Erläuterungen

Allgemeiner Teil

I. Ausgangslage

Das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 223, im Folgenden: Protokoll) hat gesetzändernden bzw. gesetzesergänzenden Inhalt und bedarf daher der Genehmigung des Nationalrats gemäß Art. 50 Abs. 1 Z 1 B-VG. Es hat nicht politischen Charakter. Es ist erforderlich, eine allfällige unmittelbare Anwendung des Protokolls im innerstaatlichen Rechtsbereich durch einen Beschluss gemäß Art. 50 Abs. 2 Z 4 B-VG, dass dieser Staatsvertrag durch Erlassung von Gesetzen zu erfüllen ist, auszuschließen. Da durch das Protokoll keine Angelegenheiten des selbständigen Wirkungsbereiches der Länder geregelt werden, bedarf es keiner Zustimmung des Bundesrates gemäß Art. 50 Abs. 2 Z 2 B-VG.

Österreich ist Vertragspartei des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, BGBl. Nr. 317/1988 (im Folgenden: Übereinkommen), und hat auch das Zusatzprotokoll betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr, BGBl. III Nr. 91/2008, ratifiziert.

Im Jahr 2012 wurden auf Europaratsebene Verhandlungen zur Modernisierung des Übereinkommens aufgenommen. An den primär im „Ad hoc Committee on Data Protection (CAHDATA)“ geführten Verhandlungen waren sowohl die Europäische Kommission im Rahmen jener Angelegenheiten, die in die Zuständigkeit der Europäischen Union (EU) fallen, als auch die EU-Mitgliedstaaten im Rahmen ihrer Zuständigkeiten (insb. Verteidigung, nationale Sicherheit) beteiligt. Die Verhandlungen, die bis zum Abschluss der parallel geführten Verhandlungen zum neuen EU-Datenschutzrechtsrahmen ausgesetzt worden waren, mündeten schließlich 2018 in das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

Anlässlich der 128. Ministertagung am 18. Mai 2018 nahm das Ministerkomitee des Europarats den Text dieses Protokolls an.

Die wesentlichen Inhalte des Protokolls sind:

- Annäherung der Vorschriften des Übereinkommens an den neuen EU-Datenschutzrechtsrahmen (etwa Stärkung und Erweiterung der datenschutzrechtlichen Betroffenenrechte, Nachschärfung der Pflichten des Verantwortlichen);
- Wegfall der Möglichkeit, bestimmte Bereiche (z. B. nationale Sicherheit oder Verteidigung) durch Erklärung vollständig vom Übereinkommen auszunehmen, bei gleichzeitiger Ausweitung der Beschränkungsmöglichkeiten in diesen Bereichen;
- Schaffung einer Beitrittsmöglichkeit für internationale Organisationen (einschließlich der EU);
- Begünstigung grenzüberschreitender Datenflüsse zwischen Vertragsstaaten;
- Stärkung und Ausbau der Aufsichtsbehörden und Schaffung eines Kooperationsmechanismus;
- Stärkung des Beratenden Ausschusses des Europarates als Aufsichtsorgan.

Das Protokoll wurde am 10. Oktober 2018 in Straßburg zur Unterzeichnung aufgelegt und unter anderem von Österreich unterzeichnet.

Das Protokoll tritt gemäß seinem Art. 37 drei Monate nach Ratifikation durch sämtliche Vertragsstaaten in Kraft. Sollte dies nicht binnen fünf Jahren erfolgen, tritt es, soweit es von zumindest 38 Vertragsstaaten ratifiziert wurde, in Bezug auf diese Vertragsstaaten in Kraft. Mit Stand 11. März 2022 wurde das Protokoll von 17 Vertragsstaaten (darunter zwölf EU-Mitgliedstaaten) ratifiziert und von 27 weiteren Vertragsstaaten unterzeichnet.

Die EU-Mitgliedstaaten wurden mit Beschluss (EU) 2019/682 zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Protokoll zur Änderung des Übereinkommens des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zu ratifizieren, ABl. Nr. L 115 vom 02.05.2019 S. 7, zur Ratifikation des Protokolls im Interesse der Union ermächtigt.

Da mit dem Protokoll das Übereinkommen im Wesentlichen an den EU-Datenschutzrechtsrahmen angeglichen wird, sind keine materiellen Änderungen des innerstaatlichen Datenschutzrechts erforderlich.

Die mit der Durchführung dieses Protokolls verbundenen Kosten finden ihre Bedeckung in den Budgets des/der zuständigen Ressorts.

Im Folgenden wird der vom Ministerkomitee des Europarates gebilligte Erläuternde Bericht zum Übereinkommen in seiner durch das Protokoll geänderten Fassung wiedergegeben.

II. Erläuternder Bericht

In den 35 Jahren, die seit der Auflage des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, auch bekannt als Übereinkommen Nr. 108, zur Unterzeichnung verstrichen sind, hat das Übereinkommen in über 40 europäischen Ländern als Grundlage für das internationale Datenschutzrecht gedient. Es hat Politik und Gesetzgebung auch weit über die Grenzen Europas hinaus beeinflusst. Angesichts der täglich neuen Herausforderungen für die Menschenrechte und Grundfreiheiten, insbesondere für das Recht auf Privatleben, schien es klar, dass das Übereinkommen modernisiert werden sollte, um den neuen Herausforderungen im Bereich des Schutzes der Privatsphäre, die sich aus der zunehmenden Nutzung neuer Informations- und Kommunikationstechnologien (IT), der Globalisierung der Verarbeitungsvorgänge und dem immer umfangreicheren Fluss personenbezogener Daten ergeben, besser gerecht zu werden und gleichzeitig den Evaluierungs- und Follow-up-Mechanismus des Übereinkommens zu stärken.

Es zeigte sich breites Einvernehmen über folgende Aspekte des Modernisierungsprozesses: Der allgemeine und technologieneutrale Charakter der Bestimmungen des Übereinkommens muss beibehalten werden; die Kohärenz und Kompatibilität des Übereinkommens mit anderen Rechtsrahmen muss gewahrt bleiben; und der offene Charakter des Übereinkommens, der ihm ein einzigartiges Potenzial als universeller Standard verleiht, muss bekräftigt werden. Der Text des Übereinkommens ist allgemeiner Natur und kann durch detailliertere, nicht verbindliche bereichsspezifische Texte, insbesondere durch Empfehlungen des Ministerkomitees, die unter Beteiligung interessierter Interessengruppen ausgearbeitet werden, ergänzt werden.

Die Modernisierungsarbeiten erfolgten im breiteren Kontext verschiedener paralleler Reformen internationaler Datenschutzinstrumente und unter gebührender Berücksichtigung der Leitlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten aus dem Jahr 1980 (neugefasst im Jahr 2013), der Leitlinien der Vereinten Nationen für die Regelung der personenbezogenen Datenbanken aus dem Jahr 1990, des Rechtsrahmens der Europäischen Union (EU) seit dem Jahr 1995[1], des Datenschutzrechtsrahmens für die Asiatisch-Pazifische Wirtschaftliche Zusammenarbeit (2004) und der „Internationalen Standards für den Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten“ aus dem Jahr 2009.[2] Insbesondere im Hinblick auf das EU-Reformpaket zum Datenschutz liefen die Arbeiten parallel und es wurde mit größter Sorgfalt auf die Gewährleistung von Kohärenz zwischen beiden Rechtsrahmen geachtet. Der Datenschutzrahmen der EU konkretisiert und erweitert die Grundsätze des Übereinkommens Nr. 108 und berücksichtigt den Beitritt zum Übereinkommen Nr. 108, insbesondere im Hinblick auf internationale Übermittlungen.[3]

Der durch Artikel 18 des Übereinkommens eingesetzte Beratende Ausschuss bereitete Entwürfe für Modernisierungsvorschläge vor, die auf seiner 29. Plenartagung (27.-30. November 2012) angenommen und dem Ministerkomitee vorgelegt wurden. Das Ministerkomitee beauftragte daraufhin den Ad-hoc-Ausschuss zum Datenschutz (CAHDATA) mit der Aufgabe, die Modernisierungsvorschläge fertigzustellen. Dies wurde anlässlich der 3. Sitzung des CAHDATA (1.-3. Dezember 2014) abgeschlossen. Im Anschluss an die Fertigstellung des EU-Datenschutzrahmens wurde ein weiterer CAHDATA eingerichtet, um offene Fragen zu prüfen. Bei der letzten CAHDATA-Sitzung (15.-16. Juni 2016) wurden die Vorschläge fertiggestellt und dem Ministerkomitee zur Prüfung und Annahme übermittelt.

Der Text des Erläuternden Berichts soll die Anwendung der Bestimmungen des Übereinkommens leiten und unterstützen und bietet einen Anhaltspunkt, wie sich die Verfasser die Funktionsweise des Übereinkommens vorgestellt haben.

Das Ministerkomitee hat den Erläuternden Bericht gebilligt. In dieser Hinsicht ist der Erläuternde Bericht Bestandteil des Zusammenhangs, in dem die Bedeutung bestimmter im Übereinkommen verwendeter Begriffe zu ermitteln ist (Anmerkung: s. Artikel 31 Absätze 1 und 2 des Wiener Übereinkommens der Vereinten Nationen über das Recht der Verträge).

---

1 Datenschutz-Grundverordnung (EU) 2016/679 („DSGVO“) und Datenschutz-Richtlinie für Polizei und Justiz (EU) 2016/680 („DSRL-PJ“).

2 Begrüßt von der 31. Internationalen Datenschutzkonferenz (International Conference of Data Protection and Privacy Commissioners), die vom 4.-6. November 2009 in Madrid stattfand.

3 Siehe insbesondere Erwägungsgrund 105 der DSGVO.

Das Protokoll wurde am 18. Mai 2018 vom Ministerkomitee angenommen. Der Anhang zum Protokoll ist ein integraler Bestandteil des Protokolls und hat die gleichen Rechtswirkungen wie die anderen Bestimmungen des Protokolls.

Dieses Protokoll wurde am 10. Oktober 2018 in Straßburg zur Unterzeichnung aufgelegt.

Zweck dieses Protokolls ist es, das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) und sein Zusatzprotokoll bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181) zu modernisieren und ihre Anwendung zu stärken. Ab seinem Inkrafttreten gilt das Zusatzprotokoll als integraler Bestandteil des Übereinkommens in seiner geltenden Fassung.

Die Erläuternden Berichte zum Übereinkommen Nr. 108 und zu seinem Zusatzprotokoll bleiben insofern relevant, als sie den historischen Zusammenhang vermitteln und die Entwicklung beider Instrumente beschreiben, und sie können für diese Zwecke in Verbindung mit dem Erläuternden Bericht zu diesem Protokoll gelesen werden.

Besonderer Teil

Die nachstehenden Erläuterungen entsprechen – mit Ausnahme der spezifischen Bezugnahmen auf die österreichische Rechtslage sowie der Erläuterungen zu den Schlussbestimmungen des Protokolls – dem Inhalt des Erläuternden Berichts zum Protokoll, der auf das Übereinkommen in seiner durch das Protokoll geänderten Fassung Bezug nimmt.

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 andere Kenntnis zu erlangen, sie zu verstehen und zu bestimmen. Dementsprechend wird in der Präambel ausdrücklich auf das Recht auf persönliche Entscheidungsfreiheit und das Recht, selbst über seine personenbezogenen Daten zu bestimmen, das sich insbesondere aus dem Recht auf Privatsphäre und der Würde des Menschen ergibt, Bezug genommen. Die Würde des Menschen erfordert, dass bei der Verarbeitung personenbezogener Daten Garantien vorgesehen werden, damit Menschen nicht als bloße Objekte behandelt werden.

Unter Berücksichtigung der Rolle des Rechts auf Schutz personenbezogener Daten in der Gesellschaft wird in der Präambel der Grundsatz betont, dass die Interessen, Rechte und Grundfreiheiten der Menschen erforderlichenfalls miteinander in Einklang zu bringen sind. Um ein sorgfältiges Gleichgewicht zwischen den verschiedenen Interessen, Rechten und Grundfreiheiten zu gewährleisten, legt das Übereinkommen bestimmte Bedingungen und Einschränkungen in Bezug auf die Verarbeitung von Informationen und den Schutz personenbezogener Daten fest. So ist beispielsweise das Datenschutzrecht in Bezug zum Recht auf „freie Meinungsäußerung“ gemäß Artikel 10 der Europäischen Menschenrechtskonvention (SEV Nr. 5), das die Meinungsfreiheit und die Freiheit zum Empfang und zur Mitteilung von Informationen einschließt, zu sehen. Darüber hinaus bestätigt das Übereinkommen, dass die Ausübung des Datenschutzrechts, das nicht absolut ist, insbesondere nicht als allgemeines Mittel zur Verhinderung des öffentlichen Zugangs zu amtlichen Dokumenten herangezogen werden sollte.[4]

Das Übereinkommen Nr. 108 schützt durch die darin festgelegten Grundsätze und die darin verankerten Werte den Menschen und bietet gleichzeitig einen Rahmen für den internationalen Datenverkehr. Dies ist von hoher Bedeutung, weil der globale Informationsfluss in der modernen Gesellschaft eine zunehmend wichtige Rolle spielt, zumal er die Ausübung der Grundrechte und -freiheiten ermöglicht und gleichzeitig Innovationen anstößt und den sozialen und wirtschaftlichen Fortschritt fördert, während er gleichzeitig eine entscheidende Rolle bei der Gewährleistung der öffentlichen Sicherheit spielt. Der Verkehr personenbezogener Daten in einer Informations- und Kommunikationsgesellschaft muss die Grundrechte und -freiheiten der Menschen respektieren. Auch bei der Entwicklung und Verwendung innovativer Technologien sollten diese Rechte respektiert werden. Dies wird dazu beitragen, Vertrauen in die Innovation und neue Technologien zu schaffen und ihre Weiterentwicklung zu ermöglichen.

Da die internationale Zusammenarbeit zwischen den Aufsichtsbehörden ein Schlüsselelement für den wirksamen Schutz der Menschen ist, zielt das Übereinkommen darauf ab, diese Zusammenarbeit zu verstärken, insbesondere indem es die Vertragsparteien zur gegenseitigen Hilfeleistung verpflichtet und

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

eine geeignete Rechtsgrundlage für einen Rahmen der Zusammenarbeit und des Informationsaustauschs für Ermittlungen und die Strafverfolgung schafft.

Zu Kapitel I – Allgemeine Bestimmungen

Zu Artikel 1 – Gegenstand und Zweck

Der erste Artikel beschreibt Gegenstand und Zweck des Übereinkommens. Dieser Artikel konzentriert sich auf das Schutzobjekt: Natürliche Personen sind bei der Verarbeitung ihrer personenbezogenen Daten zu schützen.[5] Zuletzt wurde der Datenschutz als Grundrecht in Artikel 8 der Charta der Grundrechte der EU sowie in die Verfassungen mehrerer Vertragsparteien des Übereinkommens aufgenommen.

Die im Übereinkommen festgelegten Garantien werden auf jede natürliche Person ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnortes ausgedehnt. Eine Diskriminierung zwischen Staatsbürgern und Drittstaatsangehörigen bei der Anwendung dieser Garantien ist nicht gestattet.[6] Klauseln, die den Datenschutz auf eigene Staatsangehörige oder rechtmäßig aufhältige ausländische Staatsangehörige beschränken, wären mit dem Übereinkommen unvereinbar.

Zu Artikel 2 – Begriffsbestimmungen

Die in diesem Übereinkommen verwendeten Begriffsbestimmungen sollen die einheitliche Verwendung von Begriffen zur Beschreibung bestimmter Grundkonzepte in nationalen Rechtsvorschriften sicherstellen.

Buchstabe a – „personenbezogene Daten“

„Bestimmbare natürliche Person“ bedeutet eine Person, die direkt oder indirekt identifiziert werden kann. Eine Person gilt nicht als „bestimmbar“, wenn ihre Identifizierung unangemessenen Zeit-, Arbeits- oder Mittelaufwand erfordern würde. Dies ist zum Beispiel der Fall, wenn die Identifizierung eines Betroffenen übermäßig komplexe, langwierige und kostspielige Schritte erfordern würde. Die Frage, was als „unangemessener Zeit-, Arbeits- oder Mittelaufwand“ gilt, sollte im Einzelfall beurteilt werden. Beispielsweise könnten der Zweck der Verarbeitung sowie objektive Kriterien wie die Kosten, der Nutzen einer solchen Identifizierung, die Art des Verantwortlichen, die verwendete Technologie usw. berücksichtig werden. Darüber hinaus könnten technologische und sonstige Entwicklungen beeinflussen, was unter „unangemessenem Zeit-, Arbeits- oder anderem Mittelaufwand“ zu verstehen ist.

Der Begriff „bestimmbar“ bezieht sich nicht nur auf die bürgerliche oder rechtliche Identität des Menschen als solche, sondern auch auf alles, wodurch eine Person „individualisiert“ oder herausgegriffen (und somit unterschiedlich behandelt) werden kann. Diese „Individualisierung“ könnte beispielsweise erfolgen, indem speziell auf sie 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, von Standortdaten, einer IP-Adresse oder eines anderen Merkmals Bezug genommen wird. Die Verwendung eines Pseudonyms oder eines digitalen Merkmals bzw. einer digitalen Identität führt nicht zur Anonymisierung der Daten, da der Betroffene weiterhin bestimmbar oder individualisierbar sein kann. Pseudonymisierte Daten sind daher als personenbezogene Daten zu betrachten und fallen unter die Bestimmungen des Übereinkommens. Bei der Beurteilung der Angemessenheit von Garantien, die zur Minderung der Risiken für Betroffene eingesetzt werden, sollte die Qualität der eingesetzten Pseudonymisierungstechniken gebührend berücksichtigt werden.

Daten sind nur so lange als anonym zu betrachten, wie es unmöglich ist, den Personenbezug zum Betroffenen wiederherzustellen, oder wenn eine solche Wiederherstellung unter Berücksichtigung der zum Zeitpunkt der Verarbeitung verfügbaren Technologie und der technologischen Entwicklungen unangemessenen Zeit, Arbeits- oder Mittelaufwand erfordern würde. Daten, die anonym erscheinen, weil sie kein offensichtliches Identifizierungselement enthalten, können dennoch in bestimmten Fällen (ohne unangemessenen Zeit-, Arbeits- oder Mittelaufwand) die Bestimmung eines Menschen ermöglichen. Dies ist beispielsweise dann der Fall, wenn es dem Verantwortlichen oder einer anderen Person möglich ist, einen Menschen durch die Kombination verschiedener Datenarten wie etwa physische, physiologische,

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

6 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, Z 3.3 ‚Jedermann‘ frei von Diskriminierung [‚Everyone‘ without discrimination].

genetische, wirtschaftliche oder soziale Daten (Kombination von Daten über Alter, Geschlecht, Beruf, geographischen Standort, Familienstand usw.) zu identifizieren. In diesem Fall können die Daten nicht als anonym betrachtet werden und fallen unter die Bestimmungen des Übereinkommens.

Bei der Anonymisierung von Daten sollten geeignete Maßnahmen zur Vermeidung einer Wiederherstellung des Personenbezuges getroffen werden; insbesondere sollten alle technischen Mittel eingesetzt werden, um zu gewährleisten, dass der Mensch nicht oder nicht mehr identifizierbar ist. Sie sollten angesichts der raschen technologischen Entwicklung regelmäßig neu bewertet werden.

Buchstaben b und c – „Datenverarbeitung“

Die „Datenverarbeitung“ beginnt mit der Erhebung von personenbezogenen Daten und umfasst alle Vorgänge, die mit personenbezogenen Daten ausgeführt werden, ganz gleich ob teilweise oder vollständig automatisiert. Soweit keine automatisierte Verarbeitung stattfindet, bezeichnet Datenverarbeitung einen Vorgang oder eine Reihe von Vorgängen mit personenbezogenen Daten innerhalb eines strukturierten Datensatzes, die nach bestimmten Kriterien zugänglich oder abrufbar sind, sodass es dem Verantwortlichen oder irgendeiner anderen Person möglich ist, die Daten zu einem bestimmten Betroffenen zu suchen, zu kombinieren oder abzugleichen.

Buchstabe d – „Verantwortlicher“

Der Begriff „Verantwortlicher“ bezeichnet die Person oder Stelle, die die Entscheidungsbefugnis über die Zwecke und Mittel der Verarbeitung hat, gleichgültig, ob sich diese Befugnis aus einer Rechtsvorschrift oder aus tatsächlichen Umständen, die von Fall zu Fall zu beurteilen sind, ableitet. In einigen Fällen kann es mehrere Verantwortliche oder gemeinsam Verantwortliche geben (die gemeinsam für eine Verarbeitung und möglicherweise für verschiedene Aspekte dieser Verarbeitung verantwortlich sind). Bei der Beurteilung, ob es sich bei der Person oder Stelle um einen Verantwortlichen handelt, sollte insbesondere berücksichtigt werden, ob diese Person oder Stelle die Gründe für die Verarbeitung, d.h. ihre Zwecke und die dafür eingesetzten Mittel, bestimmt. Weitere relevante Faktoren für diese Beurteilung sind u.a., ob die Person oder Stelle die Kontrolle über die Verarbeitungsmethoden, die Wahl der zu verarbeitenden Daten und darüber, wer auf die Daten zugreifen darf, hat. Als Auftragsverarbeiter gilt, wer nicht direkt dem Verantwortlichen unterstellt ist und die Verarbeitung im Auftrag des Verantwortlichen und ausschließlich nach dessen Anweisungen durchführt. Der Verantwortliche bleibt auch dann für die Verarbeitung verantwortlich, wenn ein Auftragsverarbeiter die Daten in seinem Auftrag verarbeitet.

Buchstabe e – „Empfänger“

„Empfänger“ ist eine Person oder Einrichtung, die personenbezogene Daten erhält oder der personenbezogene Daten zugänglich gemacht werden. Je nach den Umständen kann der Empfänger Verantwortlicher oder Auftragsverarbeiter sein. Ein Unternehmen kann beispielsweise bestimmte Daten von Mitarbeitern an eine Regierungsbehörde schicken, die sie als Verantwortlicher für Steuerzwecke verarbeitet. Es kann sie an ein Unternehmen übermitteln, das Speicherdienste anbietet und als Auftragsverarbeiter fungiert. Der Empfänger kann eine Behörde oder Einrichtung sein, der das Recht zur Ausübung hoheitlicher Befugnisse eingeräumt wurde; werden die von der Behörde oder Einrichtung erhaltenen Daten im Rahmen einer bestimmten Anfrage im Einklang mit dem anwendbaren Recht verarbeitet, gilt diese Behörde oder Einrichtung jedoch nicht als Empfänger. Behördliche Ersuchen um Offenlegung sollten immer schriftlich, begründet und im Einzelfall gestellt werden und nicht vollständige Dateisysteme betreffen oder zur Verknüpfung von Dateisystemen führen. Die Verarbeitung personenbezogener Daten durch diese Behörden sollte den geltenden Datenschutzbestimmungen nach Maßgabe des Verarbeitungszwecks entsprechen.

Buchstabe f – „Auftragsverarbeiter“

„Auftragsverarbeiter“ ist jede natürliche oder juristische Person (die nicht Mitarbeiter des Verantwortlichen ist), die im Auftrag des Verantwortlichen und nach dessen Anweisungen Daten verarbeitet. Die Weisungen des Verantwortlichen legen die Grenze dessen fest, was der Auftragsverarbeiter mit den personenbezogenen Daten tun darf.

Zu Artikel 3 – Anwendungsbereich

Gemäß Absatz 1 sollte jede Vertragspartei das Übereinkommen auf alle ihrer Hoheitsgewalt unterstehenden Verarbeitungen, ob im öffentlichen oder privaten Bereich, anwenden.

Die Ziele des Bestandes über einen längeren Zeitraum und der Anpassung an kontinuierliche technologische Entwicklungen rechtfertigen es, den Schutzumfang vom Begriff der „Hoheitsgewalt“ der Vertragsparteien abhängig zu machen.

Absatz 2 schließt die Verarbeitung für rein persönliche oder familiäre Tätigkeiten vom Anwendungsbereich des Übereinkommens aus. Mit diesem Ausschluss soll vermieden werden, Datenverarbeitungen, die von Menschen in ihrer Privatsphäre für Aktivitäten im Zusammenhang mit der Gestaltung ihres Privatlebens vorgenommen werden, mit unangemessenen Verpflichtungen zu belegen. Persönliche oder familiäre Aktivitäten sind Aktivitäten, die eng und objektiv mit dem Privatleben eines Menschen verbunden sind und die persönliche Sphäre anderer nicht wesentlich beeinträchtigen. Diese Aktivitäten haben keine beruflichen oder kommerziellen Aspekte und beziehen sich ausschließlich auf persönliche oder familiäre Aktivitäten wie etwa die Speicherung von Familien- oder Privatfotos auf einem Computer, die Erstellung einer Liste mit Kontaktdaten von Freunden und Familienmitgliedern, Korrespondenz usw. Die gemeinsame Nutzung von Daten im privaten Bereich umfasst insbesondere die gemeinsame Nutzung innerhalb einer Familie, eines eingeschränkten Freundeskreises oder eines der Größe nach begrenzten Kreises, der auf einer persönlichen Beziehung oder einem besonderen Vertrauensverhältnis beruht.

Ob es sich bei Tätigkeiten um „rein persönliche oder familiäre Aktivitäten“ handelt, hängt von den Umständen ab. Beispielsweise gilt die Ausnahme nicht, wenn personenbezogene Daten einer Vielzahl von Personen oder von Personen, die offensichtlich nicht dem privaten Bereich angehören, etwa auf einer öffentlichen Website im Internet zugänglich gemacht werden. Ebenso wenig kann der Betrieb eines Kamerasystems, mit dem Videoaufnahmen von Personen dauerhaft auf einem Aufzeichnungsgerät wie einer Festplatte gespeichert werden und das von jemandem im Eigenheim zum Schutz des Eigentums, der Gesundheit und des Lebens der Hauseigentümer installiert wird, jedoch – wenn auch nur teilweise – den öffentlichen Raum erfasst und dementsprechend aus dem privaten Umfeld der solcherart datenverarbeitenden Person nach außen gerichtet ist, als rein „persönliche oder familiäre“ Aktivität angesehen werden.[7]

Das Übereinkommen gilt jedoch für Datenverarbeitungen, die von Anbietern von Instrumenten zur Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Aktivitäten vorgenommen werden.

Während das Übereinkommen die Datenverarbeitung in Bezug auf Menschen betrifft, können die Vertragsparteien den Schutz in ihrem innerstaatlichen Recht auf juristische Personen betreffende Daten ausdehnen, um deren berechtigte Interessen zu schützen. Das Übereinkommen gilt für lebende Menschen: es soll nicht auf personenbezogene Daten über Verstorbene Anwendung finden. Dies hindert die Vertragsparteien jedoch nicht daran, den Schutz auf Verstorbene auszudehnen.

Zu Kapitel II – Grundsätze für den Schutz personenbezogener Daten

Zu Artikel 4 – Pflichten der Vertragsparteien

Nach diesem Artikel verpflichtet das Übereinkommen die Vertragsparteien, seine Bestimmungen in ihr Recht aufzunehmen und ihre wirksame Anwendung in der Praxis zu gewährleisten; wie dies geschieht, hängt von der anwendbaren Rechtsordnung und der Herangehensweise an die Einbindung von internationalen Übereinkünften ab.

Der Begriff „Recht der Vertragsparteien“ bezeichnet nach der Rechts- und Verfassungsordnung des jeweiligen Landes alle durchsetzbaren Vorschriften sowohl des kodifizierten Rechts als auch der Richterrechts. Es muss die qualitativen Anforderungen an die Zugänglichkeit und Voraussehbarkeit (oder „Vorhersehbarkeit“) erfüllen. Dies bedeutet, dass das Gesetz hinreichend klar sein sollte, um Menschen und anderen Einrichtungen zu ermöglichen, ihr eigenes Verhalten im Hinblick auf die zu erwartenden Rechtsfolgen ihrer Handlungen zu steuern, und dass die wahrscheinlich von diesem Gesetz betroffenen Personen Zugang zu ihm haben sollten. Es umfasst Vorschriften, die (natürlichen wie juristischen) Personen Pflichten auferlegen oder Rechte übertragen, die Organisation, Befugnisse und Verantwortlichkeiten von Behörden regeln oder Verfahren festlegen. Insbesondere umfasst es die Verfassungen der Staaten und alle schriftlichen Gesetzgebungsakte (Gesetze im formellen Sinn) sowie alle auf solchen Gesetzen beruhenden Regelungsmaßnahmen (Dekrete, Verordnungen, Erlässe und Verwaltungsrichtlinien). Es umfasst auch die im innerstaatlichen Recht anwendbaren internationalen Übereinkommen einschließlich des EU-Rechts. Darüber hinaus umfasst es alle anderen Gesetze allgemeiner Art, sei es des öffentlichen oder des Privatrechts (einschließlich des Vertragsrechts), sowie die Rechtsprechung in Ländern mit Gewohnheitsrecht und allen Ländern, die über eine etablierte Rechtsprechung zur Auslegung des kodifizierten Rechts verfügen. Darüber hinaus umfasst es jeden Akt eines Berufsverbandes aufgrund einer vom Gesetzgeber übertragenen Befugnis in Einklang mit seinen unabhängigen Regelungsbefugnissen.

7 Siehe Europäischer Gerichtshof, *František Ryneš v. Úřad*, 11. Dezember 2014, C-212/13k.

Dieses „Recht der Vertragsparteien“ kann durch freiwillige Regulierungsmaßnahmen im Bereich des Datenschutzes wie etwa Verhaltensregeln oder Standesregeln sinnvoll verstärkt werden. Solche freiwilligen Maßnahmen allein reichen jedoch nicht aus, um die vollständige Einhaltung des Übereinkommens sicherzustellen.

Im Hinblick auf internationale Organisationen[8] kann in bestimmten Situationen, abhängig von der jeweiligen nationalen Rechtsordnung, das Recht dieser internationalen Organisationen unmittelbar auf der nationalen Ebene der Mitgliedstaaten dieser Organisationen angewendet werden.

Die Wirksamkeit der Anwendung der Maßnahmen, mit denen den Bestimmungen des Übereinkommens Wirksamkeit verliehen wird, ist von entscheidender Bedeutung. Bei der Gesamtbeurteilung der Wirksamkeit der Durchführung der Bestimmungen des Übereinkommens durch eine Vertragspartei sollten die Rolle der Aufsichtsbehörde(n) und alle Rechtsmittel, die Betroffenen zur Verfügung stehen, berücksichtigt werden.

In Absatz 2 ist ferner festgelegt, dass die Maßnahmen zur Durchführung des Übereinkommens von den betreffenden Vertragsparteien zu treffen sind und zum Zeitpunkt der Ratifizierung oder des Beitritts, d.h. wenn eine Vertragspartei durch das Übereinkommen rechtlich gebunden wird, in Kraft treten müssen. Diese Bestimmung soll es dem Übereinkommensausschuss ermöglichen, zu verifizieren, ob alle „erforderlichen Maßnahmen“ getroffen wurden, um sicherzustellen, dass die Vertragsparteien des Übereinkommens ihre Verpflichtungen einhalten und das erwartete Datenschutzniveau in ihrem nationalen Recht gewährleisten. Das Verfahren und die Kriterien für diese Verifizierung sind in der Geschäftsordnung des Übereinkommensausschusses klar zu bestimmen.

Die Vertragsparteien verpflichten sich in Absatz 3, aktiv zur Bewertung der Einhaltung ihrer Verpflichtungen beizutragen, um eine regelmäßige Bewertung der Umsetzung der Grundsätze des Übereinkommens (einschließlich seiner Wirksamkeit) zu sicherzustellen. Ein mögliches Element dieses aktiven Beitrags könnte die Vorlage von Berichten der Vertragsparteien über die Anwendung ihres Datenschutzrechts sein.

Bei der Ausübung seiner Befugnisse nach Absatz 3 bewertet der Übereinkommensausschuss nicht, ob eine Vertragspartei wirksame Maßnahmen ergriffen hat, soweit sie von Ausnahmen und Beschränkungen in Übereinstimmung mit den Bestimmungen dieses Übereinkommens Gebrauch gemacht hat. Eine Vertragspartei ist daher nach Artikel 11 Absatz 3 nicht verpflichtet, dem Übereinkommensausschuss Verschlusssachen zur Verfügung zu stellen.

Die Bewertung, ob eine Vertragspartei das Übereinkommen erfüllt, wird vom Übereinkommensausschuss auf der Grundlage eines objektiven, fairen und transparenten Verfahrens vorgenommen, das vom Übereinkommensausschuss festgelegt und in seiner Verfahrensordnung umfassend erläutert wird.

Zu Artikel 5 – Rechtmäßigkeit der Datenverarbeitung und Qualität der Daten

Absatz 1 sieht vor, dass die Datenverarbeitung verhältnismäßig, d.h. im Verhältnis zum verfolgten legitimen Zweck und unter Berücksichtigung der Interessen, Rechte und Freiheiten der Betroffenen oder des öffentlichen Interesses angemessen sein muss. Eine solche Datenverarbeitung sollte nicht zu einem unverhältnismäßigen Eingriff in diese Interessen, Rechte und Freiheiten führen. Der Grundsatz der Verhältnismäßigkeit ist in allen Stadien der Verarbeitung einschließlich der Anfangsphase, d.h. bei der Entscheidung, ob die Verarbeitung vorgenommen werden soll oder nicht, zu beachten.

Absatz 2 sieht zwei alternative wesentliche Voraussetzungen für eine rechtmäßige Verarbeitung vor: die Einwilligung des Einzelnen oder eine legitime, gesetzlich vorgesehene Grundlage. Die Absätze 1, 2, 3 und 4 des Artikels 5 sind kumulativ und müssen eingehalten werden, um die Rechtmäßigkeit der Datenverarbeitung sicherzustellen.

Die Einwilligung des Betroffenen muss freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich erfolgen. Eine solche Einwilligung muss den freien Ausdruck einer bewussten Wahl darstellen und entweder durch eine Erklärung (die schriftlich, auch auf elektronischem Wege, oder mündlich abgegeben werden kann) oder durch eine eindeutige bestätigende Handlung zum Ausdruck kommen und in diesem spezifischen Zusammenhang die Zustimmung zur vorgeschlagenen Verarbeitung personenbezogener Daten zum Ausdruck bringen. Bloßes Schweigen, Untätigkeit oder vorab validierte Formulare oder Felder sollten daher nicht als Einwilligung gelten. Die Einwilligung sollte sich auf alle Verarbeitungstätigkeiten für den oder die gleichen Zwecke erstrecken (im Falle mehrerer Zwecke ist die Einwilligung für jeden unterschiedlichen Zweck zu erteilen). Es kann Fälle mit unterschiedlichen

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

Einwilligungsentscheidungen geben (z. B. wenn die Art der Daten unterschiedlich ist, obwohl der Zweck derselbe ist – wie etwa bei Gesundheitsdaten und Standortdaten: In solchen Fällen könnte der Betroffene zwar in die Verarbeitung seiner Standortdaten, nicht aber in die Verarbeitung der Gesundheitsdaten einwilligen). Der Betroffene muss über die Auswirkungen seiner Entscheidung (was der Umstand der Einwilligung mit sich bringt und in welchem Umfang die Einwilligung gegeben wird) informiert werden. Auf den Betroffenen darf weder unmittelbar noch mittelbar ungebührlicher Einfluss genommen oder Druck (wirtschaftlicher oder sonstiger Natur) ausgeübt werden und die Einwilligung sollte nicht als freiwillig gelten, wenn der Betroffene keine echte oder freie Wahl hat oder seine Einwilligung nicht vorbehaltlos verweigern oder widerrufen kann.

Im Zusammenhang mit wissenschaftlicher Forschung ist es oft nicht möglich, den Zweck der Verarbeitung personenbezogener Daten für wissenschaftliche Forschungszwecke zum Zeitpunkt der Datenerhebung vollständig zu bestimmen. Deshalb sollte es Betroffenen erlaubt sein, ihre Einwilligung für bestimmte Bereiche der wissenschaftlichen Forschung in Übereinstimmung mit anerkannten ethischen Standards für wissenschaftliche Forschung zu geben. Betroffene sollten, soweit es der beabsichtigte Zweck zulässt, die Möglichkeit haben, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten zu geben.

Eine Einverständniserklärung entbindet nicht von der Notwendigkeit, die in Kapitel II des Übereinkommens festgelegten Grundsätze für den Schutz personenbezogener Daten zu achten; beispielsweise ist die Verhältnismäßigkeit der Verarbeitung weiterhin zu berücksichtigen.

Der Betroffene hat das Recht, die von ihm erteilte Einwilligung jederzeit zu widerrufen (was vom eigenständigen Widerspruchsrecht zu unterscheiden ist). Dies beeinträchtigt nicht die Rechtmäßigkeit der Datenverarbeitung, die stattgefunden hat, bevor der Datenverantwortliche den Widerruf der Einwilligung erhalten hat, erlaubt aber keine weitere Verarbeitung der Daten, es sei denn, dies ist durch eine andere rechtmäßige, gesetzlich geregelte Grundlage gerechtfertigt.

Der Begriff „rechtmäßige, gesetzlich geregelte Grundlage“, auf den in Absatz 2 Bezug genommen wird, umfasst u.a. Datenverarbeitungen, die für die Erfüllung eines Vertrags (oder vorvertragliche Maßnahmen auf Antrag des Betroffenen), an dem der Betroffene beteiligt ist, erforderlich sind, Datenverarbeitungen, die für den Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen Person erforderlich sind, Datenverarbeitungen, die zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich sind und Datenverarbeitungen, die aus Gründen des öffentlichen Interesses oder überwiegender berechtigter Interessen des Verantwortlichen oder eines Dritten vorgenommen werden.

Datenverarbeitungen aus Gründen des öffentlichen Interesses sollten gesetzlich vorgesehen werden, u.a. für Währungs-, Haushalts- und Steuerangelegenheiten, die öffentliche Gesundheit und soziale Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und die Strafvollstreckung, den Schutz der nationalen Sicherheit, die Landesverteidigung, die Verhütung, Ermittlung, Feststellung und Verfolgung von Verstößen gegen die Standesregeln bei reglementierten Berufen, die Durchsetzung zivilrechtlicher Ansprüche und den Schutz der richterlichen Unabhängigkeit und von Gerichtsverfahren. Die Datenverarbeitung kann sowohl einem öffentlichen Interesse als auch den lebenswichtigen Interessen des Betroffenen dienen, wie beispielsweise im Falle von Daten, die für humanitäre Zwecke einschließlich der Überwachung einer lebensbedrohlichen Epidemie und ihrer Ausbreitung oder in humanitären Notfällen verarbeitet werden. Letztere können in Situationen von Naturkatastrophen auftreten, in denen die Verarbeitung personenbezogener Daten von Vermissten für eine begrenzte Zeit für Zwecke Zusammenhang mit dem Notfall – was von Fall zu Fall zu bewerten ist – erforderlich sein kann. Sie können auch in Situationen bewaffneter Konflikte oder anderer Gewalt auftreten.[9] Die Verarbeitung personenbezogener Daten durch staatliche Behörden zur Erreichung von verfassungsrechtlich oder völkerrechtlich festgelegten Zielen staatlich anerkannter Religionsgemeinschaften kann ebenfalls als Verarbeitung im öffentlichen Interesse angesehen werden.

Die Bedingungen für eine rechtmäßige Verarbeitung sind in den Absätzen 3 und 4 festgelegt. Personenbezogene Daten sollten 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 worden sein und die Verarbeitung dieser speziellen Daten muss diesen Zwecken dienen oder darf zumindest nicht unvereinbar mit ihnen sein. Der Verweis auf bestimmte „Zwecke“ bedeutet, dass es nicht erlaubt ist, Daten für unbestimmte, ungenaue oder vage Zwecke zu verarbeiten. Was als rechtmäßiger Zweck anzusehen ist, hängt von den Umständen ab, zumal

9 In denen die vier Genfer Abkommen aus dem Jahr 1949, die dazugehörigen Zusatzprotokolle aus dem Jahr 1977 und die Satzungen des Internationalen Roten Kreuzes und des Roten Halbmondes gelten.

das Ziel darin besteht, sicherzustellen, dass in jedem Fall eine Abwägung aller betroffenen Rechte, Freiheiten und Interessen vorgenommen wird; des Recht auf Schutz personenbezogener Daten einerseits und des Schutzes sonstiger Rechte andererseits, beispielsweise zwischen den Interessen des Betroffenen und den Interessen des Verantwortlichen oder der Gesellschaft.

Das Konzept der Vereinbarkeit der Verwendung sollte die Transparenz, Rechtssicherheit, Vorhersehbarkeit und Fairness der Verarbeitung nicht beeinträchtigen. Personenbezogene Daten sollten nicht in einer Weise, die der Betroffene als unerwartet, unangemessen oder in sonstiger Weise als unzulässig empfinden könnte, weiterverarbeitet werden. Um festzustellen, ob der Weiterverarbeitungszweck mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Erfüllung aller Anforderungen an die Rechtmäßigkeit der ursprünglichen Verarbeitung u.a. jeden Zusammenhang zwischen diesen Zwecken und den Zwecken der beabsichtigten Weiterverarbeitung, den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere die berechtigten Erwartungen der Betroffenen hinsichtlich deren weiterer Verwendung aufgrund ihres Verhältnisses zum Verantwortlichen, die Art der personenbezogenen Daten, die Folgen der beabsichtigten Weiterverarbeitung für die Betroffenen und das Vorhandensein angemessener Garantien sowohl beim ursprünglichen als auch bei den geplanten Weiterverarbeitungsvorgängen berücksichtigen.

Die Weiterverarbeitung personenbezogener Daten, auf die in Absatz 4 b Bezug genommen wird, für im öffentlichen Interesse liegende Archivierungszwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt von vornherein als vereinbar, sofern andere Garantien (wie beispielsweise die Anonymisierung oder Pseudonymisierung von Daten, sofern nicht die Beibehaltung der identifizierbaren Form notwendig ist, Berufsgeheimnisregelungen, Bestimmungen über Zugangsbeschränkungen und die Weitergabe von Daten für die oben genannten Zwecke, insbesondere in Bezug auf Statistiken und öffentliche Archive und andere technische und organisatorische Datensicherheitsmaßnahmen) vorhanden sind und die Vorgänge grundsätzlich jede Nutzung der erhaltenen Informationen für einen bestimmten Menschen betreffende Entscheidungen oder Maßnahmen ausschließen. „Statistische Zwecke“ beziehen sich auf die Ausarbeitung von statistischen Erhebungen oder die Erzeugung von statistischen aggregierten Ergebnissen. Statistik zielt auf die Analyse und Charakterisierung von Massen- oder Kollektivphänomenen in einer untersuchten Bevölkerung ab.[10] Statistische Zwecke können sowohl im öffentlichen als auch im privaten Bereich verfolgt werden. Die Verarbeitung von Daten für „wissenschaftliche Forschungszwecke“ zielt darauf ab, den Forschern Informationen bereitzustellen, die zum Verständnis von Phänomenen in verschiedenen wissenschaftlichen Bereichen (Epidemiologie, Psychologie, Wirtschaft, Soziologie, Linguistik, Politikwissenschaft, Kriminologie usw.) beitragen, um dauerhafte Grundsätze, Verhaltensgesetze oder Kausalitätsmuster festzulegen, die über alle jene Menschen, auf die sie sich beziehen, hinweg gelten.[11] Der Begriff „Historische Forschungszwecke“ schließt die genealogische Forschung ein. „Archivierungszwecke im öffentlichen Interesse“ können auch Archive privater Einrichtungen umfassen, wenn ein öffentliches Interesse daran besteht.

Die verarbeiteten personenbezogenen Daten sollten dem Verarbeitungszweck entsprechen, dafür erheblich sein und nicht darüber hinausgehen. Darüber hinaus sollten die Daten sachlich richtig sein und erforderlichenfalls regelmäßig auf den neuesten Stand gebracht werden.

Die Anforderung von Absatz 4 Buchstabe c, dass die Daten „nicht darüber hinausgehen“ dürfen, verlangt zunächst, dass die Datenverarbeitung auf das für den Verarbeitungszweck erforderliche Maß beschränkt wird. Sie sollten nur dann und so lange verarbeitet werden, wie die Zwecke nicht in zumutbarer Weise durch die Verarbeitung von Informationen, die keine personenbezogenen Daten enthalten, erfüllt werden können. Darüber hinaus bezieht sich diese Anforderung nicht nur auf die Quantität, sondern auch auf die Qualität der personenbezogenen Daten. Personenbezogene Daten, die dem Zweck entsprechen und dafür erheblich sind, aber einen unverhältnismäßigen Eingriff in die betroffenen Grundrechte und -freiheiten bedeuten würden, sollten als über den Verarbeitungszweck hinausgehend erachtet und nicht verarbeitet werden.

Die Anforderung des Absatzes 4 e hinsichtlich Aufbewahrungsfristen für personenbezogene Daten bedeutet, dass die Daten sobald der Zweck, für den sie verarbeitet wurden, erreicht ist, gelöscht oder nur

10 Empfehlung Nr. (97) 18 des Ministerkomitees an die Mitgliedstaaten über den Schutz personenbezogener Daten, die für statistische Zwecke erhoben und verarbeitet werden, Anhang, Punkt 1, 30. September 1997.

11 Erläuterungsprotokoll zur Empfehlung Nr. (97)18 des Ministerkomitees an die Mitgliedstaaten über den Schutz personenbezogener Daten, die für statistische Zwecke erhoben und verarbeitet werden, Ziffern 11 und 14.

in einer Form aufbewahrt werden sollten, die keine unmittelbare oder mittelbare Identifizierung des Betroffenen zulässt.

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

Zu Artikel 6 – Besondere Arten von Daten

Die Verarbeitung bestimmter Arten von Daten oder die Verarbeitung bestimmter Daten, aus denen sensiblen Informationen hervorgehen, kann zu Eingriffen in Interessen, Rechte und Freiheiten führen. Dies kann beispielsweise der Fall sein, wenn die Gefahr einer Diskriminierung oder einer Verletzung der Würde oder körperlichen Unversehrtheit eines Menschen besteht, wenn der intimste Bereich der Betroffenen wie etwa ihr Sexualleben oder ihre sexuelle Orientierung betroffen ist oder wenn die Datenverarbeitung die Unschuldsvermutung beeinträchtigen könnte. Die Datenverarbeitung sollte nur zulässig sein, wenn ergänzend zu anderen Schutzbestimmungen des Übereinkommens geeignete Garantien gesetzlich vorgesehen sind. Das Erfordernis geeigneter Garantien, die die Bestimmungen des Übereinkommens ergänzen, schließt die in Artikel 11 vorgesehene Möglichkeit, Ausnahmen und Einschränkungen der Betroffenenrechte nach Artikel 9 zuzulassen, nicht aus.

Um nachteilige Auswirkungen für den Betroffenen zu verhindern, muss die Verarbeitung sensibler Daten für rechtmäßige Zwecke mit geeigneten Garantien (die den bestehenden Risiken und den zu schützenden Interessen, Rechten und Freiheiten entsprechen) einhergehen, beispielsweise – allein oder kumulativ – mit der ausdrückliche Einwilligung des Betroffenen, einem Gesetz, das den beabsichtigten Zweck und die Mittel der Verarbeitung regelt oder die Ausnahmefälle festlegt, in denen die Verarbeitung solcher Daten zulässig ist, einer Verpflichtung zur Einhaltung eines Berufsgeheimnisses von einer Risikoanalyse ausgehenden Maßnahmen oder einer besonderen und qualifizierten organisatorischen oder technischen Sicherheitsmaßnahme (beispielsweise Datenverschlüsselung).

Bestimmte Arten der Datenverarbeitung können unabhängig vom Zusammenhang der Verarbeitung ein besonderes Risiko für Betroffene mit sich bringen. Dies ist beispielsweise bei der Verarbeitung genetischer Daten, die von Menschen hinterlassen werden und Informationen über die Gesundheit oder Abstammung dieser Person und von Dritten preisgeben können, der Fall. Genetische Daten sind alle Daten über die genetischen Merkmale eines Menschen, die entweder vererbt oder während der frühen pränatalen Entwicklung erworben wurden, wie sie sich aus der Analyse einer biologischen Probe des betreffenden Menschen ergeben: Chromosomen-, DNA- oder RNA-Analyse oder Analyse jedes anderen Elements, das es ermöglicht, gleichwertige Informationen zu erhalten. Ähnliche Risiken bestehen bei der Verarbeitung von Daten, die sich auf Straftaten (einschließlich vermuteter Straftaten), strafrechtliche Verurteilungen (auf der Grundlage des Strafrechts und im Rahmen von Strafverfahren) und damit verbundene Sicherheitsmaßnahmen (einschließlich beispielsweise Freiheitsentzug) beziehen und die die Bereitstellung geeigneter Garantien für die Rechte und Freiheiten der Betroffenen erfordern.

Die Verarbeitung biometrischer Daten, d.h. von Daten, die aus einer spezifischen technischen Verarbeitung von Daten über die physischen, biologischen oder physiologischen Merkmale eines Menschen hervorgehen und mit der die eindeutige Identifizierung oder Authentifizierung eines Menschen möglich ist, gilt ebenfalls als sensibel, wenn sie genau zur eindeutigen Identifizierung des Betroffenen eingesetzt wird.

Der Zusammenhang einer Bildverarbeitung ist für die Bestimmung des sensiblen Charakters der Daten von Bedeutung. Die Bildverarbeitung wird im Allgemeinen keine Verarbeitung sensibler Daten beinhalten, da Bilder nur dann unter die Definition der biometrischen Daten fallen, wenn sie mit bestimmten technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung eines Menschen ermöglichen. Überdies wird eine Bildverarbeitung, die auf die Offenlegung von Informationen über die Rasse, die ethnische Herkunft oder die Gesundheit abzielt (siehe den folgenden Punkt), als Verarbeitung sensibler Daten gelten. Im Gegensatz dazu werden Bilder, die von einem Videoüberwachungssystem in einem Einkaufszentrum ausschließlich aus Sicherheitsgründen verarbeitet werden, im Allgemeinen nicht als Verarbeitung sensibler Daten gelten.

Die Verarbeitung sensibler Daten kann die Rechte der Betroffenen beeinträchtigen, wenn sie der Offenbarung bestimmter Informationen dient. Während die Verarbeitung von Familiennamen in vielen Fällen ohne jedes Risiko für Menschen sein kann (z. B. zu gewöhnlichen Lohnabrechnungszwecken), könnte eine solche Verarbeitung in einigen Fällen sensible Daten beinhalten, beispielsweise wenn der Zweck darin besteht, die ethnische Herkunft oder die religiösen Überzeugungen von Menschen auf der Grundlage der sprachlichen Herkunft ihrer Namen offenzulegen. Informationen über die Gesundheit umfassen Informationen über die vergangene, gegenwärtige und zukünftige physische oder psychische Gesundheit eines Menschen und können sich auf eine kranke oder gesunde Person beziehen. Die Verarbeitung von Bildern von Personen mit einer dicken Brille, einem gebrochenen Bein, Verbrennungen

oder anderen sichtbaren Merkmalen, die sich auf die Gesundheit einer Person beziehen, kann nur dann als Verarbeitung sensibler Daten angesehen werden, wenn die Verarbeitung auf den Gesundheitsinformationen basiert, die aus den Bildern abgeleitet werden können.

Müssen sensible Daten für statistische Zwecke verarbeitet werden, so sollten sie so erhoben werden, dass der Betroffene nicht identifizierbar ist. Die Erhebung sensibler Daten ohne Identifikationsdaten ist eine Garantie im Sinne von Artikel 6. Besteht die berechtigte Notwendigkeit, sensible Daten für statistische Zwecke in identifizierbarer Form zu erheben (damit beispielsweise eine Wiederholungs- oder Längsschnitterhebung durchgeführt werden kann), so sollten geeignete Garantien vorgesehen werden.[12]

Zu Artikel 7 – Datensicherung

Der Verantwortliche und gegebenenfalls der Auftragsverarbeiter sollten für jede Verarbeitung spezifische Sicherheitsmaßnahmen technischer und organisatorischer Art ergreifen und dabei Folgendes berücksichtigen: die möglichen nachteiligen Folgen für den Menschen, das Wesen der personenbezogenen Daten, die Menge der verarbeiteten personenbezogenen Daten, den Grad der Anfälligkeit der zur Verarbeitung eingesetzten technischen Struktur, die Notwendigkeit einer Beschränkung des Zugangs zu den Daten, Anforderungen hinsichtlich einer langfristigen Aufbewahrung usw.

Die Sicherheitsmaßnahmen sollten den aktuellen Stand der Technik hinsichtlich Datensicherheitsmethoden und -techniken im Bereich der Datenverarbeitung berücksichtigen. Ihre Kosten sollten in einem angemessenen Verhältnis zur Schwere und Wahrscheinlichkeit der potentiellen Risiken stehen. Die Sicherheitsmaßnahmen sollten ständig überprüft und erforderlichenfalls aktualisiert werden.

Während die Sicherheitsmaßnahmen darauf abzielen, einer Reihe von Risiken vorzubeugen, enthält Absatz 2 eine besondere Verpflichtung für Fälle, in denen es dennoch zu einer Verletzung des Datenschutzes, die die Grundrechte und -freiheiten des Menschen ernsthaft beeinträchtigen könnte, gekommen ist. Beispielsweise könnte eine Offenlegung von Daten, die einem Berufsgeheimnis unterliegen, oder die finanzielle, rufschädigende oder körperliche Schäden oder Erniedrigung zur Folge haben könnte, als „ernsthafte“ Beeinträchtigung angesehen werden.

Wenn eine solche Verletzung des Datenschutzes stattgefunden hat, ist der Verantwortliche vorbehaltlich der nach Artikel 11 Absatz 1 zulässigen Ausnahme verpflichtet, die zuständigen Aufsichtsbehörden über den Vorfall zu unterrichten. Dies ist die Mindestanforderung. Der Verantwortliche sollte die Aufsichtsbehörden auch über alle Maßnahmen, die zur Beseitigung der Verletzung ergriffen und/oder vorgeschlagen wurden, sowie über deren mögliche Folgen unterrichten.

Die Benachrichtigung der Aufsichtsbehörden durch den Verantwortlichen schließt andere ergänzende Benachrichtigungen nicht aus. So kann der Verantwortliche auch die Notwendigkeit sehen, die Betroffenen zu benachrichtigen, insbesondere wenn die Verletzung des Datenschutzes wahrscheinlich zu einem erheblichen Risiko für die Rechte und Freiheiten von Menschen wie etwa Diskriminierung, Identitätsdiebstahl oder Betrug, finanziellem Verlust, Rufschädigung, Verlust der Vertraulichkeit von durch ein Berufsgeheimnis geschützten Daten oder einem anderen erheblichen wirtschaftlichen oder sozialen Nachteil führen wird, und ihnen angemessene und aussagekräftige Informationen insbesondere über die Kontaktstellen und mögliche Maßnahmen, die sie zur Abmilderung der nachteiligen Auswirkungen der Verletzung ergreifen könnten, zu geben. In Fällen, in denen der Verantwortliche die Betroffenen nicht von sich aus über die Verletzung des Datenschutzes informiert, sollte die Aufsichtsbehörde nach Abwägung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung die Möglichkeit haben, den Verantwortlichen dazu anzuhalten. Ebenso könnte eine Benachrichtigung anderer maßgeblicher Behörden wie etwa der für die Sicherheit von Computersystemen zuständigen Behörden wünschenswert sein.

Zu Artikel 8 – Transparenz der Verarbeitung

Der Verantwortliche muss bei der Datenverarbeitung transparent handeln, um eine Verarbeitung nach Treu und Glauben sicherzustellen und es Betroffenen zu ermöglichen, ihre Rechte im Zusammenhang mit der Datenverarbeitung zu verstehen und sie somit in vollem Umfang auszuüben.

Bestimmte wesentliche Informationen müssen den Betroffenen bei der unmittelbaren oder mittelbaren (nicht beim Betroffenen, sondern bei einem Dritten) Erhebung ihrer Daten vom Verantwortlichen zwingend in vorausschauender Weise zur Verfügung gestellt werden, vorbehaltlich der Möglichkeit, Ausnahmen gemäß Artikel 11 Absatz 1 vorzusehen. Informationen über den Namen und die Anschrift des

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

Verantwortlichen (oder der Mitverantwortlichen), die Rechtsgrundlage und die Zwecke der Datenverarbeitung, die Kategorien der verarbeiteten Daten und die Empfänger sowie die Mittel zur Ausübung der Rechte können in jedem geeigneten Format (entweder auf einer Website, mit technischen Hilfsmittel auf Privatgeräten usw.) zur Verfügung gestellt werden, sofern die Informationen dem Betroffenen nach Treu und Glauben und wirksam dargestellt werden. Die dargestellten Informationen sollten leicht zugänglich, lesbar, verständlich und an die jeweiligen Betroffenen angepasst sein (beispielsweise erforderlichenfalls in einer kinderfreundlichen Sprache). Ebenfalls vorzulegen sind alle zusätzlichen Informationen, die zur Gewährleistung einer Verarbeitung nach Treu und Glauben erforderlich oder für solche Zwecke nützlich sind, wie etwa die Aufbewahrungsdauer, die Kenntnis der der Datenverarbeitung zugrundeliegenden Überlegungen oder Informationen über Datenweitergaben an einen Empfänger in einer anderen Vertragspartei oder einer Nichtvertragspartei (einschließlich darüber, ob diese bestimmte Nichtvertragspartei ein angemessenes Datenschutzniveau bietet oder welche Maßnahmen der Verantwortliche getroffen hat, um ein solches angemessenes Datenschutzniveau zu gewährleisten).

Der Verantwortliche ist zur Bereitstellung dieser Informationen nicht verpflichtet, wenn der Betroffene sie bereits erhalten hat, im Falle einer mittelbaren Datenerhebung bei Dritten, wenn die Verarbeitung ausdrücklich gesetzlich vorgeschrieben ist, oder wenn sich dies als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert, weil der Betroffene nicht direkt identifizierbar ist oder der Verantwortliche keine Möglichkeit hat, den Betroffenen zu kontaktieren. Diese Unmöglichkeit kann sowohl rechtlicher (beispielsweise im Zusammenhang mit einem strafrechtlichen Ermittlungsverfahren) als auch praktischer (beispielsweise wenn ein Verantwortlicher nur Bilder verarbeitet und die Namen und Kontaktdaten der Betroffenen nicht kennt) Natur sein.

Der Verantwortliche kann alle verfügbaren, zumutbaren und erschwinglichen Mittel nutzen, um Betroffene kollektiv (über eine Website oder eine öffentliche Bekanntmachung) oder individuell zu informieren. Ist dies zu Beginn der Verarbeitung nicht möglich, kann es zu einem späteren Zeitpunkt erfolgen, beispielsweise wenn der Verantwortliche aus einem neuen Grund mit dem Betroffenen in Kontakt gebracht wird.

Zu Artikel 9 – Rechte des Betroffenen

Dieser Artikel listet jene Rechte auf, die jeder Mensch in Bezug auf die Verarbeitung der ihn betreffenden personenbezogenen Daten ausüben können sollte. Jede Vertragspartei stellt in ihrer Rechtsordnung sicher, dass jedem Betroffenen alle diese Rechte und die erforderlichen rechtlichen und praktischen, angemessenen und wirksamen Mittel zu ihrer Ausübung zur Verfügung stehen.

Diese Rechte umfassen die folgenden:

- das Recht jeder Person, nicht einer ausschließlich automatisierten Entscheidung unterworfen zu werden, die sie erheblich beeinträchtigt, ohne dass ihre Ansichten berücksichtigt werden (Buchstabe a);

- das Recht jeder Person, eine Bestätigung über eine Verarbeitung sie betreffender Daten zu verlangen und in angemessenen Abständen und ohne übermäßige Verzögerung oder Kosten Auskunft über die Daten zu erhalten (Buchstabe b);

- das Recht jeder Person, auf Antrag Auskunft über die Gründe für die Datenverarbeitung zu erhalten, wenn die Ergebnisse einer Verarbeitung auf sie angewendet werden (Buchstabe c);

- das Recht jeder Person, aus mit ihrer Situation zusammenhängenden Gründen Widerspruch gegen eine Verarbeitung sie betreffender personenbezogener Daten einzulegen, es sei denn, der Verantwortliche weist berechtigte Gründe für die Verarbeitung nach, die ihre Interessen oder Rechte und Grundfreiheiten überwiegen (Buchstabe d);

- das Recht jeder Person auf Berichtigung oder Löschung von unrichtigen, falschen oder unrechtmäßig verarbeiteten Daten (Buchstabe e);

- das Recht jeder Person auf ein Rechtsmittel, wenn eines der vorgenannten Rechte nicht geachtet wird (Buchstabe f);

- das Recht jeder Person, von einer Aufsichtsbehörde Unterstützung zu erhalten (Buchstabe g).

Diese Rechte müssen möglicherweise mit anderen Rechten und berechtigten Interessen in Einklang gebracht werden. Sie können gemäß Artikel 11 nur dann eingeschränkt werden, wenn dies gesetzlich vorgesehen ist und eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellt. Beispielsweise kann das Recht auf Löschung personenbezogener Daten insoweit eingeschränkt werden, als die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung aufgrund einer Rechtsvorschrift, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer Aufgabe im

öffentlichen Interesse oder in Ausübung öffentlichen Gewalt, die dem Verantwortlichen übertragenen wurde, erforderlich ist.

Wenngleich das Übereinkommen nicht festlegt, von wem ein Betroffener eine Bestätigung, Mitteilung, Berichtigung usw. erhalten kann oder gegenüber wem er Widerspruch einlegen oder seine Standpunkte äußern kann, wird dies in den meisten Fällen der Verantwortliche oder der Auftragsverarbeiter in dessen Auftrag sein. In Ausnahmefällen können die Mittel zur Ausübung der Rechte auf Auskunft, Berichtigung und Löschung die Vermittlung durch die Aufsichtsbehörde einschließen. In Bezug auf Gesundheitsdaten können die Rechte auch auf andere Weise als durch unmittelbare Auskunft ausgeübt werden. Sie können beispielsweise mit Unterstützung von medizinischem Fachpersonal ausgeübt werden, wenn dies im Interesse des Betroffenen liegt, insbesondere um ihm das Verständnis der Daten zu erleichtern oder sicherzustellen, dass der psychische Zustand des Betroffenen bei der Informationsvermittlung angemessen berücksichtigt wird – natürlich in Übereinstimmung mit deontologischen Grundsätzen.

Buchstabe a. Es ist von wesentlicher Bedeutung, dass ein Mensch, der einer ausschließlich automatisierten Entscheidung unterliegen kann, das Recht hat, eine solche Entscheidung anzufechten, indem er seinen Standpunkt und seine Argumente in sinnvoller Weise darlegt. Insbesondere sollte der Betroffene die Möglichkeit haben, vor ihrer Verwendung die mögliche Ungenauigkeit der personenbezogenen Daten, die Unerheblichkeit des auf seine besondere Situation anzuwendenden Profils oder andere Faktoren, die sich auf das Ergebnis der automatisierten Entscheidung auswirken, begründet darzulegen. Dies ist insbesondere dann der Fall, wenn Menschen durch die Anwendung algorithmischer Überlegungen, die zu einer Einschränkung oder Verweigerung einer Sozialleistung führen, oder bei einer Bewertung ihrer Kreditfähigkeit nur durch eine Software stigmatisiert werden. Dieses Recht kann ein Mensch jedoch nicht ausüben, wenn die automatisierte Entscheidung aufgrund eines Gesetz, dem der Verantwortliche unterliegt und das auch geeignete Maßnahmen zum Schutz der Rechte und Freiheiten und berechtigten Interessen der Betroffenen vorsieht, erlaubt ist.

Buchstabe b. Betroffene sollten das Recht haben, von der Verarbeitung ihrer personenbezogenen Daten Kenntnis zu erlangen. Das Auskunftsrecht sollte grundsätzlich kostenlos sein. Der Wortlaut von Buchstabe b soll es dem Verantwortlichen jedoch ermöglichen, unter bestimmten Bedingungen eine angemessene Gebühr einzuheben, wenn die Anträge exzessiv sind; außerdem soll er verschiedene Ansätze abdecken, die von einer Partei in geeigneten Fällen gewählt werden könnten. Eine solche Gebühr sollte ausnahmsweise und in jedem Fall angemessen sein und Betroffene nicht daran hindern oder davon abhalten, ihre Rechte auszuüben. Der Verantwortliche oder der Auftragsverarbeiter könnte sich auch weigern, auf offensichtlich unbegründete oder exzessive Anträge zu antworten, insbesondere im Fall von häufiger Wiederholung. Der Verantwortliche sollte eine solche Ablehnung in jedem Fall begründen. Um eine faire Ausübung des Auskunftsrechts zu gewährleisten, gilt die Mitteilung „in einer verständlichen Form“ sowohl für den Inhalt als auch für die Form einer standardisierten digitalen Mitteilung.

Buchstabe c. Betroffene sollten das Recht haben, über die der Datenverarbeitung zugrunde liegenden Überlegungen einschließlich der Folgen solcher Überlegungen, die zu daraus resultierenden Schlussfolgerungen geführt haben, Kenntnis zu erlangen, insbesondere bei der Verwendung von Algorithmen für die automatisierte Entscheidungsfindung einschließlich Profiling. Beispielsweise sollten sie im Falle einer Bonitätsprüfung das Recht haben, die der Verarbeitung ihrer Daten zugrunde liegende Logik, die zu einer „Ja“- oder „Nein“-Entscheidung führt, und nicht nur Informationen über die Entscheidung selbst zu kennen. Das Verständnis dieser Elemente trägt zur wirksamen Ausübung anderer wesentlicher Garantien wie etwa dem Widerspruchsrecht und dem Recht auf Beschwerde bei einer zuständigen Behörde bei.

Buchstabe d. Was das Widerspruchsrecht betrifft, so kann der Verantwortliche berechtigte Gründe für die Datenverarbeitung haben, die die Interessen oder Rechte und Grundfreiheiten des Betroffenen überwiegen. Beispielsweise könnten die Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen oder Gründe der öffentlichen Sicherheit als überwiegende berechtigte Gründe angesehen werden, die eine Fortsetzung der Verarbeitung rechtfertigen. Dies ist von Fall zu Fall nachzuweisen und das Versäumnis, solche zwingenden berechtigten Gründe während der Fortsetzung der Verarbeitung nachzuweisen, könnte als unrechtmäßig angesehen werden. Das Widerspruchsrecht funktioniert auf eine andere Weise und gesondert vom Recht auf Berichtigung oder Löschung (Buchstabe e).

Ein Widerspruch gegen die Datenverarbeitung zu Marketingzwecken sollte zur bedingungslosen Löschung oder Entfernung der vom Widerspruch erfassten personenbezogenen Daten führen.

Das Widerspruchsrecht kann durch Gesetz eingeschränkt werden, beispielsweise zum Zweck der Ermittlung oder Verfolgung von Straftaten. In diesem Fall kann der Betroffene gegebenenfalls die Rechtmäßigkeit der Verarbeitung, auf die sie sich stützt, bestreiten. Beruht eine Datenverarbeitung auf

einer gültigen Einwilligung des Betroffenen, so kann anstelle des Widerspruchsrechts das Recht auf Widerruf der Einwilligung ausgeübt werden. Ein Betroffener kann seine Einwilligung widerrufen und muss anschließend die sich möglicherweise aus anderen Rechtsvorschriften ergebenden Konsequenzen, wie beispielsweise eine Entschädigungspflicht gegenüber dem Verantwortlichen, tragen. Ebenso kann der Betroffene im Falle einer auf einem Vertrag beruhenden Datenverarbeitung die notwendigen Schritte zum Widerruf des Vertrags setzen.

Buchstabe e. Die Berichtigung oder Löschung muss, wenn sie gerechtfertigt ist, unentgeltlich erfolgen. Im Falle von Berichtigungen und Löschungen, die im Einklang mit dem in Buchstabe e dargelegten Grundsatz vorgenommen werden, sollten diese Berichtigungen und Löschungen den Empfängern der ursprünglichen Informationen nach Möglichkeit zur Kenntnis gebracht werden, sofern sich dies nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert.

Buchstabe g zielt darauf ab, einen wirksamen Schutz der Betroffenen sicherzustellen, indem ihnen das Recht auf Unterstützung durch eine Aufsichtsbehörde bei der Ausübung der im Übereinkommen vorgesehenen Rechte eingeräumt wird. Wenn der Betroffene im Hoheitsgebiet einer anderen Vertragspartei seinen Wohnsitz hat, kann er das Ersuchen über die von dieser Vertragspartei bezeichnete Behörde stellen. Das Unterstützungsersuchen sollte ausreichende Informationen enthalten, um die Identifizierung der betreffenden Datenverarbeitung zu ermöglichen. Dieses Recht kann nach Artikel 11 eingeschränkt oder im Interesse eines anhängigen Gerichtsverfahrens angepasst werden.

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

Zu Artikel 10 – Zusätzliche Verpflichtungen

Um die Wirksamkeit des Rechts auf Schutz personenbezogener Daten sicherzustellen, werden dem Verantwortlichen sowie gegebenenfalls dem/den Auftragsverarbeiter(n) zusätzliche Verpflichtungen auferlegt.

Gemäß Absatz 1 ist die Verpflichtung des Verantwortlichen zur Sicherstellung eines angemessenen Datenschutzes mit der Verantwortung verbunden, zu überprüfen und in der Lage zu sein, nachzuweisen, dass die Datenverarbeitung im Einklang mit dem anwendbaren Recht erfolgt. Die im Übereinkommen festgelegten Datenschutzgrundsätze, die in allen Phasen der Verarbeitung einschließlich der Planungsphase anzuwenden sind, zielen auf den Schutz der Betroffenen ab und sind gleichzeitig ein Mechanismus zur Stärkung ihres Vertrauens. Zu den geeigneten Maßnahmen, die der Verantwortliche und der Auftragsverarbeiter zur Sicherstellung der Einhaltung gegebenenfalls ergreifen müssen, zählen die Schulung der Mitarbeiter, die Einrichtung geeigneter Benachrichtigungsverfahren (beispielsweise um anzuzeigen, wann Daten aus dem System gelöscht werden müssen), die Festlegung konkreter vertraglicher Regelungen, wenn die Verarbeitung delegiert wird, um dem Übereinkommen Wirksamkeit zu verleihen, sowie die Einrichtung interner Verfahren, die die Überprüfung und den Nachweis der Einhaltung ermöglichen.

Entscheidet sich eine Vertragspartei im Einklang mit Artikel 11 Absatz 3 dafür, die Befugnisse einer Aufsichtsbehörde im Sinne des Artikels 15 in Bezug auf Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung zu beschränken, so ist der Verantwortliche nicht verpflichtet, gegenüber dieser Aufsichtsbehörde nachzuweisen, dass die Datenschutzanforderungen für Tätigkeiten, die in den Anwendungsbereich der oben genannten Ausnahme fallen, eingehalten werden.

Eine mögliche Maßnahme, die der Verantwortliche zur Erleichterung einer solchen Überprüfung und des Nachweises der Einhaltung ergreifen könnte, wäre die Benennung eines „Datenschutzbeauftragten“, der mit den zur Erfüllung seines Mandats erforderlichen Mitteln ausgestattet ist. Ein solcher Datenschutzbeauftragter, dessen Benennung der Aufsichtsbehörde angezeigt werden sollte, könnte im Verhältnis zum Verantwortlichen intern oder extern sein.

In Absatz 2 wird klargestellt, dass der Verantwortliche vor der Aufnahme einer Datenverarbeitungstätigkeit deren mögliche Auswirkungen auf die Rechte und Grundfreiheiten der Betroffenen prüfen muss. Diese Prüfung kann ohne übermäßige Formalitäten erfolgen. Sie wird auch die Einhaltung des Verhältnismäßigkeitsgrundsatzes auf der Grundlage einer umfassenden Gesamtbetrachtung der beabsichtigten Verarbeitung zu berücksichtigen haben. Unter bestimmten Umständen, wenn neben dem Verantwortlichen auch ein Auftragsverarbeiter beteiligt ist, muss auch der Auftragsverarbeiter die Risiken prüfen. Entwickler von IT-Systemen einschließlich Sicherheitsexperten oder Designer könnten zusammen mit Benutzern und Rechtsexperten die Prüfung der Risiken unterstützen.

Absatz 3 legt fest, dass zur besseren Gewährleistung eines wirksamen Schutzes die Verantwortlichen und gegebenenfalls die Auftragsverarbeiter dafür sorgen sollten, dass die Datenschutzanforderungen so früh

wie möglich, d.h. idealerweise in der Phase der Architektur und des Systementwurfs, durch technische und organisatorische Maßnahmen in die Datenverarbeitungsvorgänge integriert werden (Datenschutz durch Technikgestaltung). Diese Umsetzung von Datenschutzanforderungen sollte nicht nur in Bezug auf die für die Datenverarbeitung verwendete Technologie, sondern auch in Bezug auf die damit verbundenen Arbeits- und Verwaltungsverfahren erreicht werden. Es sollten einfach zu bedienende Funktionalitäten eingerichtet werden, die die Einhaltung des geltenden Rechts erleichtern. Beispielsweise sollte Betroffenen, soweit möglich und sachdienlich, ein sicherer Online-Zugang zu den eigenen Daten angeboten werden. Es sollte auch einfach zu bedienende Werkzeuge geben, die es Betroffenen ermöglichen, ihre Daten zu einem anderen Anbieter ihrer Wahl zu übertragen oder die Daten selbst zu behalten (Werkzeuge zur Datenübertragbarkeit). Bei der Festlegung der technischen Anforderungen für die Standardeinstellungen sollten Verantwortliche und Auftragsverarbeiter datenschutzfreundliche Voreinstellungen wählen, sodass die Nutzung von Anwendungen und Software die Rechte der Betroffenen nicht verletzt (Datenschutz durch datenschutzfreundliche Voreinstellungen), um insbesondere zu vermeiden, dass mehr Daten verarbeitet werden, als zur Erreichung des rechtmäßigen Zwecks erforderlich sind. Beispielsweise sollten soziale Netzwerke standardmäßig so konfiguriert werden, dass Beiträge oder Bilder nur mit eingeschränkten und ausgewählten Kreisen und nicht mit dem gesamten Internet geteilt werden.

Absatz 4 erlaubt es den Vertragsparteien, die in den Absätzen 1 bis 3 angeführten zusätzlichen Verpflichtungen unter Berücksichtigung der für die Interessen, Rechte und Grundfreiheiten der Betroffenen bestehenden Risiken anzupassen. Eine solche Anpassung sollte unter Berücksichtigung der Art und Menge der verarbeiteten Daten, der Art, des Umfangs und der Zwecke der Datenverarbeitung und in bestimmten Fällen der Größe der verarbeitenden Einrichtung vorgenommen werden. Die Verpflichtungen könnten beispielsweise so angepasst werden, dass kleinen und mittleren Unternehmen (KMU), die nur nicht-sensible personenbezogene Daten, die sie von Kunden im Rahmen ihrer Geschäftstätigkeit erhalten haben, verarbeiten und diese nicht für andere Zwecke wiederverwenden, keine übermäßigen Kosten entstehen. Bestimmte Kategorien von Datenverarbeitungen, wie beispielsweise eine Verarbeitung, die keine Risiken für die Betroffenen birgt, könnten sogar von einigen in diesem Artikel vorgesehenen zusätzlichen Verpflichtungen ausgenommen werden.

Zu Artikel 11 – Ausnahmen und Einschränkungen

Ausnahmen von den Bestimmungen des Kapitels II sind nicht zulässig, mit Ausnahme einiger weniger Bestimmungen (Artikel 5 Absatz 4, Artikel 7 Absatz 2, Artikel 8 Absatz 1 und Artikel 9), sofern eine solche Ausnahme gesetzlich vorgesehen ist, den Wesensgehalt der Grundrechte und -freiheiten wahrt und in einer demokratischen Gesellschaft aus den in Artikel 11 Absatz 1 Buchstaben a und b angeführten Gründen notwendig ist. Eine „in einer demokratischen Gesellschaft notwendige“ Maßnahme muss ein legitimes Ziel verfolgen und damit einem dringenden sozialen Bedürfnis entsprechen, das nicht mit weniger eingreifenden Mitteln erreicht werden kann. Eine solche Maßnahme muss außerdem in angemessenem Verhältnis zu dem verfolgten legitimen Ziel stehen und die von den nationalen Behörden vorgebrachten Rechtfertigungsgründe müssen sachgerecht und angemessen sein. Eine solche Maßnahme muss durch ein zugängliches und vorhersehbares, hinreichend detailliertes Gesetz vorgeschrieben sein.

Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach Treu und Glauben und in Bezug auf die Betroffenen transparent erfolgen und darf nur für bestimmte Zwecke erfolgen. Dies hindert die Strafverfolgungsbehörden für sich genommen nicht daran, Tätigkeiten wie verdeckte Ermittlungen oder Videoüberwachung vorzunehmn. Solche Tätigkeiten können zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten und der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die nationale und öffentliche Sicherheit, vorgenommen werden, sofern sie gesetzlich festgelegt sind und in einer demokratischen Gesellschaft unter gebührender Berücksichtigung der berechtigten Interessen der Betroffenen eine notwendige und verhältnismäßige Maßnahme darstellen.

Die Notwendigkeit solcher Ausnahmen muss von Fall zu Fall und im Lichte der wesentlichen Ziele des allgemeinen öffentlichen Interesses geprüft werden, wie in den Buchstaben a und b des ersten Absatzes ausgeführt wird. Buchstabe a listet einige Ziele des allgemeinen öffentlichen Interesses des Staates oder der internationalen Organisation auf, die Ausnahmen erfordern können.

Der Begriff „nationale Sicherheit“ sollte auf der Grundlage der einschlägigen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ausgelegt werden.[13]

13 Die einschlägige Rechtsprechung umfasst insbesondere den Schutz der Staatssicherheit und der verfassungsmäßigen Demokratie u.a. vor Spionage, Terrorismus, Terrorismusunterstützung und Separatismus. Wenn

Der Begriff „wichtige wirtschaftliche und finanzielle Interessen“ umfasst insbesondere die Anforderungen an die Steuereinhebung und die Devisenkontrolle. Der Begriff „Verhütung, Ermittlung und Verfolgung von Straftaten und die Strafvollstreckung“ in diesem Buchstaben schließt die Verfolgung von Straftaten und die Verhängung diesbezüglicher Sanktionen ein. Der Begriff „sonstige wichtige Ziele des allgemeinen öffentlichen Interesses“ umfasst unter anderem die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Verstößen gegen die Standesregeln bei reglementierten Berufen und die Durchsetzung zivilrechtlicher Ansprüche.

Buchstabe b betrifft die Rechte und Grundfreiheiten privater Parteien, wie etwa jene des oder der Betroffenen selbst (beispielsweise wenn lebenswichtige Interessen eines Betroffenen bedroht sind, weil er oder sie vermisst wird) oder Dritter, wie die Meinungsfreiheit einschließlich der Freiheit der journalistischen, wissenschaftlichen, künstlerischen oder literarischen Meinungsäußerung und das Recht, Informationen zu empfangen und weiterzugeben, das Brief- und Kommunikationsgeheimnis oder Geschäfts- oder Betriebsgeheimnisse und sonstige gesetzlich geschützte Geheimnisse. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichtenarchiven und Pressebibliotheken gelten. Um der Bedeutung der Meinungsfreiheit in jeder demokratischen Gesellschaft Rechnung zu tragen, ist es notwendig, Begriffe, die sich auf diese Freiheit beziehen, wie etwa Journalismus, weit auszulegen.

Der zweite Absatz lässt die Möglichkeit offen, die Bestimmungen der Artikel 8 und 9 in Bezug auf bestimmte Datenverarbeitungen zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken ohne erkennbare Risiken einer Verletzung der Rechte und Grundfreiheiten der Betroffenen einzuschränken. Dies könnte beispielsweise bei der Verwendung von Daten für statistische Arbeiten sowohl im öffentlichen als auch im privaten Bereich der Fall sein, sofern diese Daten in aggregierter Form veröffentlicht werden und angemessene Datenschutzgarantien bestehen (siehe Ziffer 50).

Die zusätzlichen Ausnahmen zu 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 lassen die geltenden Anforderungen in Bezug auf die Unabhängigkeit und Wirksamkeit von Überprüfungs- und Überwachungsmechanismen unberührt.[14]

Zu Artikel 12 – Sanktionen und Rechtsmittel

Damit das Übereinkommen ein wirksames Datenschutzniveau sicherstellen kann, sollten die Verpflichtungen des Verantwortlichen und des Auftragsverarbeiters sowie die Betroffenenrechte in den Rechtsordnungen der Vertragsparteien mit entsprechenden Sanktionen und Rechtsmitteln zum Ausdruck kommen.

Es bleibt jeder Vertragspartei überlassen, die Art (zivil-, verwaltungs-, strafrechtlich) dieser gerichtlichen und außergerichtlichen Sanktionen zu bestimmten. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Dasselbe gilt für Rechtsmittel: Betroffene müssen die Möglichkeit haben, eine Entscheidung oder Verhaltensweise gerichtlich zu bekämpfen, wobei die Festlegung der Modalitäten dafür den Vertragsparteien überlassen bleibt. Betroffenen müssen zudem außergerichtliche Rechtsmittel zur Verfügung gestellt werden. Ein finanzieller Ausgleich für materielle und immaterielle Schäden, die gegebenenfalls durch die Verarbeitung und kollektive Handlungen verursacht wurden, könnte ebenfalls in Betracht gezogen werden.

Zu Artikel 13 – Weitergehender Schutz

Dieser Artikel beruht auf einer ähnlichen Bestimmung, Artikel 53 der Europäischen Menschenrechtskonvention. Das Übereinkommen bestätigt die Grundsätze des Datenschutzrechts, zu deren Annahme alle Vertragsparteien bereit sind. Der Wortlaut unterstreicht, dass diese Grundsätze nur eine Grundlage darstellen, auf der die Vertragsparteien ein weitergehendes Schutzsystem aufbauen können. Der Ausdruck „größeres Maß an Schutz“ bezieht sich daher auf einen Schutzstandard, der höher, nicht niedriger ist als der bereits im Übereinkommen geforderte.

---

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).

14 Für Vertragsparteien, die Mitgliedstaaten des Europarats sind, wurden solche Voraussetzungen durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte nach Artikel 8 EMRK entwickelt (s. insb. EGMR, *Roman Zakharov v. Russland* (Beschwerde Nr. 47143/06), 4. Dezember 2015, Z 233; *Szabó und Vissy v. Ungarn* (Beschwerde Nr. 37138/14), 12. Januar 2016, Z 75 ff.).

Zu Kapitel III – Grenzüberschreitender Verkehr personenbezogener Daten[15]

Zu Artikel 14 – Grenzüberschreitender Verkehr personenbezogener Daten

Ziel dieses Artikels ist es, den (in der Präambel in Erinnerung gerufenen) freien Informationsfluss ungeachtet von Grenzen zu erleichtern und gleichzeitig einen angemessenen Schutz des Menschen bei der Verarbeitung personenbezogener Daten sicherzustellen. Eine grenzüberschreitende Datenweitergabe liegt vor, wenn personenbezogene Daten einem Empfänger, der der Hoheitsgewalt eines anderen Staates oder einer internationalen Organisation untersteht, offengelegt oder zugänglich gemacht werden.

Das Regelungsregime für grenzüberschreitenden Datenverkehr soll sicherstellen, dass personenbezogene Daten, die ursprünglich unter der Hoheitsgewalt einer Vertragspartei verarbeitet wurden (beispielsweise dort gesammelte oder gespeicherte Daten) und anschließend der Hoheitsgewalt eines Staates unterstehen, der nicht Vertragspartei des Übereinkommens ist, weiterhin unter geeigneten Garantien verarbeitet werden. Wichtig ist, dass Daten, die unter der Hoheitsgewalt einer Vertragspartei verarbeitet werden, stets durch die einschlägigen Datenschutzgrundsätze des Übereinkommens geschützt bleiben. Wenngleich es eine Vielfalt an Schutzsystemen gibt, muss der gewährte Schutz von einer solchen Qualität sein, dass die Menschenrechte nicht durch Globalisierung und den grenzüberschreitenden Datenverkehr beeinträchtigt werden.

Artikel 14 gilt nur für den Datenabfluss, nicht für den Datenzufluss, zumal letzterer durch das Datenschutzregime der empfangenden Vertragspartei abgedeckt ist.

Absatz 1 gilt für den Datenverkehr zwischen den Vertragsparteien des Übereinkommens. Der Datenverkehr kann nicht verboten oder einer besonderen Genehmigung „zum alleinigen Zweck des Schutzes personenbezogener Daten“ unterworfen werden. Das Übereinkommen beschränkt jedoch nicht die Freiheit einer Vertragspartei, die Weitergabe personenbezogener Daten an eine andere Vertragspartei zu anderen Zwecken einschließlich etwa der nationalen Sicherheit, der Landesverteidigung, der öffentliche Sicherheit oder anderen wichtigen öffentlichen Interessen (einschließlich des Schutzes von Staatsgeheimnissen) zu beschränken.

Der Grundgedanke der Bestimmung des Absatzes 1 besteht darin, dass von allen Vertragsparteien, die sich dem gemeinsamen Kern der Datenschutzbestimmungen des Übereinkommens angeschlossen haben, erwartet wird, dass sie ein Schutzniveau bieten, das als angemessen angesehen wird und daher im Prinzip den freien Datenverkehr ermöglicht. Es könnte jedoch Ausnahmefälle geben, in denen ein reales und ernsthaftes Risiko besteht, dass dieser freie Verkehr personenbezogener Daten zur Umgehung der Bestimmungen des Übereinkommens führt. Als Ausnahmeregelung muss diese Bestimmung restriktiv ausgelegt werden und die Vertragsparteien können sich in Fällen, in denen das Risiko entweder hypothetisch oder geringfügig ist, nicht auf sie berufen. Eine Vertragspartei kann sich daher in einem bestimmten Fall nur dann auf die Ausnahme berufen, wenn ihr klare und zuverlässige Beweise dafür vorliegen, dass die Weitergabe der Daten an eine andere Vertragspartei den nach dem Übereinkommen bestehenden Schutz dieser Daten mit hoher Wahrscheinlichkeit erheblich untergraben könnte. Dies könnte beispielsweise der Fall sein, wenn bestimmte im Rahmen des Übereinkommens gewährte Schutzmechanismen von der anderen Vertragspartei nicht mehr gewährleistet werden (beispielsweise, weil ihre Aufsichtsbehörde nicht mehr in der Lage ist, ihre Befugnisse wirksam auszuüben) oder wenn die an eine andere Vertragspartei weitergegebenen Daten wahrscheinlich neuerlich weitergegeben werden (Weiterübermittlung), ohne dass ein angemessenes Schutzniveau sichergestellt ist. Eine weitere völkerrechtlich anerkannte Ausnahme besteht, wenn Vertragsparteien an harmonisierte Schutzvorschriften von Staaten gebunden sind, die regionalen (wirtschaftlichen) Organisationen, die ein höheres Integrationsniveau anstreben, angehören.

Dies gilt unter anderem für die Mitgliedstaaten der EU. Wie jedoch in der Datenschutz-Grundverordnung (EU) 2016/679 ausdrücklich festgehalten ist, sind der Beitritt eines Drittlandes zum Übereinkommen Nr. 108 und dessen Umsetzung wichtige Faktoren bei der Anwendung des EU-Regimes für internationale Datenübermittlungen, insbesondere bei der Beurteilung, ob das Drittland ein angemessenes Schutzniveau bietet (was wiederum den freien Verkehr personenbezogener Daten ermöglicht).

Absatz 2 sieht die Verpflichtung vor, grundsätzlich zu gewährleisten, 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

15 Mit dem Inkrafttreten des Änderungsprotokolls gilt das Zusatzprotokoll bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181) als ein integraler Bestandteil des Übereinkommens in seiner geltenden Fassung.

angemessenes Schutzniveau besteht, unter anderem wenn dies aufgrund „überwiegender berechtigter Interessen, insbesondere wichtiger öffentlicher Interessen“, gerechtfertigt ist, soweit diese gesetzlich vorgesehen sind und solche Weitergaben in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen (Buchstabe c). Personenbezogene Daten können daher aus ähnlichen Gründen wie den in Artikel 11 Absätze 1 und 3 angeführten weitergegeben werden. In allen Fällen steht es den Vertragsparteien nach dem Übereinkommen frei, Datenweitergaben an Nichtvertragsparteien zu beschränken, sei es zum Zwecke des Datenschutzes oder aus anderen Gründen.

Absatz 2 bezieht sich auf den grenzüberschreitenden Verkehr personenbezogener Daten mit einem Empfänger, der nicht der Hoheitsgewalt einer Vertragspartei untersteht. Wie bei allen personenbezogenen Daten, die außerhalb der nationalen Grenzen fließen, ist ein angemessenes Schutzniveau sicherzustellen. In Fällen, in denen der Empfänger nicht Vertragspartei des Übereinkommens ist, sieht das Übereinkommen zwei Mechanismen vor, um sicherzustellen, dass das Datenschutzniveau tatsächlich angemessen ist; entweder durch Gesetz oder durch ad-hoc- oder genehmigte standardisierte Garantien, die rechtsverbindlich und durchsetzbar sind und ordnungsgemäß umgesetzt werden.

Die Absätze 2 und 3 gelten für alle Formen des angemessenen Schutzes, ganz gleich, ob dieser durch Gesetz oder standardisierte Garantien gewährt wird. Das Gesetz muss die maßgeblichen Elemente des Datenschutzes, wie sie in diesem Übereinkommen dargelegt sind, enthalten. Das Schutzniveau sollte für jede Weitergabe oder Kategorie von Weitergaben bewertet werden. Verschiedene Elemente der Übermittlung sollten geprüft werden, wie etwa die Art der Daten, die Zwecke und Dauer der Verarbeitung, für die die Daten weitergegeben werden, die Einhaltung der Rechtsstaatlichkeit durch das Zielland, die im betreffenden Staat oder in der betreffenden Organisation geltenden allgemeinen und bereichsspezifischen Rechtsvorschriften, und die dort geltenden Standes- und Sicherheitsvorschriften.

Ad-hoc-Garantien oder standardisierten Garantien müssen die maßgeblichen Datenschutzelemente enthalten. Darüber hinaus könnten die Vertragsbedingungen beispielsweise vorsehen, dass dem Betroffenen eine Kontaktperson aus dem Personal der für die Datenweitergabe verantwortlichen Person bereitgestellt wird, deren Aufgabe es ist, die Einhaltung der materiellen Schutzstandards sicherzustellen. Es stünde dem Betroffenen frei, diese Person jederzeit und kostenlos im Zusammenhang mit der Datenverarbeitung oder den Datenweitergaben zu kontaktieren und gegebenenfalls Unterstützung bei der Ausübung seiner Rechte zu erhalten.

Bei der Beurteilung der Angemessenheit des Schutzniveaus müssen die Grundsätze des Übereinkommens, das Ausmaß, in dem sie im Empfängerstaat oder in der Empfängerorganisation – soweit sie für den konkreten Fall der Weitergabe erheblich sind – erfüllt werden und wie der Betroffene seine Interessen im Falle der Nichteinhaltung verteidigen kann berücksichtigt werden. Bei der Beurteilung sollten die Durchsetzbarkeit der Betroffenenrechte und die Bereitstellung wirksamer administrativer und gerichtlicher Rechtsbehelfe für die Betroffenen, deren personenbezogene Daten weitergegeben werden, berücksichtigt werden. In ähnlicher Weise kann die Bewertung für einen ganzen Staat oder eine Organisation vorgenommen werden, wodurch alle Datenweitergaben an einen solchen Bestimmungsort zulässig werden.

Absatz 4 ermöglicht den Vertragsparteien eine Abweichung vom Grundsatz, ein angemessenes Schutzniveau zu verlangen, und erlaubt eine Weitergabe an einen Empfänger, der einen solchen Schutz nicht gewährleistet. Solche Ausnahmen sind nur in eingeschränkten Situationen zulässig: mit Einwilligung oder aufgrund eines spezifischen Interessen des Betroffenen und/oder wenn es überwiegende, gesetzlich vorgesehene berechtigte Interessen gibt und/oder wenn die Weitergabe im Hinblick auf die Meinungsfreiheit eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellt. Solche Ausnahmen sollten die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit beachten.

Absatz 5 sieht eine ergänzende Garantie vor: nämlich, dass der zuständigen Aufsichtsbehörde alle sachdienlichen Informationen über die in Absatz 3 b sowie auf Antrag über die in den Absätzen 4 b und 4 c genannten Datenweitergaben zur Verfügung gestellt werden. Die Behörde sollte ermächtigt sein, sachdienliche Informationen über die Umstände und Begründung dieser Weitergabe zu verlangen. Unter den in Artikel 11 Absatz 3 festgelegten Bedingungen sind Ausnahmen von Artikel 14 Absatz 5 zulässig.

Gemäß Absatz 6 sollte die Aufsichtsbehörde ermächtigt sein, einen Nachweis für die Wirksamkeit der getroffenen Maßnahmen oder das Bestehen überwiegender berechtigter Interessen zu verlangen und die Weitergabe zu untersagen, auszusetzen oder an Bedingungen zu knüpfen, wenn sich dies zum Schutz der Rechte und Grundfreiheiten der Betroffenen als notwendig erweist. Unter den in Artikel 11 Absatz 3 festgelegten Bedingungen sind Ausnahmen von Artikel 14 Absatz 6 zulässig.

Die ständig zunehmenden Datenströme und die damit einhergehende Notwendigkeit eines verstärkten Schutzes personenbezogener Daten erfordern auch eine verstärkte internationale Zusammenarbeit der zuständigen Aufsichtsbehörden bei der Durchsetzung.

Zu Kapitel IV – Aufsichtsbehörden[16]

Zu Artikel 15 – Aufsichtsbehörden

Dieser Artikel soll den wirksamen Schutz von Menschen sicherstellen, indem die Vertragsparteien verpflichtet werden, eine oder mehrere unabhängige und unparteiliche öffentliche Aufsichtsbehörden zu schaffen, die zum Schutz der Rechte und Freiheiten der Menschen bei der Verarbeitung ihrer personenbezogenen Daten beitragen. Bei diesen Behörden kann es sich um einen einzelnen Beauftragten oder ein Kollegialorgan handeln. Um ein geeignetes Rechtsmittel bieten können, müssen die Datenschutzaufsichtsbehörden über wirksame Befugnisse und Funktionen verfügen und bei der Erfüllung ihrer Aufgaben echte Unabhängigkeit genießen. Sie sind ein wesentlicher Bestandteil des Datenschutzaufsichtssystems in einer demokratischen Gesellschaft. Soweit Artikel 11 Absatz 3 Anwendung findet, können die Vertragsparteien andere geeignete Mechanismen für eine unabhängige und wirksame Überprüfung und Überwachung der Verarbeitungstätigkeiten zum Zweck der nationalen Sicherheit und der Landesverteidigung vorsehen.

Absatz 1 stellt klar, dass mehr als eine Behörde erforderlich sein könnte, um den besonderen Umständen verschiedener Rechtssysteme (z. B. Bundesstaaten) gerecht zu werden. Es können auch spezialisierte Aufsichtsbehörden eingerichtet werden, deren Tätigkeit auf einen bestimmten Bereich (Bereich der elektronischen Kommunikation, Gesundheitswesen, öffentlicher Bereich usw.) beschränkt ist. Dies gilt auch für die Verarbeitung personenbezogener Daten für journalistische Zwecke, wenn dies notwendig ist, um das Recht auf Schutz personenbezogener Daten mit der Meinungsfreiheit in Einklang zu bringen. Die Aufsichtsbehörden sollten über die notwendige Infrastruktur und die notwendigen finanziellen, technischen und personellen Mittel (Juristen, IT-Spezialisten) verfügen, um rasch und wirksam handeln zu können. Die Angemessenheit der Mittel sollte ständig überprüft werden. Artikel 11 Absatz 3 erlaubt Ausnahmen von den Befugnissen der Aufsichtsbehörden in Bezug auf die Verarbeitung von Daten für Zwecke der nationalen Sicherheit und der Landesverteidigung (wenn solche Ausnahmen vorliegen, so können andere Absätze dieses Artikels infolgedessen unanwendbar oder nicht maßgeblich sein). Dies gilt jedoch unbeschadet der geltenden Anforderungen in Bezug auf die Unabhängigkeit und Wirksamkeit der Überprüfungs- und Aufsichtsmechanismen.[17]

Die Vertragsparteien verfügen bei der Einrichtung der Behörden im Hinblick auf ihre Fähigkeit zur Wahrnehmung ihrer Aufgaben über einen gewissen Ermessensspielraum. Nach Absatz 2 müssen sie jedoch, vorbehaltlich der Möglichkeit, Ausnahmen gemäß Artikel 11 Absatz 3 vorzusehen, zumindest Untersuchungs- und Einwirkungsbefugnisse sowie die Befugnis, Entscheidungen im Hinblick auf Verstöße gegen die Bestimmungen des Übereinkommens zu treffen, haben. Letzteres kann die Verhängung von verwaltungsstrafrechtlichen Sanktionen einschließlich Geldstrafen beinhalten. Sieht die Rechtsordnung einer Vertragspartei keine verwaltungsstrafrechtlichen Sanktionen vor, so kann Absatz 2 so angewendet werden, dass die Sanktion von der zuständigen Aufsichtsbehörde vorgeschlagen und von den zuständigen nationalen Gerichten verhängt wird. In jedem Fall müssen die verhängten Sanktionen wirksam, verhältnismäßig und abschreckend sein.

Die Behörde wird vorbehaltlich der Möglichkeit, Ausnahmen gemäß Artikel 11 Absatz 3 vorzusehen, mit Untersuchungsbefugnissen wie etwa der Möglichkeit, vom Verantwortlichen und vom Auftragsverarbeiter Informationen über die Verarbeitung personenbezogener Daten zu verlangen und zu erhalten, ausgestattet. Gemäß Artikel 15 sind diese Informationen insbesondere dann zur Verfügung zu stellen, wenn sich ein Betroffener, der die in Artikel 9 vorgesehenen Rechte ausüben möchte, an die Aufsichtsbehörde wendet. Letzteres unterliegt den Ausnahmen des Artikels 11 Absatz 1.

Die in Absatz 1 vorgesehene Einwirkungsbefugnis der Aufsichtsbehörde kann im Recht der Vertragsparteien unterschiedliche Formen annehmen. So könnte die Behörde beispielsweise von sich aus oder wenn der Betroffene diese Rechte nicht persönlich ausüben kann befugt sein, den Verantwortlichen zu verpflichten, unrichtige oder unrechtmäßig verarbeitete Daten zu berichtigen, zu löschen oder zu vernichten. Eine Befugnis, gegen Verantwortliche vorzugehen, die nicht bereit sind, die erforderlichen Informationen innerhalb einer angemessenen Frist zu übermitteln, wäre ebenfalls ein äußerst wirksamer

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

17 Siehe Fußnote 14.

Ausdruck der Einwirkungsbefugnis. Diese Befugnis könnte auch die Möglichkeit einschließen, vor der Aufnahme von Datenverarbeitungsvorgängen Stellungnahmen abzugeben (wenn die Verarbeitung besondere Risiken für die Rechte und Grundfreiheiten darstellt, sollte die Aufsichtsbehörde von den Verantwortlichen bereits im frühesten Stadium der Verfahrensgestaltung konsultiert werden) oder gegebenenfalls Fälle an die jeweils zuständigen Behörden zu verweisen.

Darüber hinaus sollte nach Absatz 4 jeder Betroffene die Möglichkeit haben, von der Aufsichtsbehörde die Prüfung einer Forderung hinsichtlich seiner Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu verlangen. Dies trägt dazu bei, das Recht auf ein geeignetes Rechtsmittel im Einklang mit den Artikeln 9 und 12 zu gewährleisten. Die zur Erfüllung dieser Pflicht notwendigen Mittel sollten bereitgestellt werden. Die Aufsichtsbehörden sollten die Möglichkeit erhalten, im Rahmen der ihnen zur Verfügung stehenden Mittel Prioritäten hinsichtlich der Behandlung der Anträge und Beschwerden der Betroffenen zu setzen.

Die Vertragsparteien sollten vorbehaltlich der Möglichkeit, Ausnahmen nach Artikel 11 Absatz 3 vorzusehen, der Aufsichtsbehörde die Befugnis geben, entweder ein Gerichtsverfahren einzuleiten oder Verletzungen der Datenschutzbestimmungen den Justizbehörden zur Kenntnis zu bringen. Diese Befugnis ergibt sich aus der Befugnis zur Durchführung von Untersuchungen, die die Behörde zur Aufdeckung einer Verletzung eines individuellen Schutzrechts führen könnte. Die Vertragsparteien können der Verpflichtung, der Behörde diese Befugnis zu erteilen, nachkommen, indem sie ihr ermöglichen, Entscheidungen zu treffen.

Entfaltet eine Verwaltungsentscheidung rechtliche Wirkungen, so hat jeder Betroffene das Recht auf ein wirksames Rechtsmittel im Einklang mit dem anwendbaren nationalen Recht.

Absatz 2 e befasst sich mit der bewusstseinsfördernden Rolle der Aufsichtsbehörden. In diesem Zusammenhang erscheint es besonders wichtig, dass die Aufsichtsbehörde proaktiv für die Sichtbarkeit ihrer Aktivitäten, Funktionen und Befugnisse sorgt. Dazu muss die Aufsichtsbehörde die Öffentlichkeit durch regelmäßige Berichte informieren (siehe Ziffer 131). Sie kann auch Stellungnahmen veröffentlichen, allgemeine Empfehlungen zur richtigen Umsetzung der Datenschutzvorschriften aussprechen oder andere Kommunikationsmittel nutzen. Außerdem muss sie die Menschen sowie die Verantwortlichen und Auftragsverarbeiter über ihre Rechte und Pflichten in Bezug auf den Datenschutz informieren. Bei der Bewusstseinsförderung für Datenschutzfragen müssen die Behörden darauf achten, dass sie sich speziell an Kinder und schutzbedürftige Personengruppen in angepasster Form und Sprache wenden.

Nach Absatz 3 sind die Aufsichtsbehörden im Einklang mit dem geltenden nationalen Recht ermächtigt, Stellungnahmen zu allen Gesetzgebungs- und Vollziehungsmaßnahmen, die die Verarbeitung personenbezogener Daten vorsehen, zu erstatten. Nur allgemeine Maßnahmen sollen von dieser beratenden Befugnis erfasst werden, nicht individuelle Maßnahmen.

Zusätzlich zu dieser in Absatz 3 vorgesehenen Beratung könnte die Behörde auch um Stellungnahme ersucht werden, wenn andere Maßnahmen betreffend die Verarbeitung personenbezogener Daten wie beispielsweise Verhaltensregeln oder technische Normen vorbereitet werden.

Artikel 15 steht der Übertragung sonstiger Befugnisse an die Aufsichtsbehörden nicht entgegen.

Absatz 5 stellt klar, dass die Aufsichtsbehörden individuelle Rechte und Freiheiten nur dann wirksam schützen können, wenn sie ihre Aufgaben in völliger Unabhängigkeit wahrnehmen. Eine Reihe von Elementen trägt dazu bei, die Unabhängigkeit der Aufsichtsbehörde bei der Wahrnehmung ihrer Aufgaben sicherzustellen, unter anderem die Zusammensetzung der Behörde, die Vorgehensweise bei der Ernennung ihrer Mitglieder, die Dauer der Ausübung und die Bedingungen für die Beendigung ihrer Aufgaben, die Möglichkeit für sie, ohne ungebührliche Einschränkungen an den maßgeblichen Sitzungen teilzunehmen, die Möglichkeit, technische oder sonstige Experten hinzuzuziehen oder externe Beratungen abzuhalten, die Verfügbarkeit ausreichender Mittel für die Behörde, die Möglichkeit, eigenes Personal einzustellen oder die Annahme von Entscheidungen ohne unmittelbare oder mittelbare Einflussnahme von außen.

Das Verbot, Weisungen einzuholen oder anzunehmen, gilt für die Wahrnehmung der Pflichten als Aufsichtsbehörde. Es hindert die Aufsichtsbehörden nicht daran, fachlichen Rat einzuholen, wenn dies für notwendig erachtet wird, solange die Aufsichtsbehörden ihr eigenes unabhängiges Urteilsvermögen einsetzen.

Nach Absatz 7 ist in Bezug auf die Arbeit und die Tätigkeiten der Aufsichtsbehörden Transparenz erforderlich, beispielsweise durch die Veröffentlichung eines jährlichen Tätigkeitsberichts, der unter anderem Informationen über ihre Durchsetzungsmaßnahmen enthält.

Ungeachtet dieser Unabhängigkeit muss es im Einklang mit dem Rechtsstaatlichkeitsprinzip nach Absatz 9 möglich sein, gegen die Entscheidungen der Aufsichtsbehörden einen gerichtlichen Rechtsbehelf einzulegen.

Während Aufsichtsbehörden zwar die rechtliche Fähigkeit haben sollten, vor Gericht zu handeln und die Durchsetzung zu erwirken, sollte das Einschreiten (oder Nichteinschreiten) einer Aufsichtsbehörde einen Betroffenen nicht daran hindern, ein gerichtliches Rechtsmittel einzulegen (siehe Ziffer 124).

Artikel 15 Absatz 10 sieht vor, dass Aufsichtsbehörden nicht für die Verarbeitung durch unabhängige Organe im Rahmen ihrer gerichtlichen Tätigkeit zuständig sind. Diese Ausnahme von den Aufsichtsbefugnissen sollte im Einklang mit dem nationalen Recht streng auf reine gerichtliche Tätigkeiten beschränkt sein.

In Österreich wird die Funktion der Aufsichtsbehörde von der Datenschutzbehörde (§§ 18 bis 23 und 31 bis 35 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999) wahrgenommen.

Zu Kapitel V – Zusammenarbeit und gegenseitige Hilfeleistung

Zu Artikel 16 – Benennung von Aufsichtsbehörden

Kapitel V (Artikel 16 bis 21) enthält eine Reihe von Bestimmungen über die Zusammenarbeit und gegenseitige Hilfeleistung zwischen den Vertragsparteien durch ihre verschiedenen Behörden, um den Datenschutzbestimmungen nach dem Übereinkommen Wirksamkeit zu verleihen. Diese Bestimmungen sind außer in den in Artikel 20 genannten Fällen verpflichtend. Nach Artikel 16 benennt jede Vertragspartei eine oder mehrere Behörden und teilt dem Generalsekretär des Europarats ihre Kontaktdaten sowie gegebenenfalls ihre sachlichen und territorialen Zuständigkeiten mit. Die nachfolgenden Artikel schaffen einen detaillierten Rahmen für die Zusammenarbeit und gegenseitige Hilfeleistung.

Wenngleich die Zusammenarbeit zwischen den Vertragsparteien im Allgemeinen durch die nach Artikel 15 eingerichteten Aufsichtsbehörden erfolgen wird, kann nicht ausgeschlossen werden, dass eine Vertragspartei eine andere Behörde benennt, um den Bestimmungen des Artikels 16 Wirksamkeit zu verleihen.

Die Zusammenarbeit und allgemeine Hilfeleistung ist sowohl für Vorabkontrollen als auch für nachträgliche Kontrollen (beispielsweise zur Überprüfung der Tätigkeit eines bestimmten Datenverantwortlichen) relevant. Die ausgetauschten Informationen können rechtlicher oder sachlicher Natur sein.

Als Aufsichtsbehörde gemäß Artikel 16 soll für Österreich die Datenschutzbehörde benannt werden.

Zu Artikel 17 – Formen der Zusammenarbeit

Nach Artikel 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. Da Artikel 17 die Zusammenarbeit der Aufsichtsbehörden auf jenes Maß beschränkt, das „für die Erfüllung ihrer Aufgaben und Wahrnehmung ihrer Befugnisse“ notwendig ist und die Fähigkeit einer Aufsichtsbehörde zur Zusammenarbeit vom Umfang ihrer Befugnisse abhängt, findet die Bestimmung keine Anwendung, soweit eine Vertragspartei von Artikel 11 Absatz 3 Gebrauch macht, was 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 der Datenschutzgesetze durch gegenseitige Hilfsleistung, wobei die Rechtmäßigkeit des Handelns jeder Aufsichtsbehörde unerlässlich ist, bis hin zu einigen „weichen“ Formen wie Bewusstseinsförderung, Schulungen und Personalaustausch.

Die Aufzählung der möglichen Kooperationsmaßnahmen ist nicht abschließend. In erster Linie leisten die Aufsichtsbehörden einander gegenseitige Hilfe, insbesondere durch den Austausch sachdienlicher und nützlicher Informationen. Diese Informationen könnten zweierlei Art sein: „Informationen und Unterlagen über ihr Recht und ihre Verwaltungspraxis im Zusammenhang mit dem Datenschutz“ (was normalerweise keine Probleme bereitet, solche Informationen könnten frei ausgetauscht und öffentlich zugänglich gemacht werden) sowie vertrauliche Informationen einschließlich personenbezogener Daten.

Was personenbezogene Daten betrifft, so können diese nur ausgetauscht werden, wenn sie für die Zusammenarbeit von entscheidender Bedeutung sind, d.h. wenn ohne ihre Bereitstellung die Zusammenarbeit wirkungslos wäre, oder wenn der „Betroffene ausdrücklich, für den konkreten Fall, freiwillig und in informierter Weise in ihre Bereitstellung eingewilligt“ hat. In jedem Fall muss die

Weitergabe personenbezogener Daten im Einklang mit den Bestimmungen des Übereinkommens, insbesondere mit Kapitel II, erfolgen (siehe auch Artikel 20, der die Ablehnungsgründe regelt).

Neben der Bereitstellung sachdienlicher und nützlicher Informationen können die Ziele der Zusammenarbeit auch durch abgestimmte Untersuchungen oder Einwirkungen sowie durch gemeinsame Maßnahmen erreicht werden. Hinsichtlich der anwendbaren Verfahren sollen die Aufsichtsbehörden nach Prüfung ihrer Handlungsfähigkeit zur Aufnahme einer solchen Zusammenarbeit die anwendbaren innerstaatlichen Rechtsvorschriften wie Verwaltungs-, Zivil- oder Strafprozessordnungen oder supranationale oder völkerrechtliche Verpflichtungen, an die ihre Rechtsordnungen gebunden sind, beispielsweise Rechtshilfeabkommen, heranziehen.

Absatz 3 bezieht sich auf ein Netzwerk von Aufsichtsbehörden als Mittel, um zur Rationalisierung des Zusammenarbeitsverfahrens und damit zur Effizienz des Schutzes personenbezogener Daten beizutragen. Es ist wichtig zu beachten, dass das Übereinkommen in der Einzahl auf „ein Netzwerk“ Bezug nimmt. Dies hindert die Aufsichtsbehörden der Vertragsparteien nicht daran, sich an anderen einschlägigen Netzwerken zu beteiligen.

Zu Artikel 18 – Unterstützung von Betroffenen

Absatz 1 stellt sicher, dass Betroffene, sei es in einer Vertragspartei des Übereinkommens oder in einem Drittland, in der Lage sind, ihre in Artikel 9 anerkannten Rechte ungeachtet ihres Wohnorts oder ihrer Staatsangehörigkeit auszuüben.

Nach Absatz 2 wird Betroffenen, die im Hoheitsgebiet einer anderen Vertragspartei wohnen, die Möglichkeit eingeräumt, ihre Rechte entweder unmittelbar in jenem Land, in dem Informationen über den Betroffenen verarbeitet werden, oder mittelbar durch die Vermittlung der benannten Behörde zu verfolgen.

Darüber hinaus können Betroffene mit Wohnsitz im Ausland auch die Möglichkeit haben, ihre Rechte mit Unterstützung durch diplomatische oder konsularische Bedienstete ihres eigenen Landes auszuüben.

Absatz 3 sieht vor, dass Anträge so konkret wie möglich sein müssen, um das Verfahren zu beschleunigen.

Zu Artikel 19 – Garantien

Dieser Artikel stellt sicher, dass die Aufsichtsbehörden gegenüber Datenschutzaufsichtsbehörden anderer Vertragsparteien und im Ausland ansässigen Betroffenen an dieselbe Verpflichtung zur Wahrung der Diskretion und Vertraulichkeit gebunden sind.

Die Hilfeleistung durch eine Aufsichtsbehörde im Namen eines Betroffenen darf nur über Antrag dieses Betroffenen erfolgen. Die Behörde muss vom Betroffenen bevollmächtigt worden sein und darf nicht eigenständig in seinem oder ihrem Namen handeln. Diese Bestimmung ist von grundlegender Bedeutung für das gegenseitige Vertrauen, auf das die gegenseitige Hilfeleistung gründet.

Zu Artikel 20 – Ablehnung von Ersuchen

Dieser Artikel bestimmt, dass die Vertragsparteien verpflichtet sind, Ersuchen um Zusammenarbeit und gegenseitige Hilfeleistung nachzukommen. Die Gründe für die Ablehnung von Ersuchen sind abschließend angeführt.

Der Begriff „Erfüllung“, der in Buchstabe c verwendet wird, ist in einem breiteren Sinn zu verstehen und umfasst nicht nur die Antwort auf das Ersuchen, sondern auch die der Antwort vorausgehende Handlung. So kann eine ersuchte Behörde ein Tätigwerden beispielsweise nicht nur dann ablehnen, wenn die Übermittlung der erbetenen Informationen an die ersuchende Behörde die Rechte und Grundfreiheiten eines Menschen verletzen könnte, sondern auch dann, wenn bereits die Tatsache, dass die Informationen eingeholt werden, seine Rechte und Grundfreiheiten beeinträchtigen könnte. Darüber hinaus kann eine ersuchte Behörde nach dem anwendbaren nationalen Recht verpflichtet sein, den Schutz anderer Interessen der öffentlichen Ordnung sicherzustellen (z. B. Gewährleistung der Vertraulichkeit eines polizeilichen Ermittlungsverfahrens). Zu diesem Zweck kann eine Aufsichtsbehörde verpflichtet sein, bei ihrer Beantwortung eines Ersuchens auf bestimmte 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 Durchführung zu belasten, sieht Absatz 3 dieses Artikels vor, dass Verfahren, Formen und zu verwendende Sprache zwischen den betroffenen Vertragsparteien vereinbart werden können. Der Wortlaut dieses Absatzes verlangt kein förmliches Verfahren, sondern erlaubt Verwaltungsvereinbarungen, die sogar auf bestimmte Fälle beschränkt sein können. Außerdem ist es ratsam, dass die Vertragsparteien den zuständigen

Aufsichtsbehörden die Befugnis zum Abschluss solcher Vereinbarungen überlassen. Auch die Formen der Zusammenarbeit und Hilfeleistung können von Fall zu Fall variieren. Es liegt auf der Hand, dass für die Übermittlung eines Ersuchens um Zugang zu sensiblen medizinischen Informationen andere Anforderungen gelten werden wird als für routinemäßige Anfragen zu Einträgen in einem Einwohnerverzeichnis.

Zu Kapitel VI – Übereinkommensausschuss

Der Zweck der Artikel 22, 23 und 24 besteht darin, die wirksame Anwendung des Übereinkommens zu erleichtern und es erforderlichenfalls zu optimieren. Der Übereinkommensausschuss stellt ein weiteres Mittel der Zusammenarbeit der Vertragsparteien dar, um den auf Grundlage des Übereinkommens erlassenen Datenschutzgesetzen Wirksamkeit zu verleihen.

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

Das Wesen des Übereinkommensausschusses und das voraussichtlich angewendete Verfahren könnten ähnlich sein wie die in anderen im Rahmen des Europarates geschlossenen Übereinkommen vorgesehenen.

Da das Übereinkommen ein sich ständig weiterentwickelndes Thema behandelt, ist zu erwarten, dass sich Fragen sowohl hinsichtlich der praktischen Anwendung des Übereinkommens (Artikel 23 Buchstabe a) als auch hinsichtlich seiner Bedeutung (gleicher Artikel Buchstabe d) stellen werden.

Die Geschäftsordnung des Übereinkommensausschusses enthält Bestimmungen über das Stimmrecht der Vertragsparteien und die Modalitäten der Ausübung dieses Rechts und ist dem Änderungsprotokoll als Anhang beigefügt.

Jede Änderung der Geschäftsordnung bedarf einer Zweidrittelmehrheit, mit Ausnahme von Änderungen der Bestimmungen über das Stimmrecht und die entsprechenden Modalitäten, für die Artikel 25 des Übereinkommens gilt.

Bei ihrem Beitritt hat die EU eine Erklärung abzugeben, in der die Verteilung der Zuständigkeiten zwischen der EU und ihren Mitgliedstaaten hinsichtlich des Schutzes personenbezogener Daten nach dem Übereinkommen klargestellt wird. Anschließend wird die EU den Generalsekretär über jede wesentliche Änderung der Zuständigkeitsverteilung unterrichten.

Gemäß Artikel 25 kann der Übereinkommensausschuss Änderungen des Übereinkommens vorschlagen und andere von einer Vertragspartei oder dem Ministerkomitee unterbreitete Änderungsvorschläge prüfen (Artikel 23 Buchstaben b und c).

Um die Umsetzung der im Übereinkommen festgelegten Datenschutzgrundsätze zu gewährleisten, hat der Übereinkommensausschuss eine Schlüsselrolle bei der Bewertung der Einhaltung des Übereinkommens, entweder bei der Vorbereitung einer Bewertung des von einem Beitrittskandidaten gebotenen Datenschutzniveaus (Artikel 23 Buchstabe e) oder bei der regelmäßigen Überprüfung der Durchführung des Übereinkommens durch die Vertragsparteien (Artikel 23 Buchstabe h). Der Übereinkommensausschuss kann auch bewerten, ob das Datenschutzsystems eines Staates oder einer internationalen Organisation mit dem Übereinkommen im Einklang steht, wenn der Staat oder die Organisation dies vom Ausschuss verlangt (Artikel 23 Buchstabe f).

Bei der Erstattung solcher Gutachten über den Grad der Einhaltung des Übereinkommens arbeitet der Übereinkommensausschuss auf der Grundlage eines fairen, transparenten und öffentlichen Verfahrens, das in seiner Geschäftsordnung detailliert geregelt ist.

Darüber hinaus kann der Übereinkommensausschuss Modelle für standardisierte Garantien für Datenweitergaben genehmigen (Artikel 23 Buchstabe g).

Schließlich kann der Übereinkommensausschuss zur Lösung von zwischen den Vertragsparteien auftretenden Schwierigkeiten beitragen (Artikel 23 Buchstabe i). Bei Streitigkeiten bemüht sich der Übereinkommensausschuss um eine Lösung im Wege von Verhandlungen oder sonstiger gütlicher Mittel.

Zu Kapitel VII – Änderungen

Zu Artikel 25 – Änderungen

Das Ministerkomitee, das den ursprünglichen Wortlaut dieses Übereinkommens angenommen hat, ist auch für die Genehmigung von Änderungen zuständig.

Nach Absatz 1 kann die Initiative für Änderungen vom Ministerkomitee selbst, vom Übereinkommensausschuss oder von einer Vertragspartei (gleich, ob sie Mitgliedstaat des Europarats ist oder nicht) ergriffen werden.

Jeder Änderungsvorschlag, der nicht vom Übereinkommensausschuss stammt, sollte diesem gemäß Absatz 3 zur Stellungnahme vorgelegt werden.

Grundsätzlich tritt jede Änderung am dreißigsten Tag nachdem alle Vertragsparteien dem Generalsekretär des Europarats ihre Annahme dieser Änderung angezeigt haben in Kraft. Das Ministerkomitee kann jedoch unter bestimmten Umständen nach Anhörung des Übereinkommensausschusses einstimmig beschließen, dass solche Änderungen nach Ablauf eines Zeitabschnitts von drei Jahren in Kraft treten, es sei denn, dass eine Vertragspartei dem Generalsekretär einen Einwand notifiziert. Dieses Verfahren, das die Beschleunigung des Inkrafttretens von Änderungen unter Wahrung des Grundsatzes der Zustimmung aller Vertragsparteien bezweckt, soll für geringfügige und technische Änderungen gelten.

Zu Kapitel VIII – Schlussklauseln

Zu Artikel 26 – Inkrafttreten

Da ein weiter geographischer Geltungsbereich für die Wirksamkeit des Übereinkommens als wesentlich angesehen wird, legt Absatz 2 die Anzahl der für das Inkrafttreten erforderlichen Ratifikationen durch Mitgliedstaaten des Europarates auf fünf fest.

Das Übereinkommen liegt zur Unterzeichnung durch die Europäische Union auf.[18]

Zu Artikel 27 – Beitritt von Nichtmitgliedstaaten oder internationalen Organisationen

Das ursprünglich in enger Zusammenarbeit mit der OECD und einigen nichteuropäischen Staaten entwickelte Übereinkommen steht weltweit jedem Staat offen, der seine Bestimmungen einhält. Der Übereinkommensausschuss hat die Aufgabe, diese Einhaltung zu bewerten und eine Stellungnahme für das Ministerkomitee hinsichtlich des Datenschutzniveaus des Beitrittskandidaten vorzubereiten.

In Anbetracht der Grenzenlosigkeit des Datenverkehrs wird der Beitritt von Ländern und internationalen Organisationen auf der ganzen Welt angestrebt. Dem Übereinkommen können ausschließlich solche internationalen Organisationen beitreten, die als dem Völkerrecht unterliegende Organisationen definiert sind.

Zu Artikel 28 – Räumlicher Anwendungsbereich

Die Anwendung des Übereinkommens auf entlegene Gebiete, die der Hoheitsgewalt der Vertragsparteien unterstehen oder in deren Namen eine Vertragspartei Verpflichtungen eingehen kann, ist im Hinblick auf die Heranziehung ferner Länder für Datenverarbeitungstätigkeiten aus Kosten- oder Personalgründen oder im Hinblick auf die Nutzung wechselnder Datenverarbeitungskapazitäten bei Tag und Nacht von praktischer Bedeutung.

Zu Artikel 29 – Vorbehalte

Die in diesem Übereinkommen enthaltenen Vorschriften stellen die grundlegendsten und wesentlichsten Elemente für einen wirksamen Datenschutz dar. Aus diesem Grund lässt das Übereinkommen keine Vorbehalte zu seinen Bestimmungen, die überdies unter Berücksichtigung der nach bestimmten Artikeln zulässigen Ausnahmen und Beschränkungen angemessen flexibel sind, zu.

Zu Artikel 30 – Kündigung

Jede Vertragspartei kann das Übereinkommen jederzeit kündigen.

Zu Artikel 31 – Notifikationen

Diese Bestimmungen entsprechen den üblichen Schlussklauseln in anderen Übereinkommen des Europarates.

Zu den Schlussbestimmungen des Protokolls

Zu Artikel 36 des Protokolls – Unterzeichnung, Ratifikation und Beitritt

Ein Beitritt zum Übereinkommen ist künftig nur bei gleichzeitigem Beitritt zum Protokoll möglich.

Zu Artikel 37 des Protokolls – Inkrafttreten

Das Protokoll tritt drei Monate nach Ratifikation durch sämtliche Vertragsparteien des Übereinkommens in Kraft. Sollte dies nicht binnen fünf Jahren erfolgen, tritt es, soweit es von zumindest 38 Vertragsparteien ratifiziert wurde, in Bezug auf diese Vertragsparteien in Kraft.

---

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

Mit Inkrafttreten des Protokolls wird das – von Österreich ratifizierte (vgl. BGBl. III Nr. 91/2008) – Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (SEV Nr. 181) aufgehoben.

Zu Artikel 38 des Protokolls – Erklärungen

Mit Inkrafttreten des Protokolls wird jede Erklärung einer Vertragspartei nach Artikel 3 des Übereinkommens unwirksam. In diesem Zusammenhang ist auf die von Österreich abgegebene Erklärung gemäß Artikel 3 Absatz 2 Buchstabe b des Übereinkommens, wonach Österreich das Übereinkommen auch auf Informationen über juristische Personen oder Personengemeinschaften im Sinne des § 3 Z 2 des Datenschutzgesetzes 1978 anwendet (s. BGBl. III Nr. 137/1988), hinzuweisen.

Zu den Artikeln 39 und 40 des Protokolls – Vorbehalte und Notifikationen

Die Regelungen über Vorbehalte und Notifikationen entsprechen den diesbezüglichen Regelungen des Übereinkommens (Artikel 29 und 31).

Zum Anhang des Protokolls – Elemente der Geschäftsordnung des Übereinkommensausschusses

Die einen Anhang zum Protokoll bildende Geschäftsordnung des Übereinkommensausschusses regelt die Abstimmungsmodalitäten dieses Gremiums (vgl. Artikel 24 Absatz 3).

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-04-07T13:37:54+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	