprechen und dafür erheblich sein und dürfen nicht darüber hinausgehen. Die Daten müssen außerdem sachlich richtig sein und erforderlichenfalls auf den neuesten Stand gebracht werden.

Die Forderung in Absatz 4 Buchstabe c, dass Daten nicht über die Zwecke, für die sie verarbeitet werden, hinausgehen dürfen, bedeutet zuerst, dass die Datenverarbeitung darauf beschränkt sein sollte, was für den Zweck der Verarbeitung notwendig ist. Sie dürfen nur verarbeitet werden, wenn und solange die Zwecke der Verarbeitung nicht durch die Verarbeitung von anderen als personenbezogenen Daten erreicht werden können. Diese Forderung bezieht sich nicht nur auf die Menge, sondern auch auf die Qualität von personenbezogenen Daten. Personenbezogene Daten, die zwar den Zwecken, für die sie verarbeitet werden, entsprechen (adäquat) und dafür erheblich sind, jedoch einen unverhältnismäßigen Eingriff in die betroffenen Grundrechte und Grundfreiheiten bedeuten, sollten als über die Zwecke hinausgehend (exzessiv) angesehen und nicht verarbeitet werden.

Die Forderung in Absatz 4 Buchstabe e hinsichtlich der Fristen für die Aufbewahrung von personenbezogenen Daten bedeutet, dass die Daten gelöscht werden sollten, sobald der Zweck, für den sie verarbeitet wurden, erreicht worden ist, oder dass sie nur in einer Form aufbewahrt werden sollten, die eine unmittelbare oder mittelbare Identifizierung der betroffenen Person verhindert.

Begrenzte Ausnahmen von Artikel 5 Absatz 4 sind unter den in Artikel 11 Absatz 1 festgelegten Voraussetzungen zulässig.

Zu Artikel 6 – Besondere Kategorien von Daten

Die Verarbeitung bestimmter Typen von Daten oder die Verarbeitung bestimmter Daten zur Offenlegung sensibler Informationen kann zu Eingriffen in Interessen, Rechte und Freiheiten führen. Dies ist möglicherweise der Fall, wenn ein potenzielles Risiko der Diskriminierung oder der Verletzung der Würde oder der körperlichen Unversehrtheit einer Person besteht, wenn der persönlichste Bereich einer Person, wie ihr Sexualleben oder ihre sexuelle Orientierung, betroffen sind, oder wenn sich die Datenverarbeitung auf die Unschuldsvermutung auswirken

⁷ Empfehlung Nr. (97)18 des Ministerkomitees zum Schutz personenbezogener Daten, die zu statistischen Zwecken erhoben und verarbeitet werden, Anhang, Punkt 1, 30. September 1997.

⁸ Erläuterungsprotokoll zu Empfehlung Nr. (97)18 des Ministerkomitees zum Schutz personenbezogener Daten, die zu statistischen Zwecken erhoben und verarbeitet werden, Absätze 11 und 14.

könnte. Die Datenverarbeitung sollte dann nur zugelassen werden, wenn ergänzend zu den anderen Schutzbestimmungen des Übereinkommens weitere Garantien gesetzlich vorgesehen sind. Das Erfordernis geeigneter Garantien ergänzend zu den Bestimmungen des Übereinkommens schließt jedoch nicht die in Artikel 11 vorgesehene Möglichkeit aus, Ausnahmen oder Beschränkungen der Rechte einer betroffenen Person nach Artikel 9 zuzulassen.

Um Nachteile für die betroffene Person zu verhindern, muss die Verarbeitung von sensiblen Daten für rechtmäßige Zwecke durch geeignete Garantien flankiert werden (die an die betroffenen, schützenswerten Interessen, Rechte und Freiheiten anzupassen sind), wie zum Beispiel – einzeln oder kumulativ – die ausdrückliche Zustimmung der betroffenen Person, ein Gesetz zur Regelung des beabsichtigten Zwecks und der beabsichtigten Mittel der Datenverarbeitung oder zur Regelung der Ausnahmefälle, in denen die Verarbeitung solcher Daten zulässig ist, eine Verpflichtung zur Einhaltung eines Berufsgeheimnisses, von einer Risikoanalyse ausgehende Maßnahmen, eine bestimmte und qualifizierte organisatorische oder technische Sicherheitsvorkehrung (Datenverschlüsselung, zum Beispiel).

Bestimmte Arten der Datenverarbeitung können für die betroffenen Personen unabhängig vom Kontext der Datenverarbeitung ein bestimmtes Risiko mit sich bringen. Dies ist beispielsweise bei der Verarbeitung von genetischen Daten der Fall, aus denen sich Informationen über die Gesundheit der betreffenden Person oder ihrer Abstammung oder der von Dritten ableiten lassen. Genetische Daten sind alle Daten, die sich auf vererbte oder in der pränatalen Entwicklung erworbene genetische Merkmale einer Person beziehen, die als Ergebnis der Analyse einer biologischen Probe von der betroffenen Person gewonnen wurden. Das umfasst Chromosomen-, DNS- oder RNS-Analysen oder sonstige Analysen, mit denen gleichartige Informationen gewonnen werden können. Ein ähnliches Risiko besteht bei der Verarbeitung von Daten im Zusammenhang mit Straftaten (was Verdachtsfälle einschließt), strafrechtlichen Verurteilungen (auf der Grundlage des Strafrechts und im Rahmen von Strafverfahren) und damit im Zusammenhang stehenden Sicherheitsmaßnahmen (einschließlich Freiheitsentziehung). Das erfordert geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen.

Die Verarbeitung von biometrischen Daten, d. h. von Daten, die aus einer spezifischen technischen Verarbeitung von Daten zu körperlichen, biologischen oder physiologischen Merkmalen einer Person resultieren, anhand derer die eindeutige Identifizierung oder Authentisierung der Person möglich ist, gilt ebenfalls als sensibel, gerade wenn die Verarbeitung dazu genutzt wird, die betroffene Person zu identifizieren.

Bei Bilddaten ist für die Bestimmung des sensiblen Charakters der Daten der Kontext der Verarbeitung von Bildern erheblich. Die Verarbeitung von Bilddaten bedeutet nicht zwangsläufig auch die Verarbeitung von sensiblen Daten. Bilddaten fallen nur dann unter die Definition von biometrischen Daten, wenn sie mit Hilfe spezieller technischer Methoden verarbeitet werden, die eine eindeutige Identifizierung oder Authentisierung einer Person ermöglichen. Darüber hinaus gilt die Verarbeitung von Bilddaten als Verarbeitung sensibler Daten, wenn sie dazu dient, rassische, ethnische oder gesundheitliche Informationen offenzulegen. Im Gegensatz dazu gilt die Verarbeitung von Bildern aus einem Videoüberwachungssystem in einem Einkaufszentrum, die für Sicherheitszwecke aufgenommen wurden, nicht grundsätzlich als Verarbeitung von sensiblen Daten.

Die Verarbeitung von sensiblen Daten birgt das potentielle Risiko, die Rechte einer betroffenen Person zu beeinträchtigen, wenn diese Verarbeitung zum Zwecke der Offenlegung spezifischer Informationen dient. Die Verarbeitung von Familiennamen ist in den meisten Fällen für die betroffenen Personen nicht mit einem Risiko verbunden (z. B. für die Lohnabrechnung). In einigen Fällen kann es sich dabei aber um sensible Daten handeln, z. B. wenn die Verarbeitung dazu dient, auf der Grundlage der sprachlichen Herkunft der Namen die ethnische Herkunft oder die religiösen Überzeugungen einer Person offenzulegen. Informationen zur Gesundheit einer Person umfassen Informationen über die körperliche oder mentale Gesundheit einer Person bezogen auf Vergangenheit, Gegenwart und Zukunft und können sich auf eine gesunde oder eine kranke Person beziehen. Die Verarbeitung von Bildern von Personen mit dicken Brillen, einem gebrochenen Bein, Verbrennungen oder sonstigen sichtbaren Merkmalen, die sich auf die Gesundheit der Person beziehen, kann ausschließlich als Verarbeitung von sensiblen Daten gelten, wenn die Verarbeitung auf der Grundlage von Gesundheitsinformationen erfolgt, die sich aus den Bildern ableiten lassen.

Ist die Verarbeitung von sensiblen Daten für statistische Zwecke erforderlich, dann muss bei der Erhebung der Daten sichergestellt werden, dass die betroffenen Personen nicht identifizierbar sind. Eine Garantie im Sinne des Artikels 6 ist die Erhebung von sensiblen Daten ohne Identifizierungsdaten. Besteht ein rechtmäßiger Bedarf, sensible Daten für statistische Zwecke in identifizierbarer Form zu erheben (beispielsweise, um eine Wiederholungs- oder eine Längsschnittstudie durchzuführen), sollten geeignete Garantien etabliert werden.⁹

Zu Artikel 7 – Datensicherheit

Der Verantwortliche und gegebenenfalls der Auftragsverarbeiter sollten für jede Verarbeitung spezifische, sowohl technische als auch organisatorische Sicherheitsmaßnahmen ergreifen, wobei Folgendes zu berücksichtigen ist: die potentiellen nachteiligen Folgen für die betroffene Person, die Art der personenbezogenen Daten, die Menge der verarbeiteten personenbezogenen Daten, der Grad der Schutzbedürftigkeit der für die Verarbeitung eingesetzten technischen Architektur, die Notwendigkeit des beschränkten Zugangs zu den Daten, Anforderungen an eine langfristige Aufbewahrung usw.

Die Sicherheitsmaßnahmen sollten im Hinblick auf Datenschutzmethoden und -techniken dem Stand der Technik im Bereich der Datenverarbeitung entsprechen. Ihre Kosten sollten in einem angemessenen Verhältnis zur Schwere und Wahrscheinlichkeit der potentiellen Risiken stehen. Sicherheitsmaßnahmen sollten ständig überprüft und erforderlichenfalls aktualisiert werden.

Während die Sicherheitsmaßnahmen dazu dienen, eine Reihe von Risiken zu verhindern, enthält Absatz 2 eine konkrete Verpflichtung in den Fällen, in denen es zu einer Verletzung des Datenschutzes gekommen ist, die einen schweren Eingriff in die Rechte und Grundfreiheiten von Betroffenen darstellen können. Als „schwerer Eingriff“ ist beispielsweise die Offenlegung von Daten zu werten, die unter das Berufsgeheimnis fallen oder die zu einem finanziellen Schaden führen kann oder zu einer Rufbeschädigung oder zu körperlichem oder seelischem Schaden.

Ist es zu einer solchen Verletzung des Datenschutzes gekommen, ist der Verantwortliche für die Verarbeitung verpflichtet, die zuständige Aufsichtsbehörde über den Vorfall zu informieren,

⁹ Siehe Empfehlung des Ministerkomitees Nr. (97)18, op.cit.

vorbehaltlich der in Artikel 11 Absatz 1 gestatteten Ausnahme. Dies ist die Mindestanforderung. Der für die Verarbeitung Verantwortliche sollte außerdem die Aufsichtsbehörden über alle getroffenen und / oder vorgeschlagenen Maßnahmen informieren, die sich auf die Verletzung des Datenschutzes und deren potenzielle Folgen beziehen.

Die Benachrichtigung der Aufsichtsbehörden durch den Verantwortlichen schließt ergänzende Benachrichtigungen anderer Stellen nicht aus. So kann der Verantwortliche auch die Notwendigkeit sehen, die betroffenen Personen zu informieren, insbesondere dann, wenn die Datenschutzverletzung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, wie z. B. das Risiko der Diskriminierung, des Identitätsdiebstahls oder Betrugs, eines finanziellen Verlusts, einer Rufbeschädigung, des Verlusts der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen oder eines anderen erheblichen wirtschaftlichen und gesellschaftlichen Nachteils, und diesen betroffenen Personen angemessene und aussagekräftige Informationen zu geben, zum Beispiel zu Ansprechstellen und möglichen Maßnahmen, die von ihnen ergriffen werden könnten, um die Nachteile der Datenschutzverletzung möglichst gering zu halten. Entscheidet sich der für die Verarbeitung Verantwortliche nicht dazu, die betroffene Person spontan über die Verletzung des Datenschutzes zu informieren, kann die Aufsichtsbehörde nach Abwägung der wahrscheinlichen Nachteile dieser Verletzung den Verantwortlichen auffordern, dies zu tun. Ebenso kann es wünschenswert sein, andere zuständige Stellen, wie die für die Sicherheit von Computersystemen zuständigen Stellen, zu informieren.

Zu Artikel 8 – Transparenz der Verarbeitung

Der für die Verarbeitung Verantwortliche ist bei der Verarbeitung von Daten zu transparentem Handeln verpflichtet, um eine Verarbeitung nach Treu und Glauben sicherzustellen und die betroffenen Personen in die Lage zu versetzen, die Datenverarbeitung zu verstehen und somit von ihren Rechten im Zusammenhang mit dieser Verarbeitung vollen Gebrauch machen zu können.

Werden unmittelbar oder mittelbar (nicht von der betroffenen Person selbst, sondern über Dritte) Daten erhoben, muss der für die Verarbeitung Verantwortliche den betroffenen Personen bestimmte Informationen proaktiv zur Verfügung stellen, vorbehaltlich der Möglichkeit für Ausnahmen nach Artikel 11 Absatz 1. Dazu gehören Informationen über den Namen und die Anschrift des für die Verarbeitung Verantwortlichen (oder Mitverantwortlichen), die Rechtsgrundlage und die Zwecke der Datenverarbeitung, die Arten personenbezogener Daten, die verarbeitet werden, gegebenenfalls die Empfänger sowie die Mittel zur Ausübung der Rechte. Diese Informationen können in jeder beliebigen Form bereitgestellt werden (entweder auf einer Website oder mit Hilfe technischer Werkzeuge auf persönlichen Geräten usw.), solange die Informationen der betroffenen Person nach Treu und Glauben und wirksam zur Verfügung gestellt werden. Die zur Verfügung gestellten Informationen sollten leicht zugänglich, leicht lesbar und leicht verständlich sein und an die relevanten betroffenen Personen angepasst werden (z. B. erforderlichenfalls in einer kindgerechten Sprache). Darüber hinaus sind zusätzliche Informationen zur Verfügung zu stellen, die notwendig sind, um eine faire Datenverarbeitung zu gewährleisten, oder die für solche Zwecke nützlich sind, wie Angaben zu Aufbewahrungsfristen, zu Gründen für die Datenverarbeitung, zu Datentransfers an einen Empfänger einer anderen Partei [des Übereinkommens] oder Nicht-Partei (einschließlich Informationen dazu, ob diese bestimmte Nicht-Partei ein angemessenes Schutzniveau für Daten sicherstellt, oder zu Maßnahmen des für die Verarbeitung Verantwortlichen, um ein angemessenes Datenschutzniveau sicherzustellen).

Der für die Verarbeitung Verantwortliche ist nicht zur Bereitstellung von Informationen verpflichtet, die die betroffene Person bereits erhalten hat. Dies gilt außerdem in den Fällen einer indirekten Datenerhebung durch Dritte, wenn die Verarbeitung ausdrücklich gesetzlich vorge-schrieben ist oder wenn die Bereitstellung von Informationen unverhältnismäßige Anstrengun-gen erfordert, weil die betroffene Person nicht direkt identifizierbar ist oder wenn es für den Verantwortlichen nicht möglich ist, die betroffene Person zu kontaktieren. Diese Unmöglichkeit kann rechtlich begründet sein (wegen eines strafrechtlichen Ermittlungsverfahrens) oder prak-tische Gründe haben (z. B. wenn der Verantwortliche nur Bilder verarbeitet und die Namen und Kontaktdaten der betroffenen Personen nicht kennt).

Der Verantwortliche kann jedes verfügbare, verhältnismäßige und bezahlbare Mittel nutzen, um betroffene Personen kollektiv (über eine Website oder eine öffentliche Bekanntmachung) oder individuell zu informieren. Ist dies zu Beginn der Datenverarbeitung nicht möglich, kann es auch zu einem späteren Zeitpunkt erfolgen, z. B. wenn zwischen dem Verantwortlichen und der betroffenen Person der Kontakt aus einem neuen Grund hergestellt wird.

Zu Artikel 9 – Rechte des Betroffenen

In diesem Artikel sind die Rechte aufgeführt, die jede Person im Hinblick auf die Verarbeitung von sie betreffenden personenbezogenen Daten ausüben können sollte. Jede Partei stellt im Rahmen ihrer Rechtshoheit sicher, dass jede betroffene Person von diesen Rechten Gebrauch machen kann, und jeder betroffenen Person die zur Ausübung dieser Rechte nötigen rechtli-chen und praktischen, angemessenen und wirksamen Mittel zur Verfügung stehen.

Diese sind u. a.:

- das Recht einer jeden Person, einer ausschließlich auf einer automatisierten Daten-verarbeitung beruhenden Entscheidung, die sich erheblich auf sie auswirkt, nicht un-terworfen zu werden, ohne dass ihre Auffassungen berücksichtigt werden (Buchstabe a),
- das Recht einer jeden Person, eine Bestätigung über die Verarbeitung von sie betref-fenden personenbezogenen Daten zu erhalten und in angemessenen Abständen und ohne übermäßige Verzögerung oder Kosten Auskunft über diese Daten zu erhalten (Buchstabe b),
- das Recht einer jeden Person, auf Antrag Kenntnis über die der Datenverarbeitung zugrundeliegenden Überlegungen zu erlangen, wenn die Ergebnisse dieser Verarbei-tung auf die Person Anwendung finden (Buchstabe c),
- das Recht einer jeden Person, aus sich aus ihrer Situation ergebenden Gründen gegen die Verarbeitung von sie betreffenden personenbezogenen Daten Widerspruch einzu-legen, sofern der Verantwortliche nicht nachweisen kann, dass berechtigte Gründe für die Verarbeitung bestehen, welche die Interessen, Rechte oder Grundfreiheiten der Person überwiegen (Buchstabe d),
- das Recht einer jeden Person, die Berichtigung beziehungsweise Löschung von un-richtigen, falschen oder unrechtmäßig verarbeiteten Daten zu erwirken (Buchstabe e),
- das Recht einer jeden Person, ein Rechtsmittel einzulegen, wenn eines ihrer vorge-nannten Rechte verletzt worden ist (Buchstabe f),
- das Recht einer jeden Person, von einer Aufsichtsbehörde Unterstützung zu erhalten (Buchstabe g).

Diese Rechte sind gegebenenfalls mit anderen Rechten und rechtmäßigen Interessen in Einklang zu bringen. Sie können gemäß Artikel 11 nur begrenzt werden, wenn dies gesetzlich vorgesehen ist und als eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft anzusehen ist. Das Recht auf Löschung personenbezogener Daten kann beispielsweise beschränkt werden, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist.

Obgleich in dem Übereinkommen nicht klargestellt ist, von welcher Stelle die betroffene Person eine Bestätigung, Benachrichtigung, Richtigstellung usw. erhalten kann oder wem gegenüber sie Beschwerde einlegen oder eine Meinung ausdrücken kann, so wird dies in den meisten Fällen der Verantwortliche selbst oder in dessen Auftrag der Auftragsverarbeiter sein. In Ausnahmefällen kann das Recht auf Auskunft, Richtigstellung oder Löschung auch über eine Beteiligung der Aufsichtsbehörde erfolgen. Im Falle von Gesundheitsdaten können diese Rechte auch auf andere Weise als über eine Direktauskunft ausgeübt werden. Hier ist beispielsweise Unterstützung durch Gesundheitsfachpersonal möglich, wenn dies im Interesse der betroffenen Person ist, insbesondere wenn es darum geht, die Daten zu verstehen oder sicherzustellen, dass bei der Weitergabe von Informationen der psychologische Zustand der betroffenen Person angemessen berücksichtigt wird, selbstverständlich im Einklang mit deontologischen Grundsätzen.

Buchstabe a: Es ist von entscheidender Bedeutung, dass eine Person einer ausschließlich auf einer automatisierten Datenverarbeitung beruhenden Entscheidung nicht unterworfen wird, ohne dass ihre Auffassungen berücksichtigt werden. Die betroffene Person sollte insbesondere die Möglichkeit haben nachzuweisen, dass personenbezogene Daten möglicherweise unrichtig sind, bevor diese Daten verwendet werden, dass das auf ihre besondere Situation anzuwendende Profil oder andere Faktoren, die sich auf das Ergebnis einer automatisierten Entscheidung auswirken, nicht relevant sind. Dies trifft insbesondere dann zu, wenn Personen durch die Anwendung von Algorithmen, die zur Begrenzung eines Rechts oder zur Verwehrung einer Sozialleistung oder zur Bewertung der Kreditwürdigkeit führen, stigmatisiert werden. Eine Person kann von diesem Recht jedoch keinen Gebrauch machen, wenn die automatisierte Entscheidung aufgrund von Rechtsvorschriften, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person enthalten.

Buchstabe b: Betroffene Personen sollten Anspruch haben, von der Verarbeitung ihrer personenbezogenen Daten Kenntnis zu erlangen. Das Auskunftsrecht sollte grundsätzlich gebührenfrei sein. Hinter dem Wortlaut des Buchstaben b steht allerdings die Absicht, dem Verantwortlichen unter bestimmten Voraussetzungen die Erhebung einer angemessenen Gebühr zu gestatten, wenn die Anfragen übermäßig sind oder um verschiedene Ansätze abzudecken, die von einer Partei in geeigneten Fällen angewendet werden. Eine solche Gebühr sollte die Ausnahme darstellen und in jedem Fall verhältnismäßig sein und die betroffenen Personen keinesfalls von der Wahrnehmung ihrer Rechte abhalten. Der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter können eine Auskunft auf offensichtlich unbegründete oder exzessive Anfragen verweigern, insbesondere bei häufiger Wiederholung. Der für die Verarbeitung Verantwortliche sollte in jedem Fall eine solche Ablehnung begründen. Um eine faire Wahrnehmung des Auskunftsrechts zu gewährleisten, gilt die Mitteilung über die verarbeiteten

Daten in verständlicher Form sowohl für den Inhalt als auch für die Form einer standardisierten digitalen Mitteilung.

Buchstabe c: Betroffene Personen sollten Anspruch darauf haben, Kenntnis über die der Datenverarbeitung zugrundeliegenden Überlegungen zu erlangen, einschließlich über die Folgen dieser Überlegungen, wenn diese zu Schlussfolgerungen geführt haben, insbesondere bei der Verwendung von Algorithmen für automatisierte Entscheidungsprozesse, einschließlich Profilbildung. Beispielsweise im Fall der Einstufung der Kreditwürdigkeit sollten Betroffene nicht lediglich über die Entscheidung selbst informiert werden, sondern Anspruch darauf haben, die der Verarbeitung ihrer Daten zugrundeliegende Logik zu kennen, die am Ende zu einer positiven oder negativen Entscheidung führt. Das Verständnis dieser Elemente trägt zur wirksamen Wahrnehmung anderer wesentlicher Garantien bei, wie dem Widerspruchsrecht und dem Recht der Beschwerdeführung bei einer zuständigen Behörde.

Buchstabe d: Was das Widerspruchsrecht betrifft, so kann der Verantwortliche berechnete Gründe für die Verarbeitung haben, welche die Interessen, Rechte oder Grundfreiheiten der Person überwiegen. Solche Gründe, welche als die Interessen, Rechte oder Grundfreiheiten der Person überwiegend angesehen werden können, sind beispielsweise die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder die öffentliche Sicherheit. Dies ist jeweils im Einzelfall nachzuweisen und das Versäumnis des Nachweises überwiegender Gründe für die Verarbeitung von Daten kann als unrechtmäßig angesehen werden. Das Widerspruchsrecht greift auf andere und eigenständige Weise als das Recht auf Berichtigung oder Löschung (Buchstabe e).

Der Widerspruch gegen die Verarbeitung von Daten für Marketing-Zwecke sollte zu einer bedingungslosen Löschung oder Entfernung der von dem Widerspruch erfassten personenbezogenen Daten führen.

Das Widerspruchsrecht kann durch Gesetz begrenzt werden, beispielsweise zum Zweck der Ermittlung oder Verfolgung von Straftaten. In diesem Falle kann die betroffene Person je nach Lage der Sache die Rechtmäßigkeit der Verarbeitung in Frage stellen, auf deren Grundlage die Strafverfolgung durchgeführt wird. Werden Daten auf der Grundlage der Zustimmung der betroffenen Person verarbeitet, kann das Recht auf Rücknahme der Zustimmung an die Stelle des Widerspruchsrechts treten. Eine betroffene Person kann ihre Zustimmung zurücknehmen, muss jedoch die Folgen tragen, die sich gegebenenfalls aus anderen Rechtsvorschriften ergeben, wie die Ersatzpflicht gegenüber dem für die Verarbeitung Verantwortlichen. Liegt der Datenverarbeitung ein Vertrag zugrunde, kann die betroffene Person die notwendigen Schritte unternehmen, um den Vertrag zu widerrufen.

Buchstabe e: Die Berichtigung oder Löschung muss, sofern sie gerechtfertigt ist, gebührenfrei durchgeführt werden. Im Falle von Berichtigungen oder Löschungen, die im Einklang mit dem in Buchstabe e aufgeführten Grundsatz herbeigeführt werden, sollten die Empfänger der ursprünglichen Informationen darüber in Kenntnis gesetzt werden, sofern sich dies nicht als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Mit Buchstabe g sollen die betroffenen Personen durch das Recht auf Unterstützung von einer Aufsichtsbehörde bei der Wahrnehmung ihrer Rechte aus dem Übereinkommen wirksam geschützt werden. Lebt die betroffene Person im Hoheitsgebiet einer anderen Vertragspartei, kann sie ihren Antrag über die bezeichnete Aufsichtsbehörde dieser Vertragspartei stellen.

Das Unterstützungersuchen sollte hinreichende Informationen enthalten, um die fragliche Datenverarbeitung identifizieren zu können. Dieses Recht kann gemäß Artikel 11 im Interesse eines laufenden gerichtlichen Verfahrens beschränkt werden.

Begrenzte Ausnahmen von Artikel 9 sind unter den in Artikel 11 Absatz 1 festgelegten Voraussetzungen zulässig.

Zu Artikel 10 – Zusätzliche Verpflichtungen

Um die Wirksamkeit des Rechts auf Schutz von personenbezogenen Daten sicherzustellen, werden dem Verantwortlichen und gegebenenfalls den Auftragsverarbeitern zusätzliche Verpflichtungen auferlegt.

Gemäß Absatz 1 ist die Verpflichtung des Verantwortlichen, angemessenen Datenschutz sicherzustellen, mit der Verantwortung verbunden nachzuweisen, dass die in seiner Verantwortung durchgeführte Datenverarbeitung im Einklang mit dem Übereinkommen steht. Die im Übereinkommen festgelegten Datenschutzgrundsätze, die auf allen Stufen der Verarbeitung, einschließlich der konzeptionellen Stufe, anzuwenden sind, zielen auf den Schutz des Betroffenen ab und dienen gleichzeitig der Vertrauensbildung. Zu den geeigneten Maßnahmen, die gegebenenfalls vom Verantwortlichen und Auftragsverarbeiter zu ergreifen sind, gehören unter anderem die Schulung von Mitarbeitern, die Einrichtung geeigneter Benachrichtigungsverfahren (z. B. um anzuzeigen, wann Daten aus dem System zu löschen sind), die Festlegung konkreter Vertragsbestimmungen im Sinne des Übereinkommens im Falle einer Übertragung der Verarbeitung sowie die Einrichtung interner Verfahren zum Nachweis der Einhaltung des Übereinkommens.

Sofern eine Vertragspartei gemäß Artikel 11 Absatz 3 die Befugnisse einer Aufsichtsbehörde im Sinne des Artikels 15 unter Hinweis auf Verarbeitungstätigkeiten für Zwecke der nationalen Verteidigung und Sicherheit begrenzt, ist der Verantwortliche nicht verpflichtet, gegenüber dieser Aufsichtsbehörde nachzuweisen, dass im Zusammenhang mit Aktivitäten, die unter die vorgenannte Ausnahmeregelung fallen, die Anforderungen des Datenschutzes eingehalten werden.

Eine mögliche Maßnahme, die der Verantwortliche ergreifen kann, um den Nachweis der Einhaltung zu erleichtern, wäre die Ernennung eines Datenschutzbeauftragten mit entsprechendem Mandat. Dieser Datenschutzbeauftragte, dessen Ernennung der Aufsichtsbehörde notifiziert werden sollte, kann im Verhältnis zum Verantwortlichen intern oder extern sein.

Gemäß Absatz 2 muss der Verantwortliche vor Beginn der Datenverarbeitung die wahrscheinlichen Auswirkungen der beabsichtigten Datenverarbeitung auf die Rechte und Grundfreiheiten der betroffenen Personen untersuchen. Diese Untersuchung kann ohne übermäßige Formvorschriften durchgeführt werden. Auf der Grundlage eines umfassenden Überblicks über die beabsichtigte Verarbeitung muss dabei auch die Wahrung des Verhältnismäßigkeitsprinzips betrachtet werden. Unter bestimmten Umständen, wenn ein Auftragsverarbeiter beteiligt ist, wird auch dieser die Risiken untersuchen müssen. Bei der Untersuchung der Risiken kann auf die Unterstützung von IT-Systementwicklern, einschließlich Sicherheitsfachleuten oder Fachplanern, Nutzern und Rechtsexperten zurückgegriffen werden.

Gemäß Absatz 3 sollen die Verantwortlichen und gegebenenfalls die Auftragsverarbeiter durch technische und organisatorische Maßnahmen sicherstellen, dass Datenschutzerfordernungen so früh wie möglich berücksichtigt werden, idealerweise bereits in der Phase der Architektur-

oder Systemkonzeption (Datenschutz durch Technikgestaltung). Diese Umsetzung von Datenschutzerfordernungen sollte nicht nur im Hinblick auf die Technologie zur Datenverarbeitung verfolgt werden, sondern auch im Hinblick auf Arbeits- und Verwaltungsprozesse. Leicht nutzbare Funktionalitäten, die die Einhaltung von Datenschutzstandards erleichtern, sollten etabliert werden. So sollten betroffene Personen beispielsweise die Möglichkeit des sicheren Online-Zugriffs auf ihre eigenen Daten haben. Ebenso sollte es mit Hilfe leicht zu bedienender Werkzeuge für betroffene Personen möglich sein, ihre Daten zu einem anderen Diensteanbieter ihrer Wahl mitzunehmen oder ihre Daten selbst aufzubewahren (Werkzeuge zur Datenübertragbarkeit). Bei der Festlegung von technischen Anforderungen für Default-Einstellungen sollten Verantwortliche und Auftragsverarbeiter datenschutzfreundliche Konfigurationen wählen, damit durch die Nutzung von Anwendungen und Software die Rechte von betroffenen Personen nicht verletzt werden (Datenschutz by Default), insbesondere um zu verhindern, dass für den rechtmäßigen Zweck mehr Daten als nötig verarbeitet werden. Soziale Netzwerke sollten beispielsweise standardmäßig so konfiguriert werden, dass Posts oder Bilder nur innerhalb begrenzter und ausgewählter Kreise geteilt werden und nicht im gesamten Internet.

Gemäß Absatz 4 können die Parteien die in den Absätzen 1 bis 3 aufgeführten zusätzlichen Verpflichtungen anpassen, unter Berücksichtigung der Risiken für die Interessen, Rechte und Grundfreiheiten der betroffenen Personen. Bei einer solchen Anpassung sollten die Art und die Menge der verarbeiteten Daten, die Art, der Umfang und die Zwecke der Datenverarbeitung sowie in bestimmten Fällen die Größe der verarbeitenden Stelle Berücksichtigung finden. Die Verpflichtungen könnten zum Beispiel so angepasst werden, dass für Klein- und Mittelunternehmen, die ausschließlich nicht sensible personenbezogene Daten verarbeiten, die sie von Kunden im Rahmen ihrer Geschäftstätigkeiten erhalten und nicht für andere Zwecke weiterverwenden, keine übermäßigen Kosten entstehen. Bestimmte Kategorien der Datenverarbeitung, wie solche, die keinerlei Risiko für die betroffenen Personen mit sich bringen, können von den Zusatzverpflichtungen dieses Artikels auch gänzlich ausgenommen werden.

Zu Artikel 11 – Ausnahmen und Beschränkungen

Für die Bestimmungen von Kapitel II sind keine Ausnahmen erlaubt, außer für eine begrenzte Anzahl von Bestimmungen (Artikel 5 Absatz 4), Artikel 7 Absatz 2, Artikel 8 Absatz 11 und Artikel 9), sofern eine solche Ausnahme gesetzlich vorgesehen ist, der Wesensgehalt der Grundrechte und Grundfreiheiten gewahrt bleibt und sie in einer demokratischen Gesellschaft für die in Artikel 11 Absatz 1 Buchstabe a und b aufgeführten Gründe eine notwendige Maßnahme darstellt. Eine „in einer demokratischen Gesellschaft notwendige“ Maßnahme muss einem rechtmäßigen Ziel dienen und damit einen dringenden gesellschaftlichen Bedarf erfüllen, der sich nicht mit einer Maßnahme mit geringerem Eingriffscharakter decken ließe. Eine solche Maßnahme sollte überdies in Bezug auf das angestrebte rechtmäßige Ziel verhältnismäßig sein und die von den nationalen Behörden angeführten Rechtfertigungsgründe sollten relevant und angemessenen sein. Eine solche Maßnahme muss durch ein zugängliches und vorhersehbares Gesetz, das hinreichend ausführlich ist, vorgeschrieben werden.

Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise erfolgen, und die Daten dürfen nur für bestimmte Zwecke verarbeitet werden. Dies steht an sich der Durchführung von Maßnahmen wie verdeckten Ermittlungen oder Videoüberwachung durch die Strafverfolgungsbehörden nicht entgegen. Diese Maßnahmen können zwecks Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und zur

Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die nationale und öffentliche Sicherheit, getroffen werden, sofern sie gesetzlich geregelt sind und eine erforderliche und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen, bei der die berechtigten Interessen der betroffenen Person gebührend berücksichtigt werden.

Die Notwendigkeit solcher Ausnahmen muss im Einzelfall und im Lichte wesentlicher Ziele des allgemeinen öffentlichen Interesses geprüft werden, wie in Absatz 1, Buchstaben a und b dargelegt. In Buchstabe a sind einige im Allgemeininteresse liegende Ziele des Staates oder der internationalen Organisation aufgeführt, die Ausnahmen erfordern.

Der Begriff „nationale Sicherheit“ sollte auf der Basis der einschlägigen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ausgelegt werden.¹⁰

Der Ausdruck „wichtige wirtschaftliche und finanzielle Interessen“ bezieht sich vor allem auf die Bereiche Steuererhebung und Devisenkontrolle. Der Ausdruck „Verhütung, Ermittlung und Verfolgung von Straftaten und die Strafvollstreckung“ in Buchstabe a umfasst die Verfolgung von Straftaten und die Verhängung von diesbezüglichen Strafen. Der Ausdruck „sonstige wichtige Ziele des allgemeinen öffentlichen Interesses“ umfasst u. a. die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe und die Durchsetzung zivilrechtlicher Ansprüche.

Buchstabe b betrifft die Rechte und Grundfreiheiten von privaten Parteien, wie die der betroffenen Person selbst (z. B. wenn lebenswichtige Interessen einer betroffenen Person gefährdet sind, weil sie vermisst wird) oder von Dritten, wie das Recht der freien Meinungsäußerung, auch von Journalisten, Wissenschaftlern, Künstlern oder Schriftstellern, sowie das Recht, Informationen zu empfangen und weiterzugeben, die Vertraulichkeit der Korrespondenz und der Kommunikation oder das Geschäfts- und Unternehmensgeheimnis und sonstige gesetzlich geschützte Geheimnisse. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven gelten. Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.

Mit Absatz 2 wird die Möglichkeit eingeräumt, die Bestimmungen der Artikel 8 und 9 im Hinblick auf eine bestimmte Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken, die keine erkennbare Gefahr des Eingriffs in die Rechte und Grundfreiheiten von Betroffenen darstellt, zu beschränken. Dies betrifft beispielsweise die Nutzung von Daten für statistische Arbeiten sowohl im öffentlichen wie im privaten Bereich, sofern die Daten in aggregierter Form veröffentlicht werden und vorausgesetzt, dass angemessene Datenschutzvorkehrungen getroffen wurden.

¹⁰ Die relevante Rechtsprechung umfasst insbesondere den Schutz des Staates und der verfassungsmäßigen Demokratie u. a. vor Spionage, Terrorismus, Unterstützung für Terrorismus und Separatismus. Wenn die nationale Sicherheit auf dem Spiel steht, müssen Sicherheitsvorkehrungen gegen uneingeschränkte Macht getroffen werden. Einschlägige Entscheidungen des Europäischen Gerichtshofs für Menschenrechte sind auf der Website des Gerichtshofs erhältlich (hudoc.echr.coe.int).

Die zusätzlich zu den nach Artikel 4 Absatz 3, Artikel 14 Absätze 5 und 6 und Artikel 15 Absatz 2 Buchstaben a, b, c und d in Bezug auf Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung zulässigen Ausnahmen gelten unbeschadet der Voraussetzung einer unabhängigen und wirksamen Prüfung und Aufsicht.¹¹

Zu Artikel 12 – Sanktionen und Rechtsmittel

Damit durch das Übereinkommen ein wirksames Datenschutzniveau sichergestellt wird, sollen sich die Pflichten des Verantwortlichen und des Auftragsverarbeiters sowie die Rechte der betroffenen Personen in den Rechtsvorschriften der Parteien in Form entsprechender Sanktionen und Rechtsmittel widerspiegeln.

Es ist jeder Partei überlassen, die Art (zivilrechtlich, verwaltungsrechtlich, strafrechtlich) dieser gerichtlichen sowie außergerichtlichen Sanktionen zu bestimmen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Dasselbe gilt für Rechtsmittel: Betroffene Personen müssen die Möglichkeit haben, eine Entscheidung oder Praxis gerichtlich anzufechten, wobei die Modalitäten dafür von den Parteien bestimmt werden können. Den betroffenen Personen sind überdies außergerichtliche Rechtsmittel einzuräumen. Ein finanzieller Ausgleich für gegebenenfalls aus der Verarbeitung von Daten und kollektivem Handeln entstandene Vermögens- und Nicht-Vermögensschäden kann ebenfalls erwogen werden.

Zu Artikel 13 – Erweiterter Schutz

Dieser Artikel basiert auf einer ähnlichen Bestimmung, Artikel 53 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten. Die Konvention bestätigt die Grundsätze des Datenschutzrechts, die alle Parteien bereit sind, anzunehmen. Der Wortlaut unterstreicht, dass die Grundsätze nur eine Grundlage darstellen, auf der aufbauend die Parteien ein fortgeschrittenes Schutzsystem aufbauen könnten. Die Formulierung „ein größeres Maß an Schutz“ bezieht sich dementsprechend auf einen Schutzstandard, der höher ist, nicht niedriger, als der bereits durch das Übereinkommen geforderte Standard.

Zu Kapitel III

Grenzüberschreitender Verkehr personenbezogener Daten¹²

Zu Artikel 14 – Grenzüberschreitender Verkehr personenbezogener Daten

Das Ziel dieses Artikels ist es, den freien Informationsfluss ungeachtet von Grenzen zu erleichtern (wie in der Präambel betont) und gleichzeitig einen geeigneten Schutz von Personen bei der Verarbeitung ihrer personenbezogenen Daten sicherzustellen. Von grenzüberschreitendem Datenverkehr ist die Rede, wenn personenbezogene Daten an eine internationale Organisation oder an einen Empfänger weitergegeben oder diesem bereitgestellt werden, der der Hoheitsgewalt eines anderen Staates untersteht.

¹¹ Für Mitgliedstaaten des Europarats wurden solche Voraussetzungen durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte nach Artikel 8 der Europäischen Menschenrechtskonvention entwickelt (vgl. EGMR, Roman Zakharov v. Russia (Beschwerde Nr. 47143/06), 4. Dezember 2015, Ziffer 233; Szabo und Vissy v. Hungary (Beschwerde Nr. 37138/14), 12. Januar 2016, Ziffern 75 ff.).

¹² Mit dem Inkrafttreten des Änderungsprotokolls gilt das Zusatzprotokoll bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181) als ein integraler Bestandteil des Übereinkommens in der jeweils gültigen Fassung.

Mit der Regelung des grenzüberschreitenden Datenverkehrs soll sichergestellt werden, dass für die Weiterverarbeitung von ursprünglich unter der Hoheitsgewalt einer Vertragspartei verarbeiteten personenbezogenen Daten (beispielsweise Daten, die dort erhoben oder gespeichert wurden) durch eine Vertragspartei, die der Hoheitsgewalt eines Staates untersteht, der dem Übereinkommen nicht angehört, weiterhin geeignete Garantien gelten. Dabei geht es vor allem darum, dass Daten, die unter der Hoheitsgewalt einer Vertragspartei verarbeitet werden, stets durch die einschlägigen Datenschutzgrundsätze des Übereinkommens geschützt bleiben. Es mag eine große Vielfalt an Schutzsystemen geben, doch der tatsächlich gewährte Schutz muss so hoch sein, dass sichergestellt ist, dass Menschenrechte von der Globalisierung und der grenzüberschreitenden Datenübermittlung nicht betroffen sind.

Artikel 14 gilt lediglich für den Abfluss von Daten, nicht für den Zufluss, da letzterer durch die Datenschutzregelungen der empfangenden Vertragspartei abgedeckt ist.

Absatz 1 gilt für den Datenverkehr zwischen Vertragsparteien des Übereinkommens. „Zum alleinigen Zweck des Schutzes personenbezogener Daten“ darf die Weitergabe von Daten weder verboten noch von einer besonderen Genehmigung abhängig gemacht werden. Doch die Freiheit einer Vertragspartei, die Weitergabe von personenbezogenen Daten an eine andere Vertragspartei zu anderen Zwecken, einschließlich der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit oder sonstiger wichtiger öffentlicher Interessen zu beschränken, wird durch das Übereinkommen nicht begrenzt.

Den Bestimmungen des Absatzes 1 liegt der Gedanke zugrunde, dass von allen Vertragsparteien, die sich den gemeinsamen Basisdatenschutzbestimmungen verpflichtet haben, erwartet wird, dass sie ein geeignetes Schutzniveau anbieten, und dass somit ein freier Datenverkehr prinzipiell erlaubt ist. Es kann allerdings Ausnahmen geben, wenn ein tatsächliches und ernstes Risiko besteht, dass der freie Verkehr von personenbezogenen Daten zu einer Umgehung der Bestimmungen des Übereinkommens führt. Als Ausnahme ist diese Bestimmung restriktiv auszulegen und die Vertragsparteien können sich nicht darauf berufen, wenn das Risiko hypothetisch oder gering ist. Daher kann eine Vertragspartei sich nur in bestimmten Fällen auf die Ausnahmeregelung berufen, wenn eindeutige und zuverlässige Beweise vorliegen, dass durch die Übermittlung von Daten an eine andere Vertragspartei der diesen Daten unter dem Übereinkommen gewährte Schutz mit hoher Wahrscheinlichkeit signifikant untergraben würde. Dies kann beispielsweise der Fall sein, wenn ein bestimmter Schutz unter dem Übereinkommen durch die andere Vertragspartei nicht mehr garantiert ist (zum Beispiel weil die Aufsichtsbehörde nicht mehr in der Lage ist, ihre Aufsichtsfunktionen wirksam wahrzunehmen) oder wenn an eine andere Vertragspartei übermittelte Daten wahrscheinlich ohne die Garantie eines geeigneten Schutzniveaus von dieser Vertragspartei weitergegeben werden. Eine weitere völkerrechtlich anerkannte Ausnahme ist dann gegeben, wenn Vertragsparteien durch harmonisierte gemeinsame Schutzvorschriften von Staaten gebunden sind, die regionalen (wirtschaftlichen) Organisationen angehören, die ein höheres Niveau an Integration anstreben.

Dies trifft unter anderem auf die Mitgliedstaaten der EU zu. Wie bereits in der Datenschutz-Grundverordnung (EU) 2016/679 ausdrücklich erwähnt wird, sind der Beitritt eines Landes zum Übereinkommen Nr. 108 und dessen Umsetzung jedoch wichtige Faktoren bei der Anwendung der Vorschriften für den internationalen Datenverkehr der EU, insbesondere bei der Beurteilung, ob ein Drittstaat ein angemessenes Schutzniveau anbietet (was wiederum den freien Verkehr von personenbezogenen Daten erlauben würde).

Nach Absatz 2 besteht die Verpflichtung, dass „ein angemessenes Schutzniveau auf der Grundlage der Bestimmungen dieses Übereinkommens sichergestellt ist“. Gleichzeitig können die Vertragsparteien nach Absatz 4 Daten auch dann weitergeben, wenn kein geeignetes Schutzniveau besteht, sofern dies gerechtfertigt ist, u. a. wenn „überwiegende berechnete Interessen, insbesondere wichtige öffentliche Interessen, gesetzlich vorgesehen sind und eine solche Weitergabe in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt“ (Buchstabe c). Demnach können personenbezogene Daten aus gleichartigen Gründen wie den in Artikel 11 Absatz 1 und Absatz 3 aufgeführten weitergegeben werden. In jedem Fall bleibt es den Vertragsparteien nach dem Übereinkommen überlassen, die Weitergabe von Daten an Nicht-Vertragsparteien einzuschränken, sowohl aus Gründen des Datenschutzes als auch aus anderen Gründen.

Absatz 2 bezieht sich auf den grenzüberschreitenden Verkehr mit personenbezogenen Daten an einen Empfänger, der nicht der Hoheitsgewalt einer Vertragspartei untersteht. Werden personenbezogene Daten über die Grenzen hinweg weitergegeben, muss ein angemessenes Schutzniveau sichergestellt werden. Ist der Empfänger keine Vertragspartei des Übereinkommens, sieht das Übereinkommen zwei Mechanismen vor, um sicherzustellen, dass das Datenschutzniveau tatsächlich angemessen ist: durch das Recht oder durch Ad-hoc-Garantien oder genehmigte standardisierte Garantien, die rechtlich bindend und durchsetzbar sind und umgesetzt werden.

Die Absätze 2 und 3 gelten für alle Formen eines angemessenen Schutzes, ob durch Recht garantiert oder durch standardisierte Garantien. Das Recht muss die einschlägigen Elemente des Datenschutzes beinhalten, wie in dem Übereinkommen dargelegt. Das Schutzniveau ist für jede Weitergabe oder Kategorie von Weitergaben im Einzelfall zu beurteilen. Dabei sind verschiedene Elemente der Weitergabe zu betrachten: die Art der Daten, der Zweck und die Dauer der Verarbeitung, für die die Weitergabe erfolgt, die Achtung der Rechtsstaatlichkeit durch den Zielstaat, die in dem fraglichen Staat oder der fraglichen Organisation geltenden allgemeinen und sektorspezifischen Rechtsvorschriften sowie die dort geltenden Berufsgeheimnis- und Sicherheitsvorschriften.

Ad-hoc-Garantien oder standardisierte Garantien müssen so ausgestaltet sein, dass die einschlägigen Elemente des Datenschutzes darin enthalten sind. Darüber hinaus könnten die Vertragsbedingungen beispielsweise vorsehen, dass die betroffene Person eine Ansprechperson bei der für die Datenweitergabe zuständigen Stelle genannt bekommt, deren Aufgabe es ist, die Einhaltung der wesentlichen Datenschutzstandards sicherzustellen. Die betroffene Person könnte diese Ansprechperson jederzeit und ohne dass Kosten anfallen in Bezug auf die Datenverarbeitung oder Datenweitergabe kontaktieren und gegebenenfalls Hilfe bei der Wahrnehmung ihrer Rechte erhalten.

Bei der Beurteilung, ob ein Datenschutzniveau angemessen ist, ist zu prüfen, ob bzw. in welchem Umfang die Grundsätze des Übereinkommens in dem Empfängerstaat oder der Empfängerorganisation eingehalten werden und – sofern dies für den konkreten Fall der Datenweitergabe zutreffend ist – inwieweit die betroffene Person in der Lage ist, ihre Interessen im Falle der Nichteinhaltung zu verteidigen. Die Durchsetzbarkeit der Rechte der betroffenen Personen und die Verfügbarkeit wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten weitergegeben werden, sollte bei der Beurteilung ebenfalls berücksichtigt werden. Die Beurteilung kann allerdings auch für einen Staat oder eine Organisation insgesamt erfolgen, wodurch alle Datenübermittlungen an diesen Staat oder diese Organisation erlaubt wären.

Nach Absatz 4 ist es den Vertragsparteien gestattet, vom Grundsatz, ein angemessenes Schutzniveau zu verlangen, abzuweichen und eine Weitergabe auch an einen Empfänger zu gestatten, der diesen Schutz nicht sicherstellt. Derartige Abweichungen sind nur unter bestimmten Voraussetzungen zulässig: mit Einwilligung der betroffenen Person oder wegen spezifischer Interessen der betroffenen Person und / oder wenn überwiegende berechnigte Interessen gesetzlich vorgesehen sind und / oder wenn die Weitergabe in einer demokratischen Gesellschaft im Hinblick auf die Meinungsfreiheit eine notwendige und verhältnismäßige Maßnahme darstellt. Bei solchen Abweichungen sollten die Grundsätze der Notwendigkeit und Verhältnismäßigkeit gewahrt werden.

In Absatz 5 ist eine ergänzende Sicherheit vorgesehen: nämlich dass der zuständigen Aufsichtsbehörde alle sachdienlichen Informationen hinsichtlich der in Absatz 3 Buchstabe b genannten Weitergabe von Daten sowie auf Antrag hinsichtlich der in Absatz 4 Buchstaben b und c genannten Daten zur Verfügung gestellt werden. Die Aufsichtsbehörde ist berechnigt, sachdienliche Informationen über die Umstände der Weitergabe und die Gründe dafür zu verlangen. Unter den in Artikel 11 Absatz 3 genannten Bedingungen sind Ausnahmen von Artikel 14 Absatz 5 zulässig.

Gemäß Absatz 6 darf die Aufsichtsbehörde einen Nachweis für die Wirksamkeit der Maßnahmen oder das Vorhandensein überwiegender berechnigter Interessen verlangen und eine Datenweitergabe verbieten, aussetzen oder an Bedingungen knüpfen, wenn sich dies zum Schutz der Rechte und Grundfreiheiten der betroffenen Personen als notwendig erweist. Unter den in Artikel 11 Absatz 3 genannten Bedingungen sind Ausnahmen von Artikel 14 Absatz 6 zulässig.

Immer umfangreicher werdende Datenströme und der damit einhergehende Schutzbedarf für personenbezogene Daten erfordern ein Mehr an internationaler Zusammenarbeit unter den zuständigen Aufsichtsbehörden.

Zu Kapitel IV

Aufsichtsbehörden¹³

Zu Artikel 15 – Aufsichtsbehörden

Mit diesem Artikel soll der wirksame Schutz von Personen sichergestellt werden, indem von den Vertragsparteien verlangt wird, eine oder mehrere unabhängige und unparteiische öffentliche Aufsichtsbehörden zu schaffen, die zum Schutz der Rechte und Freiheiten von Personen im Hinblick auf die Verarbeitung von personenbezogenen Daten beitragen. Bei diesen Aufsichtsbehörden kann es sich um einen einzelnen Beauftragten handeln oder ein Kollegialorgan. Damit die Aufsichtsbehörden ein geeignetes Rechtsmittel anbieten können, müssen sie über wirksame Befugnisse und Zuständigkeiten verfügen und in der Wahrnehmung ihrer Aufgaben vollkommen unabhängig sein. Sie sind ein wesentliches Element der Datenschutzaufsicht in einer demokratischen Gesellschaft. Sofern Artikel 11 Absatz 3 gilt, können die Vertragsparteien andere angemessene Mechanismen für eine unabhängige und wirksame Überprüfung und Aufsicht über Verarbeitungstätigkeiten zum Zweck der nationalen Sicherheit und der Landesverteidigung vorsehen.

¹³ Mit dem Inkrafttreten des Änderungsprotokolls gilt das Zusatzprotokoll bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181) als ein integraler Bestandteil des Übereinkommens in der jeweils gültigen Fassung.

In Absatz 1 wird klargestellt, dass möglicherweise Bedarf an einer oder mehreren Behörden besteht, um den besonderen Umständen unterschiedlicher Rechtssysteme (z. B. föderale Staaten) gerecht zu werden. Möglich ist auch die Schaffung spezifischer Aufsichtsbehörden, deren Tätigkeit auf einen bestimmten Sektor beschränkt ist (elektronische Kommunikation, Gesundheitswesen, öffentlicher Sektor usw.). Dies gilt auch für die Verarbeitung von personenbezogenen Daten für journalistische Zwecke, wenn dies notwendig ist, um das Recht auf den Schutz von personenbezogenen Daten mit dem Recht der freien Meinungsäußerung in Einklang zu bringen. Die Aufsichtsbehörden sollten über die notwendige Infrastruktur und die notwendigen finanziellen, technischen und personellen (Juristen, IT-Spezialisten) Mittel verfügen, um unverzüglich und wirksam handeln zu können. Die Angemessenheit der Mittel sollte ständig überprüft werden. Nach Artikel 11 Absatz 3 sind, unter Verweis auf Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung, Ausnahmen von den Befugnissen der Aufsichtsbehörden zulässig (sofern solche Ausnahmen gelten, gelten andere Absätze des Artikels 11 folglich ggf. nicht bzw. sind dadurch irrelevant). Dies gilt jedoch unbeschadet der Anforderungen bezüglich der Unabhängigkeit und Wirksamkeit von Überprüfungs- und Aufsichtsmechanismen.

Was die Ausgestaltung / Ausstattung der Aufsichtsbehörden im Hinblick auf ihre Fähigkeit zur Aufgabenwahrnehmung betrifft, so haben die Vertragsparteien ein gewisses Maß an Spielraum. Vorbehaltlich der Möglichkeit, Ausnahmen nach Maßgabe des Artikels 11 Absatz 3 vorzusehen, müssen die Aufsichtsbehörden nach Absatz 2 jedoch mindestens über Untersuchungs- und Einwirkungsbefugnisse verfügen sowie über die Befugnis, Entscheidungen im Hinblick auf Verstöße gegen das Übereinkommen zu treffen. Letzteres kann die Befugnis zur Verhängung von verwaltungsrechtlichen Sanktionen, einschließlich Geldbußen, umfassen. Sind in der Rechtsordnung einer Vertragspartei keine verwaltungsrechtlichen Sanktionen vorgesehen, kann Absatz 2 auch dergestalt angewandt werden, dass die Sanktion von der zuständigen Aufsichtsbehörde vorgeschlagen und von den zuständigen nationalen Gerichten verhängt wird. In jeden Fall müssen die verhängten Sanktionen wirksam, verhältnismäßig und abschreckend sein.

Vorbehaltlich der Möglichkeit, Ausnahmen nach Maßgabe des Artikels 11 Absatz 3 vorzusehen, müssen die Aufsichtsbehörden nach Absatz 2 über Untersuchungsbefugnisse verfügen. Das heißt, sie müssen beispielsweise die Möglichkeit haben, von dem Verantwortlichen und dem Auftragsverarbeiter Informationen über die Verarbeitung von personenbezogenen Daten zu verlangen und zu erhalten. Nach Artikel 15 sollen diese Informationen insbesondere dann zur Verfügung gestellt werden, wenn sich eine betroffene Person an die Aufsichtsbehörde wendet und um Unterstützung bei der Wahrnehmung ihrer Rechte nach Artikel 9 ersucht. Letzteres gilt vorbehaltlich der Bestimmungen gemäß Artikel 11 Absatz 1.

Die Einwirkungsbefugnis der Aufsichtsbehörde gemäß Absatz 1 kann in dem jeweiligen Recht der Vertragsparteien verschiedene Formen haben. So kann die Aufsichtsbehörde befugt sein, von dem Verantwortlichen die Richtigstellung, Löschung oder Vernichtung von unrichtigen oder unrechtmäßig verarbeiteten Daten im eigenen Namen oder im Namen der betroffenen Person, sofern diese zur Wahrnehmung dieser Rechte selbst nicht in der Lage ist, zu verlangen. Die Befugnis, gegen Verantwortliche vorzugehen, die sich weigern, die geforderten Informationen in einer angemessenen Frist zur Verfügung zu stellen, wäre auch eine besonders wirksame Demonstration der Einwirkungsbefugnis der Aufsichtsbehörde. Dies könnte auch die Möglichkeit einschließen, vor der Durchführung von Datenverarbeitungstätigkeiten Stellungnahmen abzugeben (wenn die Verarbeitung besondere Risiken für die

Rechte und Freiheiten bedeutet, sollte die Aufsichtsbehörde von den Verantwortlichen zum frühestmöglichen Zeitpunkt der Prozessgestaltung konsultiert werden) oder Fälle ggf. an die relevanten zuständigen Behörden zu verweisen.

Im Übrigen sollte jede betroffene Person nach Absatz 4 die Möglichkeit haben, von der Aufsichtsbehörde die Prüfung ihrer Forderung hinsichtlich ihrer Rechte und Freiheiten im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten zu verlangen. Das trägt dazu bei, das Recht auf angemessene Rechtsmittel im Einklang mit den Artikeln 9 und 12 zu gewährleisten. Die zur Wahrnehmung dieser Aufgabe nötigen Mittel sollten bereitgestellt werden. Je nach Verfügbarkeit von Mitteln sollten die Aufsichtsbehörden die Möglichkeit haben, hinsichtlich der Behandlung von Anfragen und Beschwerden durch betroffene Personen Prioritäten zu setzen.

Die Vertragsparteien sollten, vorbehaltlich der Möglichkeit, Ausnahmen gemäß Artikel 11 Absatz 3 vorzusehen, die Aufsichtsbehörde mit der Befugnis ausstatten, sich an gerichtlichen Verfahren zu beteiligen oder Verstöße gegen Datenschutzvorschriften bei den Justizbehörden zur Kenntnis zu bringen. Diese Befugnis leitet sich ab aus der Ermittlungsbefugnis, in deren Ausübung die Aufsichtsbehörde eine Verletzung eines individuellen Schutzrechts einer Person aufdecken kann. Die Vertragsparteien können die Verpflichtung zur Übertragung dieser Befugnis an die Behörde erfüllen, indem sie die Behörde ermächtigen, Entscheidungen zu treffen.

Entfaltet eine Verwaltungsentscheidung Rechtswirkung, steht jeder betroffenen Person das Recht auf einen wirksamen Rechtsbehelf im Einklang mit dem innerstaatlichen Recht zu.

In Absatz 2 Buchstabe e geht es um die bewusstseinsfördernde Rolle der Aufsichtsbehörden. In diesem Zusammenhang scheint es besonders wichtig, dass die Aufsichtsbehörde proaktiv für die Sichtbarkeit ihrer Tätigkeiten, Aufgaben und Befugnisse sorgt. Dazu muss die Aufsichtsbehörde die Öffentlichkeit durch periodische Berichte informieren. Sie kann auch Stellungnahmen und allgemeine Empfehlungen hinsichtlich der richtigen Umsetzung von Datenschutzvorschriften abgeben oder andere Kommunikationsmittel nutzen. Sie muss darüber hinaus betroffene Personen, Verantwortliche für die Verarbeitung und Auftragsverarbeiter über ihre Rechte und Pflichten hinsichtlich des Datenschutzes informieren. Im Zuge der Förderung des Bewusstseins für Datenschutzbelange müssen die Aufsichtsbehörden den Datenschutzrechten von Kindern und anderen schutzbedürftigen Personen besondere Aufmerksamkeit widmen und sich in angepasster Form und Sprache an diese Personengruppen wenden.

Gemäß Absatz 3 können die Aufsichtsbehörden im Einklang mit nationalem Recht zu Vorschlägen für Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten vorsehen, Stellungnahmen abgeben. Diese Beratungsbefugnis bezieht sich lediglich auf allgemeine Maßnahmen, nicht jedoch auf individuelle Maßnahmen.

Zusätzlich zu dieser Konsultationsbefugnis nach Absatz 3 könnten die Aufsichtsbehörden auch um Stellungnahme gebeten werden, wenn andere Maßnahmen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten vorbereitet werden, wie zum Beispiel die Einführung von Verhaltenskodizes oder technischen Normen.

Artikel 15 ist kein Hindernis für die Übertragung anderer Befugnisse an die Aufsichtsbehörden.

In Absatz 5 wird klargestellt, dass die Aufsichtsbehörden individuelle Rechte und Freiheiten nicht wirksam schützen können, solange sie in ihrer Aufgabenwahrnehmung nicht vollkommen unabhängig sind. Es gibt eine Reihe von Elementen, die zur Sicherung der Unabhängigkeit der Aufsichtsbehörde beitragen, unter anderem die Zusammensetzung der Behörde, die Methode zur Ernennung ihrer Mitglieder, die Dauer der Ausübung und die Bedingungen für eine Beendigung ihrer Aufgaben, die Möglichkeit zur uneingeschränkten Teilnahme an relevanten Sitzungen, die Möglichkeit, technische oder andere Sachverständige hinzuziehen oder externe Konsultationen abzuhalten, die Verfügbarkeit hinreichender Mittel für die Behörde, die Möglichkeit, selbst Personal einzustellen oder die Möglichkeit zur Annahme von Entscheidungen ohne direkte oder indirekte Einflussnahme von außen.

Das Verbot, Weisungen zu erbitten oder entgegenzunehmen, bezieht sich auch auf die Ausübung der Aufgaben als Aufsichtsbehörde. Das bedeutet keine Einschränkung von Aufsichtsbehörden, sich von Sachverständigen beraten zu lassen, sofern dies für notwendig erachtet wird, vorausgesetzt, die Aufsichtsbehörden sind in ihrer Urteilsfindung unabhängig.

Nach Absatz 7 sind die Aufsichtsbehörden zu Transparenz im Hinblick auf ihre Arbeit und Tätigkeiten verpflichtet, beispielsweise durch die Veröffentlichung eines jährlichen Tätigkeitsberichts, in dem u. a. Informationen über ihre Durchsetzungsmaßnahmen aufzuführen sind.

Ungeachtet dieser Unabhängigkeit muss es möglich sein, gegen die Entscheidungen der Aufsichtsbehörden bei einem Gericht Beschwerde einzulegen, im Einklang mit dem Grundsatz der Rechtsstaatlichkeit gemäß Absatz 9.

Unbeschadet der Verfahrensfähigkeit von Aufsichtsbehörden vor Gericht darf durch die Intervention (oder das Versäumnis) einer Aufsichtsbehörde eine betroffene Person nicht daran gehindert werden, einen gerichtlichen Rechtsbehelf einzulegen.

In Artikel 15 Absatz 10 ist festgelegt, dass die Aufsichtsbehörden nicht für Verarbeitungen zuständig sind, die von unabhängigen Organen im Rahmen ihrer gerichtlichen Tätigkeit vorgenommen werden. Diese Ausnahme sollte allerdings streng begrenzt werden auf rein justizielle Tätigkeiten in Gerichtsverfahren im Einklang mit nationalem Recht.

Zu Kapitel V

Zusammenarbeit und gegenseitige Hilfeleistung

Zu Artikel 16 – Benennung von Aufsichtsbehörden

Kapitel V (Artikel 16 bis 21) enthält eine Reihe von Bestimmungen zu Zusammenarbeit und gegenseitiger Hilfeleistung zwischen den Vertragsparteien durch ihre verschiedenen Behörden in dem Bestreben, den Datenschutzvorschriften gemäß dem Übereinkommen Wirkung zu verleihen. Diese Bestimmungen sind mit Ausnahme der in Artikel 20 genannten Bestimmungen verpflichtend. Nach Artikel 16 benennt jede Vertragspartei eine oder mehrere Aufsichtsbehörden und teilt deren Namen und Anschrift sowie ihre wesentlichen und territorialen Zuständigkeiten dem Generalsekretär des Europarats mit. Die folgenden Artikel bestimmen einen detaillierten Rahmen für die Zusammenarbeit und gegenseitige Hilfeleistung.

Zwar wird die Zusammenarbeit zwischen den Vertragsparteien grundsätzlich von den nach Artikel 15 eingesetzten Aufsichtsbehörden geleistet, doch es kann nicht ausgeschlossen werden, dass eine Vertragspartei eine andere Behörde benennt, um den Bestimmungen des Artikels 16 Wirkung zu verleihen.

Relevant ist die Zusammenarbeit und allgemeine Hilfeleistung für Vorabkontrollen und Nachkontrollen (zum Beispiel um die Tätigkeiten eines bestimmten Datenverarbeiters zu überprüfen). Die ausgetauschten Informationen können rechtlicher oder tatsächlicher Natur sein.

Zu Artikel 17 – Formen der Zusammenarbeit

Nach Maßgabe des Artikels 17 arbeiten die Aufsichtsbehörden im Sinne des Artikels 15 miteinander in dem Maße zusammen, wie es zur Erfüllung ihrer Aufgaben und zur Wahrnehmung ihrer Befugnisse notwendig ist. Angesichts dessen, dass Artikel 17 die Zusammenarbeit der Aufsichtsbehörden umschreibt als das, was „zur Erfüllung ihrer Aufgaben und Wahrnehmung ihrer Befugnisse notwendig ist“ und angesichts der Tatsache, dass die Kooperationsfähigkeit einer Aufsichtsbehörde vom Umfang ihrer Befugnisse abhängt, gilt diese Bestimmung in dem Maße nicht, wie eine Vertragspartei Artikel 11 Absatz 3 anwendet, der eine Beschränkung der Befugnisse der Aufsichtsbehörden nach Artikel 15 Absatz 2 Buchstaben a bis d nach sich zieht.

Die Zusammenarbeit kann verschiedene Formen annehmen, darunter einige „harte“ Formen, wie die Durchsetzung von Datenschutzgesetzen durch gegenseitige Hilfeleistung, wobei die Rechtmäßigkeit des Handelns jeder einzelnen Aufsichtsbehörde unerlässlich ist, bis hin zu einigen „weichen“ Formen der Zusammenarbeit, wie Bewusstseinsbildung, Schulungen, Personalaustausch.

Die Aufzählung der möglichen Kooperationsmaßnahmen ist nicht abschließend. Zuallererst sollen die Aufsichtsbehörden sich gegenseitig Hilfe leisten, insbesondere durch den Austausch von nützlichen und sachdienlichen Informationen. Dabei kann es sich um zweierlei Arten von Informationen handeln: „Informationen und Unterlagen über ihr Recht und ihre Verwaltungspraxis im Zusammenhang mit dem Datenschutz“ (was normaler Weise keine Probleme aufwirft, solche Informationen können frei ausgetauscht und öffentlich zugänglich gemacht werden) sowie vertrauliche Informationen, einschließlich personenbezogener Daten.

Soweit personenbezogene Daten betroffen sind, ist ein Austausch nur zulässig, wenn dies für die Zusammenarbeit von entscheidender Bedeutung ist oder „der Betroffene hat ausdrücklich, für den konkreten Fall, freiwillig und in informierter Weise in ihre Bereitstellung eingewilligt“. In jedem Falle sind bei der Übermittlung personenbezogener Daten die Bestimmungen des Übereinkommens, insbesondere des Kapitels II einzuhalten (siehe auch Artikel 20, in dem die Ablehnungsgründe geregelt sind).

Ebenfalls im Sinne der Bereitstellung von nützlichen und sachdienlichen Informationen lassen sich die Ziele der Zusammenarbeit auch durch koordinierte Ermittlungen oder Eingriffe sowie gemeinsame Maßnahmen erreichen. Was die anzuwendenden Verfahren betrifft, so sollen die Aufsichtsbehörden geltende innerstaatliche Rechtsvorschriften heranziehen, wie Verwaltungs-, Zivil- oder Strafprozessordnung oder supra- oder internationale Verpflichtungen, die für ihre Hoheitsgebiete verbindlich sind, beispielsweise Verträge über gegenseitige Rechtshilfe, nach Prüfung ihrer Verfahrensfähigkeit zum Eintritt in derartige Kooperationen.

Absatz 3 bezieht sich auf ein Netzwerk von Aufsichtsbehörden als Mittel zur Rationalisierung des Kooperationsprozesses und damit zur Sicherung der Effizienz des Schutzes von personenbezogenen Daten. Es wird darauf hingewiesen, dass in dem Übereinkommen ausdrücklich von einem Netzwerk im Singular die Rede ist. Das hindert Aufsichtsbehörden der Vertragsparteien wiederum nicht daran, sich an anderen relevanten Netzwerken zu beteiligen.

Zu Artikel 18 – Unterstützung von Betroffenen

Mit Absatz 1 wird sichergestellt, dass betroffene Personen, ganz gleich ob sie in einem Vertragsstaat des Übereinkommens oder in einem Drittland wohnen, zur Ausübung ihrer Rechte nach Artikel 9 befähigt werden, ungeachtet ihres Wohnorts oder ihrer Staatsangehörigkeit.

Nach Absatz 2 soll einer betroffenen Person, die in einem anderen Vertragsstaat lebt, die Möglichkeit gegeben werden, ihre Rechte entweder direkt in dem Land wahrzunehmen, in dem ihre personenbezogenen Daten verarbeitet werden, oder indirekt über die bezeichnete Aufsichtsbehörde.

Im Übrigen können im Ausland ansässige betroffene Personen bei der Wahrnehmung ihrer Rechte die Unterstützung durch Botschafts- oder Konsularbeamte ihres Landes in Anspruch nehmen.

Nach Absatz 3 sollen Anträge so konkret wie möglich sein, um das Verfahren zu beschleunigen.

Zu Artikel 19 – Garantien

Mit diesem Artikel soll sichergestellt werden, dass für die Aufsichtsbehörden hinsichtlich Discretion und Vertraulichkeit gegenüber den Datenschutzbehörden anderer Vertragsparteien und im Ausland lebenden Betroffenen dieselben Verpflichtungen gelten.

Eine Aufsichtsbehörde darf im Namen einer betroffenen Person nur dann Unterstützung leisten, wenn die betroffene Person darum ersucht. Die Behörde muss von der betroffenen Person ein Mandat erhalten und darf nicht von sich aus oder im Namen der Person handeln. Diese Bestimmung ist für das gegenseitige Vertrauen, auf dem die gegenseitige Hilfeleistung basiert, von entscheidender Bedeutung.

Zu Artikel 20 – Ablehnung von Ersuchen

Nach diesem Artikel sind die Vertragsparteien verpflichtet, Ersuchen um Zusammenarbeit und gegenseitige Hilfeleistung zu erfüllen. Die Gründe für eine Ablehnung sind abschließend aufgeführt.

Der Begriff „Erfüllung“, der in Buchstabe c verwendet wird, soll in einem breiteren Sinne ausgelegt werden, d. h. er meint nicht nur die Antwort auf das Ersuchen, sondern auch die der Antwort vorausgegangene Handlung. Eine ersuchte Behörde kann es ablehnen, tätig zu werden, nicht nur wenn die Rechte und Grundfreiheiten einer Person durch die Übermittlung der erbetenen Informationen an die ersuchende Behörde beeinträchtigt würden, sondern auch, wenn das bloße Ersuchen um die Informationen diese Rechte und Grundfreiheiten gefährdet. Darüber hinaus kann eine ersuchte Behörde durch geltendes innerstaatliches Recht verpflichtet werden sicherzustellen, dass andere Interessen der öffentlichen Ordnung geschützt werden (z. B. Sicherstellung der Vertraulichkeit eines polizeilichen Ermittlungsverfahrens). Dazu kann eine Aufsichtsbehörde verpflichtet werden, bei der Beantwortung einer Anfrage auf die Übermittlung bestimmter Informationen oder Unterlagen zu verzichten.

Zu Artikel 21 – Kosten und Verfahren

Die Bestimmungen dieses Artikels entsprechen jenen in anderen völkerrechtlichen Instrumenten.

Um das Übereinkommen nicht mit einer Fülle von Einzelheiten zur Umsetzung zu überfrachten, sieht Absatz 3 vor, dass Verfahren, Formvorschriften und zu verwendende Sprachen in Abstimmung zwischen den betroffenen Vertragsparteien festgelegt werden sollen. Der Wortlaut dieses Absatzes verlangt kein förmliches Verfahren, sondern sieht die Möglichkeit von Verwaltungsvereinbarungen sogar im konkreten Einzelfall vor. Im Übrigen sollten die Vertragsparteien es den zuständigen Aufsichtsbehörden überlassen, solche Vereinbarungen zu treffen. Die Formen der Zusammenarbeit und Hilfeleistung können sich auch von Fall zu Fall unterscheiden. Es ist offensichtlich, dass für die Übermittlung eines Ersuchens um Zugang zu sensiblen medizinischen Informationen andere Auflagen gelten als für routinemäßige Anfragen zu Einträgen in einem Einwohnerverzeichnis.

Zu Kapitel VI

Übereinkommensausschuss

Der Zweck der Artikel 22, 23 und 24 ist es, die wirksame Anwendung des Übereinkommens zu erleichtern und ggf. zu optimieren. Der Übereinkommensausschuss ist ein weiteres Mittel der Zusammenarbeit der Vertragsparteien, um den Datenschutzgesetzen auf der Grundlage des Übereinkommens Wirkung zu verleihen.

Ein Übereinkommensausschuss setzt sich aus Vertretern aller Vertragsparteien, der nationalen Aufsichtsbehörden oder der Regierung zusammen.

Das Wesen des Übereinkommensausschusses und das wahrscheinlich für ihn geltende Verfahren könnten sich an den Regelungen für Übereinkommensausschüsse in anderen Übereinkommen des Europarats orientieren.

Da das Übereinkommen ein ständig wiederkehrendes Thema behandelt, ist davon auszugehen, dass Fragen sowohl im Zusammenhang mit der praktischen Anwendung des Übereinkommens (Artikel 23, Buchstabe a und mit der Begriffsbestimmung / Bedeutung (Artikel 23, Buchstabe d) aufkommen.

Die Verfahrensordnung des Übereinkommensausschusses enthält Bestimmungen zum Stimmrecht der Vertragsparteien und zu den Modalitäten der Ausübung dieses Rechts. Sie ist dem Änderungsprotokoll im Anhang beigelegt.

Änderungen der Verfahrensordnung unterliegen einer Zweidrittelmehrheit, ausgenommen Änderungen der Bestimmungen zum Stimmrecht und entsprechender Modalitäten, für die Artikel 25 des Übereinkommens gilt.

Bei Beitritt hat die EU eine Erklärung abzugeben, in der die Verteilung der Zuständigkeiten zwischen der EU und ihren Mitgliedstaaten hinsichtlich des Schutzes von personenbezogenen Daten nach dem Übereinkommen klargestellt wird. Anschließend wird die EU den Generalsekretär über wesentliche Änderungen dieser Kompetenzverteilung unterrichten.

Gemäß Artikel 25 kann der Übereinkommensausschuss Änderungen am Übereinkommen empfehlen und Änderungsvorschläge einer Vertragspartei des Übereinkommens oder des Ministerkomitees prüfen (Artikel 23 Buchstaben b und c).

Um die Umsetzung der Datenschutzgrundsätze des Übereinkommens sicherzustellen, hat der Übereinkommensausschuss eine Schlüsselrolle bei der Beurteilung der Einhaltung des

Übereinkommens, sowohl bei der Vorbereitung einer Beurteilung des auf Seiten eines Beitrittskandidaten vorhandenen Datenschutzniveaus (Artikel 23 Buchstabe e) als auch bei der periodischen Überprüfung der Umsetzung des Übereinkommens durch die Vertragsparteien (Artikel 23 Buchstabe h). Der Übereinkommensausschuss kann auch auf Ersuchen eines Staates oder einer internationalen Organisation bewerten, ob das dort gewährte Schutzniveau für personenbezogene Daten mit dem Übereinkommen im Einklang ist (Artikel 23 Buchstabe f).

Stellungnahmen zum Niveau der Einhaltung des Übereinkommens erarbeitet der Übereinkommensausschuss auf der Grundlage eines in der Verfahrensordnung dargelegten fairen, transparenten und öffentlichen Verfahrens.

Im Übrigen kann der Übereinkommensausschuss Modelle für standardisierte Garantien für Datenübermittlungen genehmigen (Artikel 23 Buchstabe g).

Schließlich kann der Übereinkommensausschuss dazu beitragen, Schwierigkeiten zwischen den Vertragsparteien beizulegen (Artikel 23 Buchstabe i). Im Falle von Streitigkeiten wird der Übereinkommensausschuss versuchen, eine Beilegung im Wege von Verhandlungen oder auf sonstigem gütlichen Wege zu erreichen.

Zu Kapitel VII

Änderungen

Zu Artikel 25 – Änderungen

Das Ministerkomitee, das den ursprünglichen Wortlaut des Übereinkommens verabschiedete, ist auch für die Annahme von Änderungen zuständig.

Gemäß Absatz 1 kann das Ministerkomitee selbst, der Übereinkommensausschuss oder eine Vertragspartei (ganz gleich, ob es sich dabei um einen Mitgliedstaat des Europarats handelt oder nicht) die Initiative für Änderungen ergreifen.

Gemäß Absatz 3 müssen Änderungsvorschläge, die nicht vom Übereinkommensausschuss selbst stammen, diesem zur Stellungnahme vorgelegt werden.

Grundsätzlich tritt jede Änderung am dreißigsten Tag nach dem Zeitpunkt in Kraft, zu dem alle Vertragsparteien dem Generalsekretär des Europarats die Annahme der Änderung angezeigt haben.

Das Ministerkomitee kann jedoch unter bestimmten Umständen nach Konsultation des Übereinkommensausschusses einstimmig beschließen, dass eine Änderung nach Ablauf eines Zeitraums von drei Jahren in Kraft tritt, es sei denn, eine Vertragspartei hat dem Generalsekretär einen Einwand dagegen notifiziert. Dieses Verfahren, mit dem das Inkrafttreten von Änderungen bei gleichzeitiger Wahrung des Grundsatzes der Zustimmung aller Vertragsparteien beschleunigt werden soll, soll für kleinere und technische Änderungen gelten.

Zu Kapitel VIII

Schlussbestimmungen

Zu Artikel 26 – Inkrafttreten

Da ein weiter geografischer Geltungsbereich für die Wirksamkeit des Übereinkommens als wesentlich angesehen wird, sind nach Absatz 2 für das Inkrafttreten des Übereinkommens Ratifizierungen von fünf Mitgliedstaaten notwendig.

Das Übereinkommen liegt zur Unterzeichnung durch die Europäische Union auf.¹⁴

Zu Artikel 27 – Beitritt von Nichtmitgliedstaaten oder internationalen Organisationen

Das ursprünglich in enger Zusammenarbeit mit der OECD und mehreren nichteuropäischen Staaten entwickelte Übereinkommen ist für jeden Staat weltweit, der die Bestimmungen des Übereinkommens erfüllt, offen. Der Übereinkommensausschuss hat die Aufgabe, die Einhaltung zu beurteilen und für das Ministerkomitee eine Stellungnahme zum Datenschutzniveau des Beitrittskandidaten vorzubereiten.

In Anbetracht der Grenzenlosigkeit von Datenströmen wird der Beitritt von Ländern und internationalen Organisationen weltweit angestrebt. Nur solche internationalen Organisationen, die als dem Völkerrecht unterliegende Organisationen definiert sind, können dem Übereinkommen beitreten.

Zu Artikel 28 – Gebietsklausel

Im Hinblick auf die Heranziehung entfernter Länder für Datenverarbeitungstätigkeiten aus Kosten- oder Personalgründen oder wegen der Möglichkeit der Datenverarbeitung wechselweise am Tage oder in der Nacht hat die Anwendung des Übereinkommens auf entlegene Gebiete, die der Rechtshoheit einer Vertragspartei unterliegen oder in deren Namen eine Vertragspartei Verpflichtungen eingehen kann, praktische Bedeutung.

Zu Artikel 29 – Vorbehalte

Die Vorschriften des Übereinkommens sind die grundlegenden und wichtigsten Bestandteile für wirksamen Datenschutz. Gegen die Bestimmungen des Übereinkommens, die mit Blick auf die unter bestimmten Artikeln zulässigen Ausnahmen und Beschränkungen im Übrigen angemessen flexibel sind, gestattet das Übereinkommen keine Vorbehalte.

Zu Artikel 30 – Kündigung

Jede Vertragspartei kann das Übereinkommen jederzeit kündigen.

Zu Artikel 31 – Notifikationen

Diese Bestimmungen entsprechen den üblichen Schlussbestimmungen in anderen Übereinkommen des Europarats.

¹⁴ Mit dem Inkrafttreten dieses Protokolls werden die vom Ministerkomitee am 15. Juni 1999 gebilligten Änderungen des Übereinkommens gegenstandslos.

Stand: 01.04.2020