BERICHT UND ANTRAG

DER REGIERUNG

AN DEN

LANDTAG DES FÜRSTENTUMS LIECHTENSTEIN

BETREFFEND

DIE RATIFIKATION DES PROTOKOLLS VOM 10. OKTOBER 2018 ZUR ÄNDERUNG DES ÜBEREINKOMMENS ZUM SCHUTZ DES MENSCHEN BEI DER AUTOMATISCHEN VERARBEITUNG PERSONENBEZOGENER DATEN

Behandlung im Landtag	
	Datum
Schlussabstimmung	

Nr. 1/2023

INHALTSVERZEICHNIS

Beilagen:

- Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übersetzung in Deutsch vom 5. November 2019)
- Erläuternder Bericht zum Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Strassburg, 10.X.1985; Sammlung der Europaratsverträge Nr. 223)
- Geltungsbereich des Protokolls zur Änderung des Übereinkommens
- Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

ZUSAMMENFASSUNG

Die gegenständliche Vorlage modernisiert das Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108, im Folgenden „Übereinkommen"; LGBl. 2004 Nr. 167). Dieses Übereinkommen wurde von Liechtenstein im Jahr 2004 ratifiziert, ebenso wie sein Zusatzprotokoll im Jahr 2010 (LGBl. 2010 Nr. 035). Bereits im Jahr 2011 nahm der Europarat jedoch die Arbeiten für die Revision des Übereinkommens auf, da die technologischen Entwicklungen und die Zunahme des grenzüberschreitenden Datenverkehrs zahlreiche neue Herausforderungen für den Schutz der Privatsphäre und der Grundrechte der Betroffenen mit sich brachten. Ziel der Revision war eine entsprechende inhaltliche Überarbeitung der Bestimmungen des Übereinkommens sowie seine Zusammenführung mit dem Zusatzprotokoll in einem einzigen Dokument („Konvention 108+"). Am 10. Oktober 2018 wurde schliesslich vom Ministerkomitee des Europarates das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (im Folgenden „Änderungsprotokoll") verabschiedet. Bislang wurde das Änderungsprotokoll von 44 Staaten unterzeichnet und von 20 Staaten auch ratifiziert. Liechtenstein unterzeichnete das Änderungsprotokoll am 7. Dezember 2020.

Gemäss dem Änderungsprotokoll werden die Pflichten des Verantwortlichen für eine Verarbeitung personenbezogener Daten ausgeweitet. So ist dieser etwa verpflichtet, der zuständigen datenschutzrechtlichen Aufsichtsbehörde („Aufsichtsbehörde")[1] bestimmte Datenschutzverletzungen zu melden. Ebenfalls ausgeweitet wird seine Pflicht, die Betroffenen über die Datenverarbeitung und ihre Rechte zu informieren. Ausserdem ist im Änderungsprotokoll die Pflicht des Verantwortlichen vorgesehen, im Vorfeld bestimmter Datenverarbeitungen eine Datenschutz-Folgenabschätzung vorzunehmen und die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen anzuwenden. Im Weiteren ist im Änderungsprotokoll ein Ausbau der Rechte der Betroffenen vorgesehen, insbesondere in Bezug auf ihr Auskunftsrecht und bei einer automatisierten Einzelentscheidung.

[1] In Liechtenstein übernimmt diese Funktion die Datenschutzstelle des Fürstentums Liechtenstein.

Die Vertragsstaaten sind ferner verpflichtet, ein Sanktionssystem und ein Rechtsmittelsystem einzurichten und den Aufsichtsbehörden die Befugnis einzuräumen, verbindliche, anfechtbare Entscheidungen zu erlassen. Des Weiteren soll die Zusammenarbeit zwischen den Aufsichtsbehörden gestärkt werden.

Schliesslich ist im Änderungsprotokoll ein Überprüfungsverfahren vorgesehen, mit dem das zuständige Organ des Europarates die Wirksamkeit der Massnahmen bewerten kann, die ein Vertragsstaat ergriffen hat, um die Bestimmungen des Übereinkommens umzusetzen.

Das überarbeitete Übereinkommen entspricht – in etwas weniger detaillierter Form – weitgehend den Datenschutzgrundsätzen der in Liechtenstein direkt anwendbaren Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden „DSGVO") und der Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden „DSRL-PJ"). Liechtenstein hat die DSGVO im Rahmen des EWR bereits am 20. Juli 2018 und die DSRL-PJ zur Wahrung des Schengen-Besitzstandes bereits am 13. Dezember 2016 übernommen. Im Zuge dessen wurde mit dem liechtensteinischen Datenschutzgesetz vom 4. Oktober 2018 (LGBl. 2018 Nr. 272) eine entsprechende Datenschutzgesetzgebung erlassen, welche auch die Bestimmungen der DSRL-PJ im nationalen Recht umsetzt. Somit sind in Liechtenstein zur Ratifikation des Änderungsprotokolls keine weiteren gesetzlichen Anpassungen mehr erforderlich. Auf die jeweiligen nationalen Verweise im Bericht und Antrag wird daher grundsätzlich verzichtet.

Liechtenstein kann mit der Ratifikation des Änderungsprotokolls einen Beitrag bei der weiteren Etablierung eines internationalen rechtlichen Rahmenwerks zum Datenschutz und zur Datenverarbeitung leisten. So können dem Übereinkommen nicht nur die Mitgliedstaaten des Europarats beitreten, sondern auch Nichtmitgliedsstaaten und internationale Organisationen. Gleichzeitig kann durch die

Ratifikation für die liechtensteinische Wirtschaft der grenzüberschreitende Datentransfer in Vertragsstaaten des Übereinkommens, die nicht zugleich Mitglied des EWR sind, deutlich erleichtert werden. Denn durch ihren Beitritt zum Übereinkommen bieten auch solche Staaten relevante Garantien für eine sichere Übermittlung personenbezogener Daten. Dies wiederum stärkt letztlich auch den Schutz für die liechtensteinischen Bürgerinnen und Bürger, wenn ihre personenbezogenen Daten grenzüberschreitend verarbeitet werden.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Äusseres, Bildung und Sport

BETROFFENE STELLEN

Datenschutzstelle
Amt für Auswärtige Angelegenheiten

Vaduz, 24. Januar 2023

LNR 2023-33

P

Sehr geehrter Herr Landtagspräsident,
Sehr geehrte Frauen und Herren Abgeordnete

Die Regierung gestattet sich, dem Hohen Landtag nachstehenden Bericht und Antrag betreffend die Ratifizierung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten an den Landtag zu unterbreiten.

I. BERICHT DER REGIERUNG

1. AUSGANGSLAGE

Am 28. Januar 1981 hat der Europarat das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Referenznummer 108, im Folgenden „Übereinkommen“) verabschiedet, das von Liechtenstein 2004 ratifiziert wurde (LGBl. 2004 Nr. 167). Dieses Übereinkommen wurde mit dem Zusatzprotokoll vom 8. November 2001 zum Übereinkommen bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (Referenznummer 181, im Folgenden „Zusatzprotokoll“) ergänzt, das Liechtenstein 2010 ratifiziert hat (LGBl. 2010 Nr. 035). Im Jahr 2011 nahm der Europarat die Arbeiten für die Revision des Übereinkommens auf, um der technologischen Entwicklung und den mit der Digitalisierung verbundenen Herausforderungen zu begegnen.

Der Beratende Ausschuss des Übereinkommens (im Folgenden „Beratender Ausschuss“) hat am 30. November 2012 einen Entwurf zur Modernisierung des Übereinkommens verabschiedet und diesen dem Ministerkomitee des Europarates (im Folgenden „Ministerkomitee“) zur Genehmigung vorgelegt. Das Ministerkomitee hat einen Ad-hoc-Ausschuss Datenschutz (im Folgenden „CAHDATA“) zur Prüfung des Entwurfs eingesetzt. Die Arbeiten des CAHDATA wurden im Juni 2016 mit der Verabschiedung des „Entwurfs zur Modernisierung des Übereinkommens vom Juni 2016“ abgeschlossen. Am 18. Mai 2018 führten die Revisionsarbeiten schliesslich zur Verabschiedung des Änderungsprotokolls zum Übereinkommen (Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Referenznummer 223, im Folgenden „Änderungsprotokoll“).

Die Auflegung zur Unterzeichnung des Änderungsprotokolls erfolgte am 10. Oktober 2018. Liechtenstein hat das Abkommen am 7. Dezember 2020 unterzeichnet. Bislang wurde das Änderungsprotokoll von 39 Mitgliedstaaten des Europarates (inkl. Liechtenstein) unterzeichnet, wovon 18 dieses ebenfalls bereits ratifizierten. Zu diesen zählen etwa Deutschland sowie Österreich, welche das Änderungsprotokoll im Oktober 2021 respektive im Juli 2022 ratifiziert haben. Auch Italien vollzog die Ratifikation bereits im Juli 2021. Die Schweiz hat das Abkommen im November 2019 unterzeichnet, aber bisher noch nicht ratifiziert. Des Weiteren wurde das Änderungsprotokoll von fünf der neun Nichtmitgliedstaaten des Europarates, die dem Übereinkommen beigetreten sind, unterzeichnet und von zweien ratifiziert.[2] Weitere Ratifizierungen könnten in verhältnismässig naher Zukunft erfolgen, denn am 9. April 2019 hat die Europäische Union (EU) die Mitgliedstaaten

[2] Stand vom 11. Januar 2023. Gesamthaft wurde das Änderungsprotokoll von 20 Staaten ratifiziert. Die fünf Nichtmitgliedstaaten des Europarats, welche das Übereinkommen unterzeichnet haben, sind Argentinien, Mauritius, Russland (seit dem 16. März 2022 suspendiert), Tunesien und Uruguay, wobei Mauritius und Uruguay ebenfalls bereits ratifizierten.

ausdrücklich ermächtigt, das Änderungsprotokoll in ihrem Interesse zu ratifizieren.

2. BEGRÜNDUNG DER VORLAGE

Wie das Übereinkommen und sein Zusatzprotokoll soll auch das mit dem Änderungsprotokoll überarbeitete Übereinkommen zu einem universellen rechtlichen Instrument für den Datenschutz werden. Bereits das bisherige Übereinkommen liegt zur Ratifizierung durch Staaten auf, die nicht Mitglied des Europarates sind. Von dieser Möglichkeit sowie vom Status als Beobachter wird bereits heute rege Gebrauch gemacht, was die internationale Bedeutung des Übereinkommens als rechtlicher Standard für Datenschutz unterstreicht. Das Interesse von aussereuropäischen Staaten an einer Ratifizierung – auch des überarbeiteten Übereinkommens – wird voraussichtlich noch weiter zunehmen, da es nicht zuletzt beim grenzüberschreitenden Datentransfer zwischen EU/EWR und Drittstaaten eine wichtige Rolle spielen kann (z.B. wenn es darum geht, einen Angemessenheitsbeschluss der Europäischen Kommission gemäss Art. 45 der Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG[3] (Datenschutz-Grundverordnung, im Folgenden „DSGVO“) zu erlangen).

Mit der Ratifizierung des Änderungsprotokolls setzt sich Liechtenstein massgeblich für die Etablierung eines internationalen rechtlichen Rahmenwerks zur Datenverarbeitung und für den Datenschutz ein. Damit wird das Datenschutzniveau auf internationaler Ebene weiter vereinheitlicht und erhöht und der grenzüberschreitende Datentransfer von und nach Drittstaaten insbesondere für die Wirtschaft erleichtert, da Drittstaaten durch den Beitritt zum Übereinkommen den

[3] ABI. Nr. L 119 vom 4. Mai 2016 S. 1.

EU/EWR-Mitgliedstaaten relevante Garantien für eine sichere Übermittlung der Daten bieten können. Dies wiederum stärkt auch den Schutz für die liechtensteinischen Bürgerinnen und Bürger, wenn ihre personenbezogenen Daten grenzüberschreitend verarbeitet werden.

3. SCHWERPUNKTE DER VORLAGE

Mit dem Änderungsprotokoll wird das Übereinkommen einerseits inhaltlich modernisiert, um den neuen Herausforderungen an den Schutz der Privatsphäre zu begegnen, die mit der Nutzung von Informations- und Kommunikationstechnologien und dem stetig anwachsenden Strom personenbezogener Daten einhergehen. Andererseits wird das Regelwerk auch strukturell vereinfacht, indem die Bestimmungen des Zusatzprotokolls direkt ins Übereinkommen aufgenommen werden.

Grundsätzlich entspricht das Änderungsprotokoll den Datenschutzgrundsätzen, die im Rahmen der DSGVO und der Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[4] (im Folgenden „DSRL-PJ“) vorgesehen sind. Das Änderungsprotokoll ist jedoch weniger detailliert. Es gilt für alle Verarbeitungen von personenbezogenen Daten natürlicher Personen, die der Gerichtsbarkeit der Vertragsparteien unterstehen, sowohl im öffentlichen als auch im privaten Sektor. Vom Geltungsbereich ausgeschlossen sind nur Datenverarbeitungen, die zur Ausübung rein persönlicher oder familiärer Tätigkeiten vorgenommen werden.

---

[4] ABI. Nr. L119 vom 4. Mai 2016 S. 89.

Im Vergleich zum ursprünglichen Übereinkommen erweitert das Änderungsprotokoll die Pflichten des Verantwortlichen für eine Datenverarbeitung. So ist dieser etwa verpflichtet, der zuständigen Aufsichtsbehörde bestimmte Datenschutzverletzungen zu melden (Art. 9 des Änderungsprotokolls). Seine Pflicht, den Betroffenen über die Datenverarbeitung und seine Rechte zu informieren, wird ebenfalls ausgeweitet, insbesondere in Bezug auf Art und Umfang der mitzuteilenden Informationen (Art. 10 des Änderungsprotokolls). Ausserdem ist im Änderungsprotokoll die Pflicht des Verantwortlichen vorgesehen, im Vorfeld bestimmter Datenverarbeitungen eine Datenschutz-Folgenabschätzung vorzunehmen. Er soll darüber hinaus die Datenschutzgrundsätze „Datenschutz durch Technik“ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ anwenden (Art. 12 des Änderungsprotokolls).

Das Änderungsprotokoll sieht auch einen Ausbau der Rechte der Betroffenen im Vergleich zum ursprünglichen Übereinkommen vor, insbesondere in Bezug auf ihr Auskunftsrecht und im Fall einer automatisierten Einzelentscheidung (Art. 11 des Änderungsprotokolls). In Liechtenstein werden diese Rechte bereits über die DSGVO und das Datenschutzgesetz (LGBl 2018.272; DSG) gewährleistet.

Die Vertragsparteien sind ferner verpflichtet, ein Sanktionssystem und ein Rechtsmittelsystem einzurichten (Art. 15 des Änderungsprotokolls) und den Aufsichtsbehörden die Befugnis einzuräumen, verbindliche, anfechtbare Entscheidungen zu erlassen (Art. 19 des Änderungsprotokolls). In Liechtenstein wird dies ebenfalls bereits über die DSGVO und das DSG gewährleistet.

Da die Bestimmungen des Übereinkommens nicht direkt anwendbar sind, verpflichtet das Änderungsprotokoll jede Vertragspartei, in ihrem innerstaatlichen Recht die notwendigen Massnahmen zu ergreifen, um den Bestimmungen dieses Erlasses Wirkung zu verleihen. Diese Massnahmen müssen spätestens bei der Ratifizierung des Übereinkommens in Kraft treten (Art. 6 des Änderungsprotokolls).

Die Vertragsparteien können keine Vorbehalte zu den Bestimmungen des Änderungsprotokolls anbringen. Hingegen wurden die Ausnahmen und Einschränkungsmöglichkeiten zu den Bestimmungen des überarbeiteten Übereinkommens deutlich erweitert (Art. 14 des Änderungsprotokolls). Die bereits abgegebenen Erklärungen der Vertragsparteien zum Übereinkommen erlöschen mit Inkrafttreten des Änderungsprotokolls (Art. 38 des Änderungsprotokolls).

Weiter ist ein Überprüfungsverfahren vorgesehen, mit dem das zuständige Organ des Europarates die Wirksamkeit der Massnahmen bewerten kann, die eine Vertragspartei ergriffen hat, um die Bestimmungen des Übereinkommens umzusetzen (Art. 6 und 29 des Änderungsprotokolls).

Das überarbeitete Übereinkommen entspricht den Datenschutzgrundsätzen der DSGVO und der DSRL-PJ weitgehend bzw. die DSGVO und die DSRL-PJ sind noch detaillierter ausgestaltet und gehen in einigen Bereichen weiter als das überarbeitete Übereinkommen. Liechtenstein hat die direkt anwendbare DSGVO im Rahmen des EWR bereits am 20. Juli 2018 und die DSRL-PJ zur Wahrung des Schengen-Besitzstandes bereits am 13. Dezember 2016 übernommen. Die Bestimmungen der DSRL-PJ wurden in der Folge mittels der neuen Datenschutzgesetzgebung im nationalen Recht umgesetzt. Somit sind in Liechtenstein zur Ratifikation des Änderungsprotokolls keine weiteren gesetzlichen Anpassungen mehr erforderlich.

4. VERNEHMLASSUNG

Die Bestimmungen des Änderungsprotokolls sind aufgrund der in Liechtenstein geltenden DSGVO und des liechtensteinischen DSG bereits gesetzlich implementiert. Zur Ratifikation sind in Liechtenstein daher keine weiteren spezifischen Gesetzesanpassungen mehr erforderlich. Aus diesen Gründen wurde auf eine Vernehmlassung verzichtet.

5. ERLÄUTERUNGEN ZU DEN EINZELNEN BESTIMMUNGEN

Der Europarat gilt bis heute als wichtiger internationaler Wegbereiter eines wirksamen Datenschutzrechts. Dies nicht zuletzt deshalb, weil sein Übereinkommen aus dem Jahr 1981 als Grundlage und Referenzwerk für zahlreiche nationale und internationale Erlasse wie auch für die DSGVO diente. Umgekehrt wird die Modernisierung des Übereinkommens durch parallele Reformen und Neuerungen anderer internationaler Datenschutzinstrumente geprägt. So wurde gemäss dem Erläuternden Bericht zum Änderungsprotokoll etwa grösste Sorgfalt darauf verwendet, Kohärenz und Widerspruchsfreiheit zwischen den entsprechenden Rechtsrahmen von EU/EWR und dem Europarat sicherzustellen.[5]

Im Ergebnis sind die Grundsätze der Verarbeitung personenbezogener Daten in der DSGVO und der DSRL-PJ wie auch im überarbeiteten Übereinkommen weitgehend deckungsgleich, und auch die einzelnen Bestimmungen der Regelwerke sind sehr ähnlich. Allerdings sind die Betroffenenrechte in der DSGVO und DSRL-PJ deutlich detaillierter gefasst und eine betroffene Person geniesst somit auch weiterhin innerhalb des EU/EWR-Raums unter der in Liechtenstein geltenden DSGVO sowie dem liechtensteinischen DSG mehr und umfassendere Rechte als unter dem überarbeiteten Übereinkommen (z.B. das Recht auf Vergessenwerden oder das Recht auf Datenübertragbarkeit). Auch die Pflichten für Verantwortliche und Auftragsverarbeiter gehen in der DSGVO und DSRL-PJ bzw. im liechtensteinischen DSG weiter.[6]

Durch das Änderungsprotokoll kommen somit für Betroffene und Verantwortliche in Liechtenstein keine weiteren neuen Rechte oder Pflichten hinzu.

---

[5] Vgl. Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal, Strasbourg, 10.X.2018, Rz. 3.

[6] Art. 13 des überarbeiteten Übereinkommens (Art. 11 bisheriges Übereinkommen) sieht explizit die Möglichkeit vor, „dass eine Vertragspartei den Betroffenen ein grösseres Mass an Schutz als das in diesem Übereinkommen vorgeschriebene gewährt".

5.1 Präambel

Zu Art. 1 Änderungsprotokoll (Änderung der Präambel)

In der Präambel wird festgehalten, dass eines der Hauptziele des überarbeiteten Übereinkommens darin besteht, die Kontrolle über personenbezogene Daten zu verstärken. Die persönliche Entscheidungsfreiheit wird dabei betont. Dies ist das Recht jedes Einzelnen, selbst über seine personenbezogenen Daten und deren Verarbeitung zu bestimmen. Ausserdem verweist die Präambel darauf, dass das Recht auf den Schutz personenbezogener Daten in Bezug auf dessen gesellschaftliche Rolle zu betrachten ist. Dieser Schutz ist mit anderen Menschenrechten und Grundfreiheiten, einschliesslich der freien Meinungsäusserung, in Einklang zu bringen. Das Recht auf den Schutz personenbezogener Daten sollte in der Regel auch kein Hindernis für den Zugang der Bürgerinnen und Bürger zu amtlichen Dokumenten darstellen.

Die Präambel betont, dass die Weitergabe von Daten für die Gesellschaft von grosser Bedeutung ist. Das überarbeitete Übereinkommen legt einen Rahmen fest, dank dem Betroffene ihre Rechte wahrnehmen können, ohne dass Innovationen, der soziale und wirtschaftliche Fortschritt oder der Schutz der öffentlichen Sicherheit beeinträchtigt werden.

Schliesslich wird in der Präambel die Bedeutung der internationalen Zusammenarbeit zwischen den Aufsichtsbehörden der Vertragsparteien des überarbeiteten Übereinkommens anerkannt.

5.2 Allgemeine Bestimmungen

Zu Art. 2 Änderungsprotokoll (Änderung von Art. 1 des Übereinkommens; Gegenstand und Zweck)

Art. 2 des Änderungsprotokolls ändert Art. 1 des Übereinkommens dahingehend, dass in Art. 1 des überarbeiteten Übereinkommens klarer definiert wird, was der

Zweck des Übereinkommens ist: Es ist dies der Schutz jeder natürlichen Person sowie die Gewährleistung ihrer Rechte und Freiheiten in Hinblick auf die Verarbeitung ihrer personenbezogenen Daten.

Zu Art. 3 Änderungsprotokoll (Änderung von Art. 2 des Übereinkommens; Begriffsbestimmungen)

Art. 3 des Änderungsprotokolls hebt die Begriffe „automatisierte Datei“ und „automatisierte Verarbeitung“ auf. Stattdessen definiert er den Begriff „Datenverarbeitung“. Der Begriff „Inhaber der Datensammlung“ wird durch den Begriff „Verantwortlicher“ ersetzt. Das Änderungsprotokoll führt auch die Begriffe „Empfänger“ und „Auftragsverarbeiter“ ein. Damit erfolgt eine Annäherung der Terminologie an die DSGVO und DSRL-PJ.

Zu Art. 4 Änderungsprotokoll (Änderung von Art. 3 des Übereinkommens; Geltungsbereich)

Art. 4 des Änderungsprotokolls erweitert den Geltungsbereich des überarbeiteten Übereinkommens auf jegliche, gänzlich oder teilweise automatisierte oder strukturierte Verarbeitung personenbezogener Daten unter der Jurisdiktion der Vertragspartei (Art. 3 Abs. 1 des überarbeiteten Übereinkommens). Jedoch ist das überarbeitete Übereinkommen auf die Datenverarbeitung, die von einer natürlichen Person zur Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten vorgenommen wird, nicht mehr anwendbar (Art. 3 Abs. 2 des überarbeiteten Übereinkommens). Die Abs. 3 bis 6 von Art. 3 des Übereinkommens werden aufgehoben, da die Vertragsparteien nicht mehr die Möglichkeit haben, Erklärungen abzugeben (siehe Art. 38 des Änderungsprotokolls).

5.3 Grundsätze für den Schutz personenbezogener Daten

Zu Art. 5 Änderungsprotokoll (Änderung Überschrift des Kapitels II)

Die bisherige Überschrift des Kapitels II „Grundsätze für den Datenschutz“ wird durch folgende Überschrift ersetzt: „Grundsätze für den Schutz personenbezogener Daten“.

Zu Art. 6 Änderungsprotokoll (Änderung von Art. 4 des Übereinkommens; Pflichten der Vertragsparteien)

Art. 6 Abs. 1 und 2 des Änderungsprotokolls ändern Art. 4 Abs. 1 und 2 des Übereinkommens insofern, als sie in etwas geänderter Formulierung bestimmen, dass jede Vertragspartei die Bestimmungen des überarbeiteten Übereinkommens in ihrem innerstaatlichen Recht umsetzen muss. Auch müssen die gesetzgeberischen Massnahmen getroffen worden und in Kraft getreten sein, wenn der betreffende Staat das Änderungsprotokoll ratifiziert. Wie aus dem zusätzlich einzufügenden Art. 4 Abs. 3 des überarbeiteten Übereinkommens hervorgeht, ist diese Massnahme darauf ausgerichtet, dass das zuständige Organ des Europarates, d. h. der Übereinkommensausschuss (siehe Art. 27 ff. des Änderungsprotokolls), überprüfen kann, ob alle erforderlichen Massnahmen getroffen wurden, und sicherstellen kann, dass die Vertragspartei die eingegangenen Verpflichtungen einhält und in ihrem innerstaatlichen Recht ein angemessenes Niveau des Schutzes personenbezogener Daten gewährleistet. Der Übereinkommensausschuss kann auch eine Bewertung der Gesetzgebung der Vertragspartei vornehmen (Art. 4 Abs. 3 Bst. a des überarbeiteten Übereinkommens).

Zu Art. 7 Änderungsprotokoll (Änderung von Art. 5 des Übereinkommens; Rechtmässigkeit der Datenverarbeitung und Qualität der Daten)

Art. 7 des Änderungsprotokolls beinhaltet verschiedene Änderungen von Art. 5 des Übereinkommens. Dieser regelt fortan die Rechtmässigkeit der Datenverarbeitung und die Qualität der Daten.

Das Änderungsprotokoll führt das Verhältnismässigkeitsprinzip genauer aus. Gemäss dem überarbeiteten Art. 5 Abs. 1 muss jede Datenverarbeitung in Bezug auf den verfolgten rechtmässigen Zweck verhältnismässig sein und in allen Phasen der Verarbeitung auf das unbedingt Notwendige beschränkt sein.

Der Grundsatz der Rechtmässigkeit der Verarbeitung wird konkretisiert (Art. 5 Abs. 2 des überarbeiteten Übereinkommens). Die Rechtmässigkeit einer Verarbeitung ergibt sich entweder aus der Einwilligung des Betroffenen oder aus einer rechtmässigen, gesetzlich geregelten Grundlage. Der Erläuternde Bericht führt den Begriff Einwilligung genauer aus. Die Einwilligung des Betroffenen in die Verarbeitung seiner Daten ist nur rechtsgültig, wenn er der Datenverarbeitung für den konkreten Fall freiwillig, in informierter Weise und unmissverständlich zustimmt.

Das Änderungsprotokoll führt den Grundsatz der Zweckbindung näher aus (Art. 5 Abs. 4 Bst. b des überarbeiteten Übereinkommens). Personenbezogene Daten müssen für eindeutige, festgelegte und rechtmässige Zwecke erhoben werden. Die derzeitige Anforderung, dass der Zweck einer Verarbeitung mit dem ursprünglichen Zweck der Erhebung vereinbar bleiben muss, gilt weiterhin. Gemäss Präzisierung im Änderungsprotokoll ist diese Anforderung vorbehaltlich geeigneter Datenschutzgarantien bei einer Weiterverarbeitung für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfüllt. Die übrigen Grundsätze, die im überarbeiteten Art. 5 Abs. 3 und 4 vorgesehen sind, bleiben unverändert.

Zu Art. 8 Änderungsprotokoll (Änderung von Art. 6 des Übereinkommens; Besondere Arten von Daten)

Das Änderungsprotokoll erweitert den Katalog der besonders schützenswerten Daten. Nach dem Art. 6 Abs. 1 des überarbeiteten Übereinkommens ist die Verarbeitung von genetischen oder von biometrischen Daten, anhand derer eine Person eindeutig identifizierbar ist, künftig nur erlaubt, wenn in einer gesetzlichen

Grundlage angemessene Garantien vorgesehen sind. Diese Garantien sind in Liechtenstein durch die DSGVO und das DSG sichergestellt. Der Begriff „personenbezogene Daten über Strafurteile“ wird durch den Begriff „personenbezogene Daten bezüglich Straftaten, Strafverfahren und Strafurteilen und damit zusammenhängenden Sicherungsmassnahmen“ ersetzt. Schliesslich sind in Art. 6 zusätzlich zu Daten über politische Meinungen auch Daten über die Gewerkschaftszugehörigkeit erwähnt.

Zu Art. 9 Änderungsprotokoll (Änderung von Art. 7 des Übereinkommens; Datensicherung)

Der in Art. 7 Abs. 1 des überarbeiteten Übereinkommens festgelegte Grundsatz der Datensicherung bleibt im Wesentlichen unverändert. In Art. 7 Abs. 2 führt das Änderungsprotokoll hingegen eine neue Bestimmung für Verletzungen des Datenschutzes ein. Diese Bestimmung verpflichtet die Vertragsparteien, für den Verantwortlichen die Pflicht vorzusehen, Verletzungen des Datenschutzes, die einen schweren Eingriff in die Rechte und Grundfreiheiten von Betroffenen darstellen können, unverzüglich der zuständigen Aufsichtsbehörde zu melden.

Zu Art. 10 Änderungsprotokoll (Einführung eines neuen Art. 8 des Übereinkommens; Transparenz der Verarbeitung)

Das Änderungsprotokoll führt einen neuen Art. 8 ein, der die Informationspflicht des Verantwortlichen regelt. Diese Bestimmung ersetzt Art. 8 Bst. a des Übereinkommens.

Gemäss dem neuen Art. 8 ist der Verantwortliche verpflichtet, den Betroffenen über alle ihn betreffenden Datenverarbeitungen in Kenntnis zu setzen. Der Verantwortliche teilt dem Betroffenen Folgendes mit: seine Identität, die Rechtsgrundlage und den Zweck der Datenverarbeitung, die Arten der verarbeiteten Daten, gegebenenfalls die Empfänger oder Kategorien von Empfängern sowie die Mittel zur Ausübung der in Art. 9 des überarbeiteten Übereinkommens

dargelegten Rechte. Die Informationspflicht entfällt, wenn der Betroffene bereits über diese Informationen verfügt (Art. 8 Abs. 2), wenn die Verarbeitung ausdrücklich gesetzlich vorgeschrieben ist oder wenn sich die Information als unmöglich erweist oder mit unverhältnismässig hohem Aufwand verbunden ist (Art. 8 Abs. 3).

Zu Art. 11 Änderungsprotokoll (Ersatz von Art. 8 des Übereinkommens durch Art. 9 und Änderung; Rechte des Betroffenen)

Das Änderungsprotokoll stärkt die Rechte der betroffenen Personen. Der neue Art. 9 sieht vor, dass der Betroffene das Recht hat, nicht einer ausschliesslich auf einer automatisierten Datenverarbeitung beruhenden Entscheidung unterworfen zu werden, ohne dass er seinen Standpunkt geltend machen kann, es sei denn, die Entscheidung ist gesetzlich vorgesehen (Art. 9 Abs. 1 Bst. a und Abs. 2). Er hat auch das Recht, auf Antrag Kenntnis über die der Datenverarbeitung zugrundeliegenden Überlegungen zu erlangen (Art. 9 Abs. 1 Bst. c), und jederzeit gegen die Verarbeitung von ihn betreffenden personenbezogenen Daten Widerspruch einzulegen, sofern der Verantwortliche nicht nachweisen kann, dass berechtigte Gründe für die Verarbeitung bestehen (Art. 9 Abs. 1 Bst. d). Bei der Ausübung seiner Rechte muss der Betroffene unabhängig von seiner Staatsangehörigkeit oder seinem Wohnsitz die Hilfe einer Aufsichtsbehörde in Anspruch nehmen können (Art. 9 Abs. 1 Bst. g).

Das Auskunftsrecht der betroffenen Personen wird ausgebaut. Gemäss Art. 9 Abs. 1 Bst. b hat der Betroffene das Recht, nicht nur eine Bestätigung über die Verarbeitung von ihn betreffenden Daten und die Mitteilung über die verarbeiteten Daten in verständlicher Form, sondern auch alle verfügbaren Informationen über den Ursprung und die Aufbewahrungsfrist der Daten sowie alle sonstigen Informationen zu erhalten, zu deren Bereitstellung der Verantwortliche nach Art. 8 Abs. 1 des überarbeiteten Übereinkommens verpflichtet ist.

Zu Art. 12 Änderungsprotokoll (Einführung eines neuen Art. 10 des Übereinkommens; zusätzliche Verpflichtungen)

Das Änderungsprotokoll führt einen neuen Art. 10 des Übereinkommens ein, der die Pflichten des Verantwortlichen und gegebenenfalls des Auftragsverarbeiters erweitert. Gemäss Art. 10 Abs. 1 müssen die Vertragsparteien für den Verantwortlichen und den Auftragsverarbeiter die Pflicht vorsehen, die Anforderungen des überarbeiteten Übereinkommens einzuhalten und dies gegenüber der zuständigen Aufsichtsbehörde nachweisen zu können. Ausserdem müssen die Vertragsparteien für den Verantwortlichen und den Auftragsverarbeiter die Pflicht vorsehen, die wahrscheinlichen Auswirkungen der beabsichtigten Datenverarbeitung auf die Rechte und Grundfreiheiten der Betroffenen zu untersuchen und sie so auszugestalten, dass das Risiko des Eingriffs in diese Rechte und Grundfreiheiten verhindert oder miniert wird (Art. 10 Abs. 2) sowie unter Berücksichtigung der Art der Verarbeitung und gegebenenfalls ihrer Grösse die Grundsätze des „Datenschutzes durch Technik“ und des „Datenschutzes durch datenschutzfreundliche Voreinstellungen“ anzuwenden (Art. 10 Abs. 3 und 4).

Zu Art. 13 Änderungsprotokoll (Verschiebung bisheriger Artikel)

Die bisherigen Art. 9 bis 12 des Übereinkommens werden die Art. 11 bis 14 des überarbeiteten Übereinkommens.

Zu Art. 14 Änderungsprotokoll (Ersatz von Art. 9 des Übereinkommens durch Art. 11 und Änderung; Ausnahmen und Einschränkungen)

Wie Art. 9 im ursprünglichen Übereinkommen sieht auch der neue Art. 11 vor, dass die Grundsätze des Datenschutzes nicht eingeschränkt werden dürfen. Ausnahmen können jedoch vorgesehen werden in Bezug auf gewisse Bestimmungen und unter der Voraussetzung, dass eine solche Einschränkung gesetzlich vorgesehen ist und einer notwendigen und verhältnismässigen Massnahme zum Schutz bestimmter Interessen entspricht, die in Art. 11 Abs. 1 aufgeführt sind. Das

Änderungsprotokoll erweitert dabei den Katalog der schutzwürdigen Interessen: Es erwähnt neben den bisher schon genannten Interessen neu auch die Landesverteidigung, wichtige wirtschaftliche und finanzielle Interessen des Staates (und nicht mehr nur die Währungsinteressen), die Unparteilichkeit und Unabhängigkeit der Justiz, die Ermittlung und Verfolgung von Straftaten und die Strafvollstreckung (und nicht mehr nur die Bekämpfung von Straftaten) sowie sonstige wichtige Ziele des allgemeinen öffentlichen Interesses.

Art. 11 Abs. 2 ist neu und sieht vor, dass in Bezug auf die Datenverarbeitung zu Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unter bestimmten Voraussetzungen Anwendungsbeschränkungen der Art. 8 und 9 festgelegt werden können. Schliesslich werden die Vertragsparteien auch ermächtigt, im Hinblick auf Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung bestimmte spezifische Ausnahmen vorzusehen (Art. 14 Abs. 3 des überarbeiteten Übereinkommens). Damit würde das Änderungsprotokoll insgesamt weitergehende Ausnahmen erlauben als die DSGVO. Aufgrund des EWRs bleiben für Liechtenstein jedoch die restriktiveren Beschränkungsmöglichkeiten gemäss DSGVO massgeblich, die theoretisch weitergehenden Ausnahmen haben somit für Liechtenstein keine Relevanz.

Zu Art. 15 Änderungsprotokoll (Ersatz von Art. 10 des Übereinkommens durch Art. 12 und Änderung; Sanktionen und Rechtsmittel)

Der Anwendungsbereich des neuen Art. 12 wird erweitert: Die Vertragsparteien sind verpflichtet, geeignete gerichtliche und aussergerichtliche Sanktionen und Rechtsmittel für Verstösse gegen die Bestimmungen des Übereinkommens festzulegen. Dies kann in Liechtenstein über zwei Wege geschehen: Entweder kann über die Datenschutzstelle eine Beschwerde eingereicht werden, oder es kann der gerichtliche Klageweg einschlagen werden.

5.4 Bekanntgabe von Personendaten ins Ausland

Zu Art. 16 Änderungsprotokoll (Änderung Überschrift des Kapitels III)

Die bisherige Überschrift des Kapitels III „Grenzüberschreitender Datenverkehr" wird durch folgende Überschrift ersetzt: „Grenzüberschreitender Verkehr personenbezogener Daten".

Zu Art. 17 Änderungsprotokoll (Ersatz von Art. 12 des Übereinkommens durch Art. 14 und Änderung; Grenzüberschreitender Verkehr personenbezogener Daten)

Gemäss Art. 17 des Änderungsprotokolls wird Art. 12 des Übereinkommens zu Art. 14 des überarbeiteten Übereinkommens. Darin wird Art. 2 des Zusatzprotokolls mit einer Reihe von Änderungen aufgenommen.

Der erste Satz von Art. 14 Abs. 1 des überarbeiteten Übereinkommens entspricht Art. 12 Abs. 2 des derzeitigen Übereinkommens, der den freien Datenverkehr zwischen den Vertragsparteien gewährleistet. Art. 17 des Änderungsprotokolls schränkt diesen Grundsatz ein, indem er vorsieht, dass jede Vertragspartei in bestimmten Fällen die Weitergabe von Daten an einen Empfänger, welcher der Hoheitsgewalt einer anderen Vertragspartei untersteht, verbieten oder von einer besonderen Genehmigung abhängig machen kann, beispielsweise wenn eine Vertragspartei durch harmonisierte gemeinsame Schutzvorschriften von Staaten, die einer regionalen internationalen Organisation angehören, gebunden ist (zweiter und dritter Satz von Art. 14 Abs. 1 des überarbeiteten Übereinkommens).

Der Grundsatz, wonach personenbezogene Daten nur an einen Drittstaat weitergegeben werden dürfen, wenn ein angemessenes Schutzniveau gewährleistet ist, bleibt im Vergleich zum gegenwärtigen Übereinkommen unverändert. In Art. 14 Abs. 3 des überarbeiteten Übereinkommens wird genauer ausgeführt, dass ein angemessenes Schutzniveau durch das Recht dieses Staates sichergestellt werden

kann, einschliesslich der anwendbaren völkerrechtlichen Verträge oder Übereinkünfte, oder durch Ad-hoc-Garantien oder genehmigte standardisierte Garantien, die von den an der Weitergabe beteiligten Personen angenommen worden sind und umgesetzt werden. Gemäss dem Änderungsprotokoll müssen die Vertragsparteien auch vorsehen, dass die Aufsichtsbehörde von der Person, welche die Daten weitergibt, verlangen kann, dass sie alle sachdienlichen Informationen hinsichtlich der Weitergabe von Daten zur Verfügung stellt (Art. 14 Abs. 5 des überarbeiteten Übereinkommens). Sie kann vom Verantwortlichen auch verlangen, die Wirksamkeit der getroffenen Garantien nachzuweisen, und sie ist berechtigt, gegebenenfalls die Datenweitergabe zu verbieten oder auszusetzen (Art. 14 Abs. 6 des überarbeiteten Übereinkommens).

Mit Art. 17 des Änderungsprotokolls werden die in Art. 2 Abs. 2 des Zusatzprotokolls vorgesehenen Ausnahmen in den Art. 14 Abs. 4 des überarbeiteten Übereinkommens aufgenommen. Somit können personenbezogene Daten trotz des Fehlens eines angemessenen Datenschutzniveaus in einen Drittstaat weitergegeben werden. Dies nicht nur, wenn dies aufgrund überwiegender Interessen, einschliesslich jener des Betroffenen, erforderlich ist, sondern auch wenn der Betroffene ausdrücklich, für den konkreten Fall und freiwillig eingewilligt hat, nachdem er über die Gefahren aufgeklärt wurde, die bei Fehlen geeigneter Garantien entstehen können (Art. 14 Abs. 4 Bst. a), oder wenn diese Datenweitergabe in einer demokratischen Gesellschaft im Hinblick auf die Meinungsfreiheit eine notwendige und verhältnismässige Massnahme darstellt (Art. 14 Abs. 4 Bst. d).

5.5 Aufsichtsbehörden

Zu Art. 18 Änderungsprotokoll (Einführung eines neuen Kapitels IV; Aufsichtsbehörden)

Nach Kapitel III des Übereinkommens wird ein neues Kapitel IV mit folgender Überschrift eingefügt: „Kapitel IV – Aufsichtsbehörden“.

Zu Art. 19 Änderungsprotokoll (Einführung eines neuen Art. 15; Aufsichtsbehörden)

Mit Art. 19 des Änderungsprotokolls werden die Bestimmungen von Art. 1 des Zusatzprotokolls mit einer Reihe von Änderungen in Art. 15 des überarbeiteten Übereinkommens aufgenommen.

Wie bisher haben die Aufsichtsbehörden Untersuchungs- und Einwirkungsbefugnisse und können gerichtliche Schritte einleiten. Gemäss dem neuen Art. 15 Abs. 2 Bst. c und Abs. 9 sind sie zudem befugt, anfechtbare Entscheidungen zu treffen, und können insbesondere verwaltungsrechtliche Sanktionen verhängen. Nicht zuständig sind die Aufsichtsbehörden lediglich für Verarbeitungen, die von Organen im Rahmen ihrer gerichtlichen Tätigkeit vorgenommen werden (Art. 15 Abs. 10 des überarbeiteten Übereinkommens).

Mit Art. 19 des Änderungsprotokolls werden den Aufsichtsbehörden neue Aufgaben verliehen. Sie sind namentlich dafür zuständig, zum einen das öffentliche Bewusstsein für den Datenschutz (Art. 15 Abs. 2 Bst. e Ziff. i und ii des überarbeiteten Übereinkommens) und zum anderen das Bewusstsein bei den Verantwortlichen und den Auftragsverarbeitern für ihre Pflichten (Art. 15 Abs. 2 Bst. e Ziff. iii des überarbeiteten Übereinkommens) zu fördern.

Nach Art. 15 Abs. 3 des überarbeiteten Übereinkommens werden die zuständigen Aufsichtsbehörden bei allen Vorschlägen für Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten vorsehen, zu Rate gezogen.

Mit Art. 19 des Änderungsprotokolls wird im Weiteren das Recht des Betroffenen festgelegt, an die Aufsichtsbehörde zu gelangen (ursprünglich Art. 1 Abs. 2 Bst. b des Zusatzprotokolls). Art. 15 Abs. 4 des überarbeiteten Übereinkommens sieht nun vor, dass sich die Aufsichtsbehörde mit Anträgen und Beschwerden von Betroffenen zu befassen und sie über den Fortgang auf dem Laufenden zu halten hat.

Wie bisher muss die Unabhängigkeit der Aufsichtsbehörden gewährleistet werden (Art. 15 Abs. 5 des überarbeiteten Übereinkommens). Mit der Änderung von Art. 19 des Änderungsprotokolls müssen die Vertragsparteien künftig auch sicherstellen, dass die Aufsichtsbehörden mit den zur wirksamen Erfüllung ihrer Aufgaben und Wahrnehmung ihrer Befugnisse nötigen Ressourcen ausgestattet werden (Art. 15 Abs. 6 des überarbeiteten Übereinkommens).

In Liechtenstein ist die dafür zuständige Aufsichtsbehörde die Datenschutzstelle.

5.6 Zusammenarbeit und gegenseitige Hilfeleistung

Zu Art. 20 Änderungsprotokoll (Änderung Überschrift des Kapitels V, Verschiebung Kapitel und Artikel)

Die Kapitel IV bis VII des Übereinkommens werden neu nummeriert zu Kapitel V bis VIII des Übereinkommens. Die Überschrift des bisherigen „Kapitel V – Beratender Ausschuss“ wird durch die Überschrift „Kapitel V – Zusammenarbeit und gegenseitige Hilfeleistung“ ersetzt.

Zu Art. 21 Änderungsprotokoll (Ersatz von Art. 13 des Übereinkommens durch Art. 16 und Änderung; Benennung von Aufsichtsbehörden)

Art. 16 Abs. 1 des überarbeiteten Übereinkommens sieht vor, dass die Vertragsparteien sich verpflichten, zusammenzuarbeiten und einander Hilfe zu leisten. Die Verpflichtung, eine oder mehrere Aufsichtsbehörden zu benennen, bleibt unverändert.

Zu Art. 22 Änderungsprotokoll (Einführung eines neuen Art. 17; Formen der Zusammenarbeit)

Mit Art. 22 des Änderungsprotokolls wird ein neuer Art. 17 eingeführt, der die verschiedenen Formen der Zusammenarbeit der Aufsichtsbehörden nicht abschliessend regelt. So ist insbesondere vorgesehen, dass die gemäss Übereinkommen von den Vertragsparteien designierten datenschutzrechtlichen Aufsichtsbehörden

einander durch den Austausch notwendiger Informationen Hilfe leisten und dass sie ihre Untersuchungen abstimmen oder sie gemeinsame Massnahmen durchführen. Sie bilden auch ein Netzwerk, um ihre Zusammenarbeit zu organisieren und zu stärken.

Zu Art. 23 Änderungsprotokoll (Ersatz von Art. 14 des Übereinkommens durch Art. 18 und Änderung; Unterstützung von Betroffenen)

Mit Art. 23 des Änderungsprotokolls wird die Unterstützung von Betroffenen, ungeachtet ihres Wohnorts oder ihrer Staatsangehörigkeit, in Art. 18 des überarbeiteten Übereinkommens gewährleistet. Wie bisher kann ein Betroffener mit Wohnsitz in einer anderen Vertragspartei seine Rechte direkt im Staat ausüben, in dem seine personenbezogenen Daten verarbeitet werden, oder indirekt durch die von diesem Staat benannte datenschutzrechtliche Aufsichtsbehörde.

Zu Art. 24 Änderungsprotokoll (Ersatz von Art. 15 des Übereinkommens durch Art. 19 und Änderung; Garantien)

Wie im geltenden Übereinkommen in Art. 15 ist im neuen Art. 19 Abs. 1 vorgesehen, dass bei gegenseitiger Hilfeleistung zwischen datenschutzrechtlichen Aufsichtsbehörden diese den Grundsatz der Spezialität beachten müssen, d. h., dass sie übermittelte Auskünfte nur zu den Zwecken verwenden dürfen, die dem Antrag oder Ersuchen um Unterstützung zugrunde liegen. Im Weiteren ist es den Aufsichtsbehörden nicht erlaubt, im Namen eines Betroffenen von sich aus und ohne dessen ausdrückliche Genehmigung einen Antrag auf Unterstützung zu stellen (Art. 19 Abs. 2 des überarbeiteten Übereinkommens). Die Verpflichtung zur Verschwiegenheit ist künftig in Art. 15 Abs. 8 des überarbeiteten Übereinkommens vorgesehen.

Zu Art. 25 Änderungsprotokoll (Ersatz von Art. 16 des Übereinkommens durch Art. 20 und Änderung; Ablehnung von Ersuchen)

Durch Art. 25 des Änderungsprotokolls werden lediglich redaktionelle Änderungen vorgenommen.

Zu Art. 26 Änderungsprotokoll (keine Auswirkung auf die deutsche Übersetzung)

Durch Art. 26 des Änderungsprotokolls werden sprachliche Änderungen in Art. 17 Abs. 1 des Übereinkommens aufgeführt, welche neu in Art. 21 geregelt sind, jedoch keine Auswirkungen auf die deutsche Übersetzung haben.

5.7 Übereinkommensausschuss

Zu Art. 27 Änderungsprotokoll (Änderung Überschrift des Kapitels VI)

Die Überschrift des bisherigen Kapitels V „Beratender Ausschuss“ (neues Kapitel VI) des Übereinkommens wird durch folgende Überschrift im überarbeiteten Übereinkommen ersetzt: „Kapitel VI – Übereinkommensausschuss“.

Zu Art. 28 Änderungsprotokoll (Ersatz von Art. 18 des Übereinkommens durch Art. 22 und Änderung; Zusammensetzung des Ausschusses)

Art. 28 des Änderungsprotokolls ergänzt den neuen Art. 22 des Übereinkommens mit einer Bestimmung über die Vertretung und die finanzielle Beteiligung von Vertragsparteien, die nicht Mitglied des Europarates sind. Des Weiteren kann ein Beobachter nun mit einer Zweidrittelmehrheit (bisher einstimmiger Beschluss) zur Teilnahme an die Sitzungen eingeladen werden.

Zu Art. 29 Änderungsprotokoll (Ersatz von Art. 19 des Übereinkommens durch Art. 23 und Änderung; Aufgaben des Ausschusses)

Der in den Art. 18 ff. des Übereinkommens vorgesehene Beratende Ausschuss wird durch einen Übereinkommensausschuss ersetzt. Mit der Änderung in Art. 29 des Änderungsprotokolls werden ihm im Art. 23 des überarbeiteten Übereinkommens neue Aufgaben übertragen und damit seine Funktion gestärkt. Um die

Anwendung des überarbeiteten Übereinkommens zu erleichtern oder zu verbessern, kann der Übereinkommensausschuss nun Empfehlungen abgeben, statt nur Vorschläge zu unterbreiten (Art. 23 Bst. a überarbeiteten Übereinkommen). Er hat auch die Aufgabe, vor jedem neuen Beitritt zum Übereinkommen eine Stellungnahme für das Ministerkomitee zum Schutzniveau für personenbezogene Daten zu erarbeiten, das der Beitrittskandidat gewährleistet (Art. 23 Bst. e). Schliesslich überprüft er die Durchführung des überarbeiteten Übereinkommens durch die Vertragsparteien und empfiehlt gegebenenfalls Massnahmen für eine überprüfte Vertragspartei (Art. 23 Bst. h).

Zu Art. 30 Änderungsprotokoll (Ersatz von Art. 20 des Übereinkommens durch Art. 24 und Änderung; Verfahren)

Art. 30 des Änderungsprotokolls sieht vor, dass die Abstimmungsmodalitäten im Übereinkommensausschuss in den Elementen der Geschäftsordnung festgelegt werden, die sich im Anhang des Änderungsprotokolls finden (siehe dazu weiter unten Ziff. 5.10). Zusätzlich zur Erarbeitung der übrigen Elemente seiner Geschäftsordnung soll der Übereinkommensausschuss gemäss dem neuen Art. 24 Abs. 4 darin auch, auf der Grundlage objektiver Kriterien, die Verfahren für die Bewertung und Überprüfung von beitrittswilligen und bestehenden Vertragsparteien nach Art. 4 Abs. 3 und 23 Bst. e, f und h des überarbeiteten Übereinkommens festlegen (Überprüfungsverfahren).

5.8 Änderungen

Zu Art. 31 Änderungsprotokoll (Ersatz von Art. 21 des Übereinkommens durch Art. 25 und Änderung; Änderungen)

Die hauptsächliche Änderung von Art. 25 des überarbeiteten Übereinkommens besteht in der Einführung eines Abs. 7. Grundsätzlich tritt jede Änderung innerhalb von 30 Tagen nach dem Tag in Kraft, an dem alle Vertragsparteien dem Europarat mitgeteilt haben, dass sie die Änderung gutheissen. Gemäss Art. 25 Abs. 7 des

überarbeiteten Übereinkommens kann das Ministerkomitee jedoch unter bestimmten Bedingungen beschliessen, das Inkrafttreten geringfügiger Änderungen um drei Jahre zu verschieben, sofern keine Vertragspartei einen Einwand notifiziert.

5.9 Schlussklauseln

Zu Art. 32 Änderungsprotokoll (Ersatz von Art. 22 des Übereinkommens durch Art. 26 und Änderung; Inkrafttreten)

Durch Art. 32 Änderungsprotokoll kann das überarbeitete Übereinkommen auch explizit von der EU unterzeichnet und ratifiziert werden (Art. 26 Abs. 1 des überarbeiteten Übereinkommens).

Zu Art. 33 Änderungsprotokoll (Ersatz von Art. 23 des Übereinkommens durch Art. 27 und Änderung; Beitritt von Nichtmitgliedstaaten oder internationalen Organisationen)

Art. 33 des Änderungsprotokolls sieht vor, dass das überarbeiteten Übereinkommen nicht nur von Drittstaaten (bisheriger Art. 23 Abs. 1), sondern auch von internationalen Organisationen unterzeichnet werden kann (Art. 27 des überarbeiteten Übereinkommens). Gegebenenfalls überprüft der Übereinkommensausschuss das Datenschutzniveau, das vom Bewerberstaat bzw. von der Organisation gewährleistet wird (Art. 27 i.V.m. Art. 23 Bst. e des überarbeiteten Übereinkommens).

Zu Art. 34 Änderungsprotokoll (Ersatz von Art. 24 des Übereinkommens durch Art. 28 und Änderung; Räumlicher Geltungsbereich)

Da das Änderungsprotokoll auch zur Unterzeichnung durch die EU und internationale Organisationen aufliegt, wird in Art. 34 die Bestimmung zum räumlichen Geltungsbereich geändert, indem vorgesehen wird, dass auch die EU oder eine sonstige internationale Organisation einzelne oder mehrere Hoheitsgebiete

bezeichnen kann, auf die das überarbeitete Übereinkommen Anwendung findet. Der bisherige Art. 24 sprach lediglich von Staaten, der neue Art. 28 jedoch von „Staaten, der Europäischen Union oder sonstigen internationalen Organisationen".

Zu Art. 35 Änderungsprotokoll (Änderung Verweise, Begriffe)

In Art. 35 Änderungsprotokoll werden kleine Verweise und Begriffsänderungen aufgeführt.

Zu Art. 36 Änderungsprotokoll (Unterzeichnung, Ratifikation und Beitritt)

Diese Bestimmung regelt den Beitritt zum Änderungsprotokoll. Sie sieht insbesondere vor, dass jeder bestehende Vertragsstaat des Übereinkommens dem Änderungsprotokoll beitreten kann. Ein Staat, der bisher jedoch noch keine Vertragspartei des Übereinkommens ist, kann neu nur noch Vertragspartei des Übereinkommens werden, wenn er gleichzeitig auch dem Änderungsprotokoll beitritt (Art. 36 Abs. 2 des Änderungsprotokolls).

Zu Art. 37 Änderungsprotokoll (Inkrafttreten)

Nach Art. 37 Abs. 1 und Abs. 2 tritt das Änderungsprotokoll drei Monate, nachdem es von allen Vertragsparteien des Übereinkommens ratifiziert wurde, in Kraft, oder nach einem Zeitraum von fünf Jahren nach dem Tag, an dem es zur Unterzeichnung aufgelegt wurde (11. Oktober 2023), für diejenigen Staaten, die das Protokoll ratifiziert haben, sofern dem Protokoll mindestens 38 Vertragsparteien angehören.[7] Sollte dies bis Fristablauf nicht der Fall sein, tritt das Änderungsprotokoll spätestens dann in Kraft, sobald die erforderlichen 38 Ratifikationen vorliegen.

[7] Gemäss Stand vom 11. Januar 2023 sind für die Erreichung von 38 Ratifikationen und dem gleichzeitigen Inkrafttreten des Änderungsprotokolls noch weitere 18 Ratifikationen erforderlich.

Zu Art. 38 Änderungsprotokoll (Erklärungen im Zusammenhang mit dem Übereinkommen)

Diese Bestimmung sieht vor, dass mit Inkrafttreten des Änderungsprotokolls bzw. des überarbeiteten Übereinkommens die Erklärungen der Vertragsparteien nach Art. 3 des Übereinkommens unwirksam werden.

Bei der Ratifizierung des Übereinkommens hat Liechtenstein einerseits die Anwendung des Übereinkommens auch auf die Verarbeitung von „Personendaten von juristischen Personen, rechtsfähigen Personengesellschaften und auf Sammlungen von Personendaten, die nicht automatisiert bearbeitet werden“ erklärt, und andererseits die Nichtanwendung des Übereinkommens auf Personendaten, die vom Landtag oder parlamentarischen Kommissionen im Rahmen von Beratungen oder von der Finanzverwaltung bearbeitet werden, sowie auf Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet, erklärt (LGBl 2004.167; Übereinkommen). Eine weitere Erklärung zur Nichtanwendung des Übereinkommens auf Datensätze, die zur Erfüllung von Sorgfaltspflichten gemäss Sorgfaltspflichtgesetz (LGBl 2009.047; SPG) angelegt werden, wurde bereits 2010 teilweise zurückgezogen. Die künftige Unwirksamkeit dieser Erklärungen ist für Liechtenstein nicht problematisch, denn der Geltungsbereich des überarbeiteten Übereinkommens entspricht dem aktuellen Geltungsbereich der DSGVO und des DSG.

Zu Art. 39 Änderungsprotokoll (Vorbehalte)

Nach Art. 39 des Änderungsprotokolls können Vertragsparteien keine Vorbehalte zum Änderungsprotokoll anbringen. Bereits bisher bestand im Übereinkommen (bisheriger Art. 25) keine Möglichkeit, Vorbehalte anzubringen, noch ist dies in der durch das Änderungsprotokoll überarbeiteten Fassung des Übereinkommens vorgesehen.

Zu Art. 40 Änderungsprotokoll (Notifikationen)

Diese Bestimmung sieht vor, dass das Sekretariat des Europarates den Mitgliedstaaten des Europarates und jeder anderen Vertragspartei des Übereinkommens jeden weiteren Beitritt zum Änderungsprotokoll und den Zeitpunkt seines Inkrafttretens notifiziert (bisheriger Art. 27).

5.10 Anhang des Änderungsprotokolls: Elemente der Geschäftsordnung des Übereinkommensausschusses

Im Anhang des Änderungsprotokolls sind die Elemente festgelegt, die in die Geschäftsordnung des Übereinkommensausschusses aufzunehmen sind, insbesondere die Stimmberechtigung jeder Vertragspartei und die Mehrheiten, mit denen Beschlüsse des Übereinkommensausschusses verabschiedet werden können (siehe ebenfalls Art. 24 Abs. 3 des überarbeiteten Übereinkommens bzw. Art. 30 des Änderungsprotokolls).

6. VERFASSUNGSMÄSSIGKEIT / RECHTLICHES

Dem Beitritt des Fürstentums Liechtenstein zum Änderungsprotokoll stehen keine verfassungsrechtlichen Bestimmungen entgegen. Der Inhalt des Änderungsprotokolls bzw. das überarbeitete Übereinkommen entspricht – in etwas weniger detaillierter Form – den Datenschutzgrundsätzen der DSGVO und der DSRL-PJ weitgehend. Liechtenstein hat die direkt anwendbare DSGVO im Rahmen des EWR bereits am 20. Juli 2018 und die DSRL-PJ zur Wahrung des Schengen-Besitzstandes bereits am 13. Dezember 2016 übernommen. Die Bestimmungen der DSRL-PJ wurden in der Folge mit dem neuen liechtensteinischen DSG im nationalen Recht umgesetzt. Die Verfassungsmässigkeit der Bestimmungen wurde deshalb schon zu diesen Zeitpunkten jeweils geprüft und sichergestellt. Zur beantragten Ratifikation des Änderungsprotokolls sind in Liechtenstein daher keine verfassungsrechtlichen oder weiteren gesetzlichen Anpassungen mehr erforderlich.

7. AUSWIRKUNGEN AUF VERWALTUNGSTÄTIGKEIT, RESSOURCENEINSATZ UND NACHHALTIGE ENTWICKLUNG

7.1 Neue und veränderte Kernaufgaben

Mit dieser Vorlage werden weder neue Kernaufgaben eingeführt noch bestehende Kernaufgaben verändert.

7.2 Personelle, finanzielle, organisatorische und räumliche Auswirkungen

Die nationale Umsetzung wird für Liechtenstein keine nennenswerten personellen Auswirkungen haben. Abgesehen von gewissen Berichterstattungserfordernissen fallen keine neuen Verpflichtungen für Liechtenstein an. Die nationale Umsetzung des Änderungsprotokolls ist bereits durch die DSGVO und das DSG gegeben.

Mit dem Änderungsprotokoll wird ein Überprüfungsverfahren eingeführt, welches periodisch die Einhaltung der Bestimmungen der überarbeiteten Konvention in den Vertragsstaaten überprüft. Obwohl mit einem gewissen Aufwand für die Berichterstattung und die Information an den Übereinkommensausschuss gerechnet werden muss, ist davon auszugehen, dass er sich im Rahmen anderer Abkommen bewegt und mit den bestehenden Personalressourcen bewältigt werden kann.

7.3 Betroffene UNO-Nachhaltigkeitsziele und Auswirkungen auf deren Umsetzung

Die Auswirkungen auf die nachhaltige Entwicklung lassen sich anhand der 17 Nachhaltigkeitsziele (Sustainable Developmenet Goals; SDGs) wie folgt zusammenfassen:

Auswirkungen der gegenständlichen Gesetzesanpassungen auf die SDGs		
Betroffenes Ziel	***Relevante Unterziele***	***Zu erwartende Auswirkungen durch die Regierungsvorlage***
SDG 16 Frieden, Gerechtigkeit und starke Institutionen	16.3, 16.10	Mit der Ratifizierung des Änderungsprotokolls wird zur Etablierung eines internationalen rechtlichen Rahmenwerks zur Datenverarbeitung und zum Datenschutz beigetragen, welches gerade im digitalen Zeitalter von besonderer Relevanz ist. Mit der weiteren Vereinheitlichung des Datenschutzniveaus auf internationaler Ebene und der Erleichterung des grenzüberschreitenden Datentransfers von und nach Drittstaaten können Garantien für eine sichere Übermittlung der Daten sichergestellt werden. Vor diesem Hintergrund werden, im Einklang mit den nationalen Rechtsvorschriften und völkerrechtlichen Übereinkünften, einerseits der öffentliche Zugang zu Informationen bzw. die Verarbeitung von personenbezogenen Daten gewährleistet und andererseits die Grundfreiheiten der natürlichen Personen geschützt. Dies trägt zur Förderung der Rechtsstaatlichkeit auf nationaler und internationaler Ebene bei.

Es ist zu erwarten, dass sich die Umsetzung dieser Gesetzesvorlage positiv auf das SDG auswirken wird. Zwischen den Unterzielen des SDGs bestehen keine Zielkonflikte.

7.4 Evaluation

Da weder neue Aufgaben geschaffen noch bestehende verändert werden, ist eine Evaluation des gegenständlichen Änderungsprotokolls nicht notwendig.

II. ANTRAG DER REGIERUNG

Aufgrund der vorstehenden Ausführungen unterbreitet die Regierung dem Landtag den

A n t r a g ,

der Hohe Landtag wolle diesen Bericht und Antrag zur Kenntnis nehmen und der Ratifikation des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten seine Zustimmung erteilen.

Genehmigen Sie, sehr geehrter Herr Landtagspräsident, sehr geehrte Frauen und Herren Abgeordnete, den Ausdruck der vorzüglichen Hochachtung.

REGIERUNG DES
FÜRSTENTUMS LIECHTENSTEIN

gez. Daniel Risch

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Sammlung der Europaratsverträgen - Nr. 223

Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Straßburg/Strasbourg, 10.X.2018

Zwischen AUT, BEL, CHE, LIE und DEU abgestimmte Übersetzung;
Endfassung vom 5. November 2019

Präambel

Die Mitgliedstaaten des Europarats und die anderen Vertragsparteien des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108), das am 28. Januar 1981 in Straßburg zur Unterzeichnung aufgelegt wurde (im Folgenden als „Übereinkommen" bezeichnet), –

im Hinblick auf die Entschließung Nr. 3 zu Datenschutz und Persönlichkeitsbereich im dritten Jahrtausend, die auf der 30. Konferenz der Justizminister des Europarats (Istanbul, Türkei, 24. – 26. November 2010) angenommen wurde;

im Hinblick auf die Entschließung 1843 (2011) der Parlamentarischen Versammlung des Europarats zum Schutz des Persönlichkeitsbereichs und der personenbezogenen Daten im Internet und in Onlinemedien sowie die Entschließung 1986 (2014) zur Verbesserung des Nutzerschutzes und der Nutzersicherheit im Internet;

im Hinblick auf die Stellungnahme 296 (2017) zum Entwurf eines Protokolls zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) und seines Erläuternden Berichts, die vom Ständigen Ausschuss im Namen der Parlamentarischen Versammlung des Europarats am 24. November 2017 angenommen wurde;

in der Erwägung, dass sich seit der Annahme des Übereinkommens im Hinblick auf die Verarbeitung von personenbezogenen Daten neue Herausforderungen für den Schutz des Menschen ergeben haben;

angesichts der Notwendigkeit sicherzustellen, dass das Übereinkommen auch weiterhin eine herausgehobene Rolle beim Schutz des Menschen bei der Verarbeitung personenbezogener Daten und in einem allgemeineren Sinne für den Schutz der Menschenrechte und Grundfreiheiten spielt –

sind wie folgt übereingekommen:

Artikel 1

1 Der erste Beweggrund in der Präambel des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„Die Mitgliedstaaten des Europarats und die anderen Unterzeichner dieses Übereinkommens –".

2 Der dritte Beweggrund der Präambel des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„angesichts der Notwendigkeit, die Würde des Menschen und den Schutz der Menschenrechte und Grundfreiheiten jedes Menschen sowie, im Hinblick auf die Diversifizierung, Intensivierung und Globalisierung der Datenverarbeitung und des Verkehrs von personenbezogenen Daten, die persönliche Entscheidungsfreiheit auf der Grundlage des Rechts jedes Einzelnen, selbst über seine personenbezogenen Daten und die Verarbeitung solcher Daten zu bestimmen, sicherzustellen,".

3 Der vierte Beweggrund der Präambel des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„unter Hinweis darauf, dass das Recht auf den Schutz personenbezogener Daten in Bezug auf dessen gesellschaftliche Rolle zu betrachten ist und dass es mit anderen Menschenrechten und Grundfreiheiten, einschließlich der freien Meinungsäußerung, in Einklang zu bringen ist,".

4 Nach dem vierten Beweggrund der Präambel des Übereinkommens wird folgender Beweggrund eingefügt:

„im Hinblick darauf, dass dieses Übereinkommen es zulässt, dass bei der Durchführung der darin festgelegten Vorschriften der Grundsatz des Zugangsrechts zu amtlichen Dokumenten berücksichtigt wird,".

5 Der bisherige fünfte Beweggrund der Präambel des Übereinkommens wird gestrichen. Ein neuer fünfter und ein neuer sechster Beweggrund werden angefügt; sie lauten wie folgt:

„in Anerkennung der Notwendigkeit, die grundlegenden Werte der Achtung des Persönlichkeitsbereichs und des Schutzes personenbezogener Daten weltweit zu fördern und dadurch zum freien Informationsaustausch zwischen den Völkern beizutragen,

in Anerkennung des Interesses, die internationale Zusammenarbeit zwischen den Vertragsparteien des Übereinkommens zu stärken –".

Artikel 2

Der Wortlaut des Artikels 1 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„Zweck dieses Übereinkommens ist es, jede natürliche Person ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnorts im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten zu schützen und dadurch zur Wahrung ihrer Menschenrechte und Grundfreiheiten, und insbesondere des Rechts auf einen Persönlichkeitsbereich, beizutragen."

Artikel 3

1 Artikel 2 Buchstabe b des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„b bedeutet ‚Datenverarbeitung' jeden Vorgang oder jede Vorgangsreihe, der beziehungsweise die im Zusammenhang mit personenbezogenen Daten ausgeführt wird, wie das Erheben, die Speicherung, die Aufbewahrung, die Veränderung, das Auslesen, die Offenlegung, die Bereitstellung, das Löschen oder die Vernichtung solcher Daten oder die Anwendung von logischen und/oder arithmetischen Operationen auf solche Daten;".

2 Artikel 2 Buchstabe c des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„c bedeutet, sofern keine automatisierte Verarbeitung stattfindet, ‚Datenverarbeitung' einen Vorgang oder eine Vorgangsreihe, der beziehungsweise die im Zusammenhang mit personenbezogenen Daten innerhalb einer strukturierten Reihe solcher Daten ausgeführt wird, auf die nach spezifischen Kriterien zugegriffen werden kann oder die nach spezifischen Kriterien ausgelesen werden können;".

3 Artikel 2 Buchstabe d des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„d bedeutet ‚Verantwortlicher' die natürliche oder juristische Person, die Behörde, den Dienst, die Einrichtung oder jede andere Stelle, die beziehungsweise der allein oder gemeinsam mit anderen Entscheidungsbefugnis im Hinblick auf die Datenverarbeitung hat;".

4 Nach Artikel 2 Buchstabe d des Übereinkommens werden folgende neue Buchstaben eingefügt:

„e bedeutet ‚Empfänger' eine natürliche oder juristische Person, eine Behörde, einen Dienst, eine Einrichtung oder jede andere Stelle, der beziehungsweise dem personenbezogene Daten offengelegt oder bereitgestellt werden;

f bedeutet ‚Auftragsverarbeiter' eine natürliche oder juristische Person, eine Behörde, einen Dienst, eine Einrichtung oder jede andere Stelle, die beziehungsweise der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet."

Artikel 4

1 Artikel 3 Absatz 1 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Jede Vertragspartei verpflichtet sich, dieses Übereinkommen auf die unter ihrer Hoheitsgewalt erfolgenden Datenverarbeitungen im öffentlichen und im privaten Sektor anzuwenden und dadurch das Recht jedes Menschen auf Schutz seiner personenbezogenen Daten zu sichern."

2 Artikel 3 Absatz 2 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„2 Dieses Übereinkommen findet keine Anwendung auf die Datenverarbeitung, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird."

3 In Artikel 3 des Übereinkommens werden die Absätze 3 bis 6 gestrichen.

Artikel 5

Die Überschrift des Kapitels II des Übereinkommens wird durch folgende Überschrift ersetzt:

„**Kapitel II – Grundsätze für den Schutz personenbezogener Daten**".

Artikel 6

1 Artikel 4 Absatz 1 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Jede Vertragspartei trifft in ihrem Recht die erforderlichen Maßnahmen, um den Bestimmungen dieses Übereinkommens Wirksamkeit zu verleihen und seine wirksame Anwendung sicherzustellen."

2 Artikel 4 Absatz 2 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„2 Diese Maßnahmen werden von jeder Vertragspartei getroffen und müssen bis zum Zeitpunkt der Ratifikation dieses Übereinkommens oder des Beitritts dazu in Kraft getreten sein."

3 Nach Artikel 4 Absatz 2 des Übereinkommens wird ein neuer Absatz angefügt:

„3 Jede Vertragspartei verpflichtet sich,

a dem in Kapitel VI vorgesehenen Übereinkommensausschuss zu ermöglichen, die Wirksamkeit der von ihr in ihrem Recht getroffenen Maßnahmen zu bewerten, mit denen den Bestimmungen dieses Übereinkommens Wirksamkeit verliehen werden soll, und

b diesen Bewertungsprozess aktiv zu unterstützen."

Artikel 7

1 Die Überschrift des Artikels 5 wird durch folgende Überschrift ersetzt:

„**Artikel 5 – Rechtmäßigkeit der Datenverarbeitung und Qualität der Daten**".

2 Der Wortlaut des Artikels 5 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Die Datenverarbeitung muss in Bezug auf den verfolgten rechtmäßigen Zweck verhältnismäßig sein und in allen Phasen der Verarbeitung ein ausgewogenes Verhältnis zwischen allen betroffenen Interessen, ob öffentlich oder privat, und den zu wahrenden Rechten und Freiheiten widerspiegeln.

2 Jede Vertragspartei sieht vor, dass die Datenverarbeitung auf der Grundlage der freiwilligen, für den konkreten Fall, in informierter Weise und unmissverständlich erfolgten Einwilligung des Betroffenen oder auf einer anderen rechtmäßigen, gesetzlich geregelten Grundlage durchgeführt werden kann.

3 Personenbezogene Daten, die verarbeitet werden, müssen auf rechtmäßige Weise verarbeitet werden.

4 Personenbezogene Daten, die verarbeitet werden:

a müssen nach Treu und Glauben und in einer transparenten Weise verarbeitet werden;

b müssen für eindeutige, festgelegte und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden; vorbehaltlich geeigneter Garantien ist eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke mit solchen Zwecken vereinbar;

c müssen den Zwecken, für die sie verarbeitet werden, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen;

d müssen sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sein;

e müssen so aufbewahrt werden, dass die Betroffenen nicht länger identifiziert werden können, als es die Zwecke, für die sie verarbeitet werden, erfordern."

Artikel 8

Der Wortlaut des Artikels 6 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Die Verarbeitung von

– genetischen Daten,

– personenbezogenen Daten bezüglich Straftaten, Strafverfahren und Strafurteilen und damit zusammenhängenden Sicherungsmaßnahmen,

– biometrischen Daten, anhand derer eine Person eindeutig identifizierbar ist,

– personenbezogenen Daten, aus denen Informationen über die rassische oder ethnische Herkunft, politische Meinungen, die Gewerkschaftszugehörigkeit, religiöse oder sonstige Überzeugungen, die Gesundheit oder das Sexualleben hervorgehen,

ist nur erlaubt, wenn es ergänzend zu den Garantien dieses Übereinkommens geeignete gesetzlich verankerte Garantien gibt.

2 Diese Garantien müssen vor den Risiken schützen, die eine Verarbeitung sensibler Daten für die Interessen, Rechte und Grundfreiheiten des Betroffenen darstellen kann, insbesondere vor dem Risiko einer Diskriminierung."

Artikel 9

Der Wortlaut des Artikels 7 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Jede Vertragspartei sieht vor, dass der Verantwortliche und gegebenenfalls der Auftragsverarbeiter gegen Risiken, wie unbeabsichtigten oder unbefugten Zugang zu oder Vernichtung, Verlust, Verwendung, Veränderung oder Offenlegung von personenbezogenen Daten, geeignete Sicherheitsvorkehrungen trifft.

2 Jede Vertragspartei sieht vor, dass der Verantwortliche die Verletzungen des Datenschutzes, die einen schweren Eingriff in die Rechte und Grundfreiheiten von Betroffenen darstellen können, unverzüglich zumindest der zuständigen Aufsichtsbehörde nach Artikel 15 melden muss."

Artikel 10

Nach Artikel 7 des Übereinkommens wird ein neuer Artikel 8 mit folgender Überschrift und folgendem Wortlaut eingefügt:

„**Artikel 8 – Transparenz der Verarbeitung**

1 Jede Vertragspartei sieht vor, dass der Verantwortliche den Betroffenen Folgendes mitteilt:

a seine Identität und seinen gewöhnlichen Wohnsitz oder seine gewöhnliche Niederlassung;

b die Rechtsgrundlage und die Zwecke der beabsichtigten Datenverarbeitung;

c die Arten personenbezogener Daten, die verarbeitet werden;

d gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

e die Mittel zur Ausübung der in Artikel 9 dargelegten Rechte

sowie alle notwendigen zusätzlichen Informationen, um eine faire und transparente Verarbeitung der personenbezogenen Daten sicherzustellen.

2 Absatz 1 findet keine Anwendung, wenn der Betroffene bereits über diese Informationen verfügt.

3 Werden die personenbezogenen Daten nicht unmittelbar bei den Betroffenen erhoben, so ist der Verantwortliche nicht verpflichtet, solche Informationen mitzuteilen, sofern die Verarbeitung ausdrücklich gesetzlich vorgeschrieben ist oder wenn sich dies als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist.“

Artikel 11

1 Der bisherige Artikel 8 des Übereinkommens wird zu Artikel 9 und seine Überschrift wird durch folgende Überschrift ersetzt:

„**Artikel 9 – Rechte des Betroffenen**“.

2 Der Wortlaut des Artikels 8 (neuer Artikel 9) des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Jede natürliche Person hat das Recht:

a nicht einer ausschließlich auf einer automatisierten Datenverarbeitung beruhenden Entscheidung, die sich erheblich auf sie auswirkt, unterworfen zu werden, ohne dass ihre Auffassungen berücksichtigt werden;

b auf Antrag, in angemessenen Abständen und ohne übermäßige Verzögerung oder Kosten eine Bestätigung über die Verarbeitung von sie betreffenden personenbezogenen Daten, Mitteilung über die verarbeiteten Daten in verständlicher Form, alle verfügbaren Informationen über den Ursprung und die Aufbewahrungsfrist der Daten sowie alle sonstigen Informationen zu erhalten, zu deren Bereitstellung der Verantwortliche verpflichtet ist, um die Transparenz der Verarbeitung nach Artikel 8 Absatz 1 sicherzustellen;

c auf Antrag Kenntnis über die der Datenverarbeitung zugrunde liegenden Überlegungen zu erlangen, wenn die Ergebnisse dieser Verarbeitung auf die Person Anwendung finden;

d jederzeit aus sich aus ihrer Situation ergebenden Gründen gegen die Verarbeitung von sie betreffenden personenbezogenen Daten Widerspruch einzulegen, sofern der Verantwortliche nicht nachweisen kann, dass berechtigte Gründe für die Verarbeitung bestehen, welche die Interessen oder Rechte und Grundfreiheiten der Person überwiegen;

e auf Antrag, unentgeltlich und ohne übermäßige Verzögerung die Berichtigung beziehungsweise Löschung solcher Daten zu erwirken, wenn die Daten im Widerspruch zu den Bestimmungen dieses Übereinkommens verarbeitet werden oder worden sind;

f ein Rechtsmittel nach Artikel 12 einzulegen, wenn ihre Rechte aufgrund dieses Übereinkommens verletzt worden sind;

g unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnsitz bei der Ausübung ihrer Rechte aufgrund dieses Übereinkommens die Unterstützung einer Aufsichtsbehörde im Sinne des Artikels 15 in Anspruch zu nehmen.

2 Absatz 1 Buchstabe a findet keine Anwendung, wenn die Entscheidung aufgrund eines Gesetzes, dem der Verantwortliche unterliegt, zulässig ist und dieses Gesetz geeignete Maßnahmen zum Schutz der Rechte, Freiheiten und berechtigten Interessen des Betroffenen enthält.“

Artikel 12

Nach dem neuen Artikel 9 des Übereinkommens wird ein neuer Artikel 10 mit folgender Überschrift und folgendem Wortlaut eingefügt:

„**Artikel 10 – Zusätzliche Verpflichtungen**

1 Jede Vertragspartei sieht vor, dass die Verantwortlichen und gegebenenfalls die Auftragsverarbeiter alle geeigneten Maßnahmen treffen, um die Verpflichtungen dieses Übereinkommens einzuhalten, und dass sie vorbehaltlich der nach Artikel 11 Absatz 3 angenommenen innerstaatlichen Rechtsvorschriften, insbesondere gegenüber der in Artikel 15 vorgesehenen zuständigen Aufsichtsbehörde nachweisen können, dass die in ihrer Verantwortung durchgeführte Datenverarbeitung im Einklang mit den Bestimmungen dieses Übereinkommens steht.

2 Jede Vertragspartei sieht vor, dass die Verantwortlichen und gegebenenfalls die Auftragsverarbeiter die wahrscheinlichen Auswirkungen der beabsichtigen Datenverarbeitung auf die Rechte und Grundfreiheiten der Betroffenen vor dem Beginn der Datenverarbeitung untersuchen und die Datenverarbeitung so gestalten, dass das Risiko des Eingriffs in diese Rechte und Grundfreiheiten verhindert oder minimiert wird.

3 Jede Vertragspartei sieht vor, dass die Verantwortlichen und gegebenenfalls die Auftragsverarbeiter technische und organisatorische Maßnahmen treffen, die die Auswirkungen des Rechts auf den Schutz personenbezogener Daten in allen Phasen der Datenverarbeitung berücksichtigen.

4 Jede Vertragspartei kann im Hinblick auf die für die Interessen, Rechte und Grundfreiheiten der Betroffenen entstehenden Risiken in den Rechtsvorschriften, mit denen diesem Übereinkommen Wirksamkeit verliehen wird, die Anwendung der Absätze 1, 2 und 3 entsprechend der Beschaffenheit und dem Umfang der Daten, der Art, dem Umfang und dem Zweck ihrer Verarbeitung und gegebenenfalls der Größe des Verantwortlichen oder Auftragsverarbeiters anpassen."

Artikel 13

Die bisherigen Artikel 9 bis 12 des Übereinkommens werden die Artikel 11 bis 14 des Übereinkommens.

Artikel 14

Der Wortlaut des Artikels 9 (neuer Artikel 11) des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Ausnahmen von den Bestimmungen dieses Kapitels sind nicht zulässig, abgesehen von Ausnahmen von 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 Grundfreiheiten wahrt und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt

a zum Schutz der nationalen Sicherheit, für die Landesverteidigung, für die öffentliche Sicherheit, für wichtige wirtschaftliche und finanzielle Interessen des Staates, für die Unparteilichkeit und Unabhängigkeit der Justiz oder für die Verhütung, Ermittlung und Verfolgung von Straftaten und die Strafvollstreckung sowie für sonstige wichtige Ziele des allgemeinen öffentlichen Interesses;

b zum Schutz des Betroffenen oder der Rechte und Grundfreiheiten anderer Personen, insbesondere der Meinungsfreiheit.

2 In Bezug auf die Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken können Anwendungsbeschränkungen der Artikel 8 und 9 gesetzlich vorgesehen werden, wenn keine erkennbare Gefahr des Eingriffs in die Rechte und Grundfreiheiten von Betroffenen besteht.

3 Zusätzlich zu den nach Absatz 1 zulässigen Ausnahmen kann jede Vertragspartei im Hinblick auf Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung Ausnahmen von Artikel 4 Absatz 3, Artikel 14 Absätze 5 und 6 und Artikel 15 Absatz 2 Buchstaben a, b, c und d durch Gesetz und nur in dem Maße vorsehen, wie dies in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zur Erfüllung eines solchen Zwecks darstellt.

Dies berührt nicht das Erfordernis, dass Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung einer unabhängigen und wirksamen Prüfung und Aufsicht nach Maßgabe der innerstaatlichen Rechtsvorschriften der jeweiligen Vertragspartei unterliegen müssen."

Artikel 15

Der Wortlaut des Artikels 10 (neuer Artikel 12) des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„Jede Vertragspartei verpflichtet sich, geeignete gerichtliche und außergerichtliche Sanktionen und Rechtsmittel für Verstöße gegen die Bestimmungen dieses Übereinkommens festzulegen."

Artikel 16

Die Überschrift des Kapitels III wird durch folgende Überschrift ersetzt:

„**Kapitel III – Grenzüberschreitender Verkehr personenbezogener Daten**".

Artikel 17

1 Die Überschrift des Artikels 12 (neuer Artikel 14) des Übereinkommens wird durch folgende Überschrift ersetzt:

„**Artikel 14 – Grenzüberschreitender Verkehr personenbezogener Daten**".

2 Der Wortlaut des Artikels 12 (neuer Artikel 14) des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Eine Vertragspartei darf zum alleinigen Zweck des Schutzes personenbezogener Daten die Weitergabe solcher Daten an einen Empfänger, der der Hoheitsgewalt einer anderen Vertragspartei des Übereinkommens untersteht, nicht verbieten oder von einer besonderen Genehmigung abhängig machen. Die Vertragspartei kann dies jedoch tun, wenn eine tatsächliche und ernste Gefahr besteht, dass die Weitergabe an eine andere Vertragspartei, oder von dieser anderen Vertragspartei an eine Nichtvertragspartei, zu einer Umgehung der Bestimmungen des Übereinkommens führen würde. Eine Vertragspartei kann dies ebenfalls tun, wenn sie durch harmonisierte gemeinsame Schutzvorschriften von Staaten, die einer regionalen internationalen Organisation angehören, gebunden ist.

2 Untersteht der Empfänger der Hoheitsgewalt eines Staates oder befindet er sich im Zuständigkeitsbereich einer internationalen Organisation, der beziehungsweise die nicht Vertragspartei dieses Übereinkommens ist, so darf die Weitergabe personenbezogener Daten nur erfolgen, wenn ein angemessenes Schutzniveau auf der Grundlage der Bestimmungen dieses Übereinkommens sichergestellt ist.

3 Ein angemessenes Schutzniveau kann sichergestellt werden durch

a das Recht dieses Staates oder dieser internationalen Organisation, einschließlich der anwendbaren völkerrechtlichen Verträge oder Übereinkünfte, oder

b Ad-hoc-Garantien oder genehmigte standardisierte Garantien aufgrund rechtlich bindender und durchsetzbarer Instrumente, die von den an der Weitergabe und Weiterverarbeitung beteiligten Personen angenommen worden sind und umgesetzt werden.

4 Ungeachtet der Absätze 1 bis 3 kann jede Vertragspartei vorsehen, dass personenbezogene Daten weitergegeben werden dürfen, wenn

a der Betroffene ausdrücklich, für den konkreten Fall und freiwillig eingewilligt hat, nachdem er über die Gefahren aufgeklärt wurde, die bei Fehlen geeigneter Garantien entstehen können, oder

b dies wegen spezifischer Interessen des Betroffenen im Einzelfall erforderlich ist oder

c überwiegende berechtigte Interessen, insbesondere wichtige öffentliche Interessen, gesetzlich vorgesehen sind und eine solche Weitergabe in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt oder

d dies in einer demokratischen Gesellschaft im Hinblick auf die Meinungsfreiheit eine notwendige und verhältnismäßige Maßnahme darstellt.

5 Jede Vertragspartei sieht vor, dass der zuständigen Aufsichtsbehörde im Sinne des Artikels 15 dieses Übereinkommens alle sachdienlichen Informationen hinsichtlich der in Absatz 3 Buchstabe b genannten Weitergabe von Daten sowie auf Anfrage hinsichtlich der in Absatz 4 Buchstaben b und c genannten Daten zur Verfügung gestellt werden.

6 Jede Vertragspartei sieht ebenfalls vor, dass die Aufsichtsbehörde verlangen darf, dass die Person, die Daten weitergibt, die Wirksamkeit der Garantien oder das Vorhandensein überwiegender berechtigter Interessen nachweist und dass die Aufsichtsbehörde eine solche Datenweitergabe verbieten, aussetzen oder an Bedingungen knüpfen darf, um die Rechte und Grundfreiheiten der Betroffenen zu schützen.“

3 Eingegliedert in den Wortlaut des Artikels 12 (neuer Artikel 14) des Übereinkommens sind die Bestimmungen des Artikels 2 des Zusatzprotokolls von 2001 betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (SEV Nr. 181) über grenzüberschreitenden Verkehr personenbezogener Daten an einen Empfänger, der nicht der Hoheitsgewalt einer Vertragspartei des Übereinkommens untersteht.

Artikel 18

Nach Kapitel III des Übereinkommens wird ein neues Kapitel IV mit folgender Überschrift eingefügt:

„**Kapitel IV – Aufsichtsbehörden**“.

Artikel 19

Ein neuer Artikel 15 gliedert Artikel 1 des Zusatzprotokolls von 2001 (SEV Nr. 181) ein; er hat folgenden Wortlaut:

„**Artikel 15 – Aufsichtsbehörden**

1 Jede Vertragspartei sieht vor, dass eine oder mehrere Behörden dafür zuständig sind, die Einhaltung der Bestimmungen dieses Übereinkommens sicherzustellen.

2 Zu diesem Zweck:

a haben diese Behörden Untersuchungs- und Einwirkungsbefugnisse;

b erfüllen sie die Aufgaben im Zusammenhang mit der in Artikel 14 vorgesehenen Weitergabe von Daten, insbesondere die Genehmigung standardisierter Garantien;

c haben sie die Befugnis, Entscheidungen im Hinblick auf Verstöße gegen die Bestimmungen dieses Übereinkommens zu treffen, und können insbesondere verwaltungsrechtliche Sanktionen verhängen;

d haben sie die Befugnis, bei Verstößen gegen die Bestimmungen dieses Übereinkommens gerichtliche Schritte einzuleiten oder Verstöße bei den zuständigen Justizbehörden anzuzeigen;

e fördern sie

i das öffentliche Bewusstsein für ihre Aufgaben und Befugnisse sowie für ihre Tätigkeiten;

ii das öffentliche Bewusstsein für die Rechte der Betroffenen und die Wahrnehmung dieser Rechte;

iii das Bewusstsein bei den Verantwortlichen und den Auftragsverarbeitern für die ihnen aus diesem Übereinkommen entstehenden Pflichten;

besondere Aufmerksamkeit wird den Datenschutzrechten von Kindern und anderen schutzbedürftigen Personen gewidmet.

3 Die zuständigen Aufsichtsbehörden werden bei allen Vorschlägen für Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten vorsehen, zu Rate gezogen.

4 Jede zuständige Aufsichtsbehörde befasst sich mit Anträgen und Beschwerden von Betroffenen hinsichtlich ihrer Datenschutzrechte und hält die Betroffenen über den Fortgang auf dem Laufenden.

5 Die Aufsichtsbehörden handeln bei der Wahrnehmung ihrer Aufgaben und Befugnisse in völliger Unabhängigkeit und Unparteilichkeit; dabei holen sie Weisungen weder ein noch nehmen sie sie entgegen.

6 Jede Vertragspartei stellt sicher, dass die Aufsichtsbehörden mit den zur wirksamen Erfüllung ihrer Aufgaben und Wahrnehmung ihrer Befugnisse nötigen Ressourcen ausgestattet werden.

7 Jede Aufsichtsbehörde erstellt und veröffentlicht einen periodischen Tätigkeitsbericht.

8 Die Mitglieder und das Personal der Aufsichtsbehörden unterliegen der Verpflichtung zur Verschwiegenheit im Hinblick auf vertrauliche Informationen, zu denen sie bei der Erfüllung ihrer Aufgaben und der Wahrnehmung ihrer Befugnisse Zugang haben oder hatten.

9 Gegen Entscheidungen der Aufsichtsbehörden steht der gerichtliche Rechtsweg **(1)** offen.

10 Die Aufsichtsbehörden sind nicht für Verarbeitungen zuständig, die von Organen im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen werden.“

(1) Für die Bundesrepublik Deutschland heißt es nur „Rechtsweg“.

Artikel 20

1 Die Kapitel IV bis VII des Übereinkommens werden umnummeriert zu Kapitel V bis VIII des Übereinkommens.

2 Die Überschrift des Kapitels V wird durch die Überschrift „**Kapitel V – Zusammenarbeit und gegenseitige Hilfeleistung**“ ersetzt

3 Ein neuer Artikel 17 wird eingefügt; die bisherigen Artikel 13 bis 27 des Übereinkommens werden die Artikel 16 bis 31 des Übereinkommens.

Artikel 21

1 Die Überschrift des Artikels 13 (neuer Artikel 16) des Übereinkommens wird durch folgende Überschrift ersetzt:

„**Artikel 16 – Benennung von Aufsichtsbehörden**“.

2 Artikel 13 (neuer Artikel 16) Absatz 1 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Die Vertragsparteien verpflichten sich, zusammenzuarbeiten und einander bei der Durchführung dieses Übereinkommens Hilfe zu leisten.“

3 Artikel 13 (neuer Artikel 16) Absatz 2 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„2 Zu diesem Zweck

a benennt jede Vertragspartei eine oder mehrere Aufsichtsbehörden im Sinne des Artikels 15, deren Bezeichnung und Anschrift sie dem Generalsekretär des Europarats mitteilt;

b gibt jede Vertragspartei, die mehrere Aufsichtsbehörden benannt hat, in der unter Buchstabe a genannten Mitteilung die Zuständigkeit jeder dieser Behörden an.“

4 Artikel 13 (neuer Artikel 16) Absatz 3 des Übereinkommens wird gestrichen.

Artikel 22

Nach dem neuen Artikel 16 des Übereinkommens wird ein neuer Artikel 17 mit folgender Überschrift und folgendem Wortlaut eingefügt:

„**Artikel 17 – Formen der Zusammenarbeit**

1 Die Aufsichtsbehörden arbeiten miteinander in dem Maße zusammen, wie es zur Erfüllung ihrer Aufgaben und Wahrnehmung ihrer Befugnisse notwendig ist, indem sie insbesondere

a einander durch den Austausch sachdienlicher und nützlicher Informationen Hilfe leisten und miteinander unter der Bedingung, dass im Hinblick auf den Schutz personenbezogener Daten alle Vorschriften und Garantien dieses Übereinkommens eingehalten werden, zusammenarbeiten;

b ihre Untersuchungen oder ihre Einwirkung abstimmen oder gemeinsame Maßnahmen durchführen;

c Informationen und Unterlagen über ihr Recht und ihre Verwaltungspraxis im Zusammenhang mit dem Datenschutz zur Verfügung stellen.

2 Zu den in Absatz 1 genannten Informationen zählen nicht die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, es sei denn, diese sind für die Zusammenarbeit von entscheidender Bedeutung oder der Betroffene hat ausdrücklich, für den konkreten Fall, freiwillig und in informierter Weise in ihre Bereitstellung eingewilligt.

3 Um ihre Zusammenarbeit zu organisieren und ihre in den Absätzen 1 und 2 vorgesehenen Aufgaben zu erfüllen, bilden die Aufsichtsbehörden der Vertragsparteien ein Netzwerk."

Artikel 23

1 Die Überschrift des Artikels 14 (neuer Artikel 18) des Übereinkommens wird durch folgende Überschrift ersetzt:

„**Artikel 18 – Unterstützung von Betroffenen**".

2 Der Wortlaut des Artikels 14 (neuer Artikel 18) des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Jede Vertragspartei unterstützt jeden Betroffenen ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts bei der Ausübung seiner Rechte nach Artikel 9 dieses Übereinkommens.

2 Ein im Hoheitsgebiet einer anderen Vertragspartei wohnender Betroffener hat die Möglichkeit, seinen Antrag über die benannte Aufsichtsbehörde dieser Vertragspartei stellen.

3 Der Antrag auf Unterstützung muss alle erforderlichen Angaben enthalten, insbesondere über

a den Namen, die Anschrift und alle anderen für die Identifizierung des den Antrag stellenden Betroffenen erheblichen Einzelheiten;

b die Datenverarbeitung, auf die sich der Antrag bezieht, oder den dafür Verantwortlichen;

c den Zweck des Antrags."

Artikel 24

1 Die Überschrift des Artikels 15 (neuer Artikel 19) des Übereinkommens wird durch folgende Überschrift ersetzt:

„**Artikel 19 – Garantien**".

2 Der Wortlaut des Artikels 15 (neuer Artikel 19) des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Hat eine Aufsichtsbehörde einer Vertragspartei von einer Aufsichtsbehörde einer anderen Vertragspartei Auskünfte erhalten, die einem Antrag auf Unterstützung dienen oder Antwort auf ein eigenes Ersuchen geben, so darf sie diese Auskünfte nur zu den Zwecken verwenden, die dem Antrag oder Ersuchen zugrunde liegen.

2 Es ist einer Aufsichtsbehörde in keinem Fall erlaubt, im Namen eines Betroffenen von sich aus und ohne dessen ausdrückliche Einwilligung einen Antrag auf Unterstützung zu stellen.“

Artikel 25

1 Die Überschrift des Artikels 16 (neuer Artikel 20) des Übereinkommens wird durch folgende Überschrift ersetzt:

„**Artikel 20 – Ablehnung von Ersuchen**“.

2 Der einleitende Halbsatz des Artikels 16 (neuer Artikel 20) des Übereinkommens wird durch folgenden Halbsatz ersetzt:

„Eine Aufsichtsbehörde, an die nach Artikel 17 ein Ersuchen gerichtet wird, kann nur ablehnen, diesem stattzugeben, wenn“.

3 Artikel 16 (neuer Artikel 20) Buchstabe a des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„a das Ersuchen mit ihren Befugnissen nicht vereinbar ist;“.

[Als Folge der Neufassung des einleitenden Halbsatzes des Artikels 16 wird die deutsche Übersetzung des Artikels 16 (neuer Artikel 20) Buchstabe b des Übereinkommens wie folgt gefasst:

„b das Ersuchen den Bestimmungen dieses Übereinkommens nicht entspricht;“.]

4 Artikel 16 (neuer Artikel 20) Buchstabe c des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„c seine Erfüllung mit der Souveränität, der nationalen Sicherheit oder der öffentlichen Ordnung der Vertragspartei, die sie benannt hat, oder mit den Rechten und Grundfreiheiten der Personen, die der Hoheitsgewalt dieser Vertragspartei unterstehen, nicht vereinbar wäre.“

Artikel 26

1 [Änderung ohne Auswirkung auf die deutsche Übersetzung.]

2 Artikel 17 (neuer Artikel 21) Absatz 1 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Für die Zusammenarbeit und Hilfe, welche die Vertragsparteien einander nach Artikel 17 gewähren, und für Unterstützung, die sie Betroffenen nach den Artikeln 9 und 18 leisten, werden keine Auslagen oder Gebühren außer für Sachverständige und Dolmetscher erhoben. Diese Auslagen oder Gebühren werden von der ersuchenden Vertragspartei getragen.“

3 [Änderung ohne Auswirkung auf die deutsche Übersetzung.]

Artikel 27

Die Überschrift des Kapitels V (neues Kapitel VI) des Übereinkommens wird durch folgende Überschrift ersetzt:

„**Kapitel VI – Übereinkommensausschuss**“

Artikel 28

1 In Artikel 18 (neuer Artikel 22) Absatz 1 des Übereinkommens werden die Wörter „Beratender Ausschuss“ durch das Wort „Übereinkommensausschuss“ ersetzt.

2 Artikel 18 (neuer Artikel 22) Absatz 3 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„3 Der Übereinkommensausschuss kann mit einer Zweidrittelmehrheit der Vertreter der Vertragsparteien beschließen, einen Beobachter zur Teilnahme an seinen Sitzungen einzuladen.“

3 Nach Artikel 18 (neuer Artikel 22) Absatz 3 des Übereinkommens wird ein neuer Absatz 4 angefügt:

„4 Eine Vertragspartei, die nicht Mitglied des Europarats ist, trägt nach Maßgabe der vom Ministerkomitee in Abstimmung mit der Vertragspartei festgelegten Modalitäten zur Finanzierung der Tätigkeiten des Übereinkommensausschusses bei.“

Artikel 29

1 Im einleitenden Halbsatz des Artikels 19 (neuer Artikel 23) des Übereinkommens werden die Wörter „Beratender Ausschuss“ durch das Wort „Übereinkommensausschuss“ ersetzt.

2 In Artikel 19 (neuer Artikel 23) Buchstabe a des Übereinkommens wird das Wort „Vorschläge“ durch das Wort „Empfehlungen“ ersetzt.

3 In Artikel 19 (neuer Artikel 23) Buchstabe b des Übereinkommens wird der Verweis auf „Artikel 21“ und in Artikel 19 (neuer Artikel 23) Buchstabe c des Übereinkommens wird der Verweis auf „Artikel 21 Absatz 3“ durch einen Verweis auf „Artikel 25“ beziehungsweise auf „Artikel 25 Absatz 3“ ersetzt.

4 Der Wortlaut des Artikels 19 (neuer Artikel 23) Buchstabe d des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„d kann zu allen Fragen im Zusammenhang mit der Auslegung oder Anwendung dieses Übereinkommens Stellung nehmen;“.

5 Nach Artikel 19 (neuer Artikel 23) Buchstabe d des Übereinkommens werden die folgenden neuen Buchstaben angefügt:

„e erarbeitet vor jedem neuen Beitritt zum Übereinkommen eine Stellungnahme für das Ministerkomitee hinsichtlich des Schutzniveaus für personenbezogene Daten, das der Beitrittskandidat gewährleistet, und empfiehlt gegebenenfalls zu treffende Maßnahmen zur Einhaltung der Bestimmungen dieses Übereinkommens;

f kann auf Ersuchen eines Staates oder einer internationalen Organisation bewerten, ob das dort gewährte Schutzniveau für personenbezogene Daten mit den Bestimmungen dieses Übereinkommens im Einklang steht und nötigenfalls zu treffende Maßnahmen zur Einhaltung der Bestimmungen dieses Übereinkommens empfehlen;

g kann Modelle für die in Artikel 14 genannten standardisierten Garantien entwickeln oder genehmigen;

h überprüft die Durchführung dieses Übereinkommens durch die Vertragsparteien und empfiehlt Maßnahmen für den Fall, dass eine Vertragspartei das Übereinkommen nicht einhält;

i ermöglicht nötigenfalls die gütliche Beilegung aller mit der Anwendung des Übereinkommens verbundenen Schwierigkeiten."

Artikel 30

Der Wortlaut des Artikels 20 (neuer Artikel 24) des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Der Übereinkommensausschuss wird vom Generalsekretär des Europarats einberufen. Seine erste Sitzung findet innerhalb von zwölf Monaten nach Inkrafttreten dieses Übereinkommens statt. Danach tritt er mindestens einmal jährlich sowie immer dann zusammen, wenn ein Drittel der Vertreter der Vertragsparteien dies verlangt.

2 Im Anschluss an jede Sitzung unterbreitet der Übereinkommensausschuss dem Ministerkomitee des Europarats einen Bericht über seine Arbeit und die Wirksamkeit dieses Übereinkommens.

3 Die Abstimmungsmodalitäten im Übereinkommensausschuss sind in den Elementen der Geschäftsordnung enthalten, die den Anhang des Protokolls SEV Nr. 223 bilden.

4 Der Übereinkommensausschuss erstellt die anderen Elemente seiner Geschäftsordnung und legt insbesondere die Verfahren für die Bewertung und Überprüfung nach Artikel 4 Absatz 3 und Artikel 23 Buchstaben e, f und h auf der Grundlage objektiver Kriterien fest."

Artikel 31

1 Der Wortlaut des Artikels 21 (neuer Artikel 25) Absätze 1 bis 4 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Änderungen dieses Übereinkommens können von einer Vertragspartei, vom Ministerkomitee des Europarats oder vom Übereinkommensausschuss vorgeschlagen werden.

2 Jeder Änderungsvorschlag wird den Vertragsparteien dieses Übereinkommens, den anderen Mitgliedstaaten des Europarats, der Europäischen Union und jedem Nichtmitgliedstaat oder jeder internationalen Organisation, die nach Artikel 27 zum Beitritt zu diesem Übereinkommen eingeladen worden sind, vom Generalsekretär des Europarats übermittelt.

3 Darüber hinaus wird jede von einer Vertragspartei oder vom Ministerkomitee vorgeschlagene Änderung dem Übereinkommensausschuss übermittelt; dieser teilt dem Ministerkomitee seine Stellungnahme zu der vorgeschlagenen Änderung mit.

4 Das Ministerkomitee prüft die vorgeschlagene Änderung und jede Stellungnahme des Übereinkommensausschusses und kann die Änderung genehmigen.“

2 Nach Artikel 21 (neuer Artikel 25) Absatz 6 des Übereinkommens wird folgender neuer Absatz 7 angefügt:

„7 Darüber hinaus kann das Ministerkomitee nach Konsultation des Übereinkommensausschusses einstimmig beschließen, dass eine bestimmte Änderung nach Ablauf eines Zeitabschnitts von drei Jahren nach dem Tag, an dem sie zur Annahme vorgelegt wurde, in Kraft tritt, es sei denn, eine Vertragspartei hat dem Generalsekretär des Europarats einen Einwand gegen das Inkrafttreten notifiziert. Wurde ein solcher Einwand notifiziert, so tritt die Änderung am ersten Tag des Monats nach dem Tag in Kraft, an dem die Vertragspartei des Übereinkommens, die den Einwand notifiziert hat, ihre Annahmeurkunde beim Generalsekretär des Europarats hinterlegt hat.“

Artikel 32

1 Der Wortlaut des Artikels 22 (neuer Artikel 26) Absatz 1 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Dieses Übereinkommen liegt für die Mitgliedstaaten des Europarats und die Europäische Union zur Unterzeichnung auf. Es bedarf der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.“

2 In Artikel 22 (neuer Artikel 26) Absatz 3 des Übereinkommens werden die Wörter „jeden Mitgliedstaat, der“ durch die Wörter „jede Vertragspartei, die“ ersetzt.

Artikel 33

Die Überschrift und der Wortlaut des Artikels 23 (neuer Artikel 27) des Übereinkommens werden durch folgende Überschrift und folgenden Wortlaut ersetzt:

„**Artikel 27 – Beitritt von Nichtmitgliedstaaten oder internationalen Organisationen**

1 Nach Inkrafttreten dieses Übereinkommens kann das Ministerkomitee des Europarats nach Konsultation der Vertragsparteien dieses Übereinkommens und mit deren einhelliger Zustimmung sowie unter Berücksichtigung der nach Artikel 23 Buchstabe e vom Übereinkommensausschuss erarbeiteten Stellungnahme durch einen mit der in Artikel 20 Buchstabe d der Satzung des Europarats vorgesehenen Mehrheit und mit einhelliger Zustimmung der Vertreter der Vertragsstaaten, die Anspruch auf einen Sitz im Ministerkomitee haben, gefassten Beschluss jeden Nichtmitgliedstaat des Europarats oder eine internationale Organisation einladen, diesem Übereinkommen beizutreten.

2 Für alle Staaten oder internationale Organisationen, die diesem Übereinkommen nach Absatz 1 beitreten, tritt das Übereinkommen am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegung der Beitrittsurkunde beim Generalsekretär des Europarats folgt.“

Artikel 34

Der Wortlaut des Artikels 24 (neuer Artikel 28) Absätze 1 und 2 des Übereinkommens wird durch folgenden Wortlaut ersetzt:

„1 Jeder Staat, die Europäische Union oder eine sonstige internationale Organisation kann bei der Unterzeichnung oder bei der Hinterlegung der Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde einzelne oder mehrere Hoheitsgebiete bezeichnen, auf die dieses Übereinkommen Anwendung findet.

2 Jeder Staat, die Europäische Union oder eine sonstige internationale Organisation kann jederzeit danach durch eine an den Generalsekretär des Europarats gerichtete Erklärung die Anwendung dieses Übereinkommens auf jedes weitere in der Erklärung bezeichnete Hoheitsgebiet erstrecken. Das Übereinkommen tritt für dieses Hoheitsgebiet am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Erklärung beim Generalsekretär folgt."

Artikel 35

1 Im einleitenden Halbsatz des Artikels 27 (neuer Artikel 31) des Übereinkommens werden die Wörter „jedem Staat, der" durch die Wörter „jeder Vertragspartei, die" ersetzt.

2 Unter Buchstabe c wird der Verweis „nach den Artikeln 22, 23 und 24" durch den Verweis „nach den Artikeln 26, 27 und 28" ersetzt.

Artikel 36 – Unterzeichnung, Ratifikation und Beitritt

1 Dieses Protokoll liegt für die Vertragsstaaten des Übereinkommens zur Unterzeichnung auf. Es bedarf der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.

2 Nachdem dieses Protokoll zur Unterzeichnung aufgelegt wurde und bevor es in Kraft tritt, drückt jeder andere Staat seine Zustimmung, durch dieses Protokoll gebunden zu sein, aus, indem er ihm beitritt. Ein Staat kann nicht Vertragspartei des Übereinkommens werden, ohne gleichzeitig diesem Protokoll beizutreten.

Artikel 37 – Inkrafttreten

1 Dieses Protokoll tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem alle Vertragsparteien des Übereinkommens nach Artikel 36 Absatz 1 ihre Zustimmung ausgedrückt haben, durch das Protokoll gebunden zu sein.

2 Ist das Protokoll nicht nach Absatz 1 in Kraft getreten, so tritt es nach einem Zeitabschnitt von fünf Jahren nach dem Tag, an dem es zur Unterzeichnung aufgelegt wurde, für jene Staaten in Kraft, die nach Absatz 1 ihre Zustimmung ausgedrückt haben, durch das Protokoll gebunden zu sein, sofern dem Protokoll mindestens 38 Vertragsparteien angehören. Für die Vertragsparteien des Protokolls werden alle Bestimmungen des geänderten Übereinkommens unmittelbar mit Inkrafttreten wirksam.

3 Bis zum Inkrafttreten dieses Protokolls und unbeschadet der Bestimmungen über das Inkrafttreten und den Beitritt von Nichtmitgliedstaaten oder internationalen Organisationen kann eine Vertragspartei des Übereinkommens bei der Unterzeichnung dieses Protokolls oder jederzeit danach erklären, dass sie die Bestimmungen dieses Protokolls vorläufig anwenden wird. In diesem Fall werden die Bestimmungen dieses Protokolls nur in Bezug auf die anderen Vertragsparteien des Übereinkommens angewendet, die eine diesbezügliche Erklärung abgegeben haben. Eine solche Erklärung wird am ersten Tag des dritten Monats wirksam, der auf den Tag ihres Eingangs beim Generalsekretär des Europarats folgt.

4 Mit Inkrafttreten dieses Protokolls wird das Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (SEV Nr. 181) aufgehoben.

5 Mit Inkrafttreten dieses Protokolls werden die vom Ministerkomitee am 15. Juni 1999 in Straßburg genehmigten Änderungen des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten gegenstandslos.

Artikel 38 – Erklärungen im Zusammenhang mit dem Übereinkommen

Mit Inkrafttreten dieses Protokolls wird jede Erklärung einer Vertragspartei nach Artikel 3 des Übereinkommens unwirksam.

Artikel 39 – Vorbehalte

Vorbehalte zu diesem Protokoll sind nicht zulässig.

Artikel 40 – Notifikationen

Der Generalsekretär des Europarats notifiziert den Mitgliedstaaten des Europarats und jeder anderen Vertragspartei des Übereinkommens

a jede Unterzeichnung;

b jede Hinterlegung einer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde;

c den Zeitpunkt des Inkrafttretens dieses Protokolls nach Artikel 37;

d jede andere Handlung, Notifikation oder Mitteilung im Zusammenhang mit diesem Protokoll.

Zu Urkund dessen haben die hierzu gehörig befugten Unterzeichneten dieses Protokoll unterzeichnet.

Geschehen zu Straßburg am 10. Oktober 2018 in englischer und französischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist, in einer Urschrift, die im Archiv des Europarats hinterlegt wird. Der Generalsekretär des Europarats übermittelt allen Mitgliedstaaten des Europarats, anderen Vertragsparteien des Übereinkommens und allen zum Beitritt zum Übereinkommen eingeladenen Staaten beglaubigte Abschriften.

Anhang des Protokolls: Elemente der Geschäftsordnung des Übereinkommensausschusses

1 Jede Vertragspartei ist stimmberechtigt und hat eine Stimme.

2 Der Übereinkommensausschuss ist in einer Sitzung beschlussfähig, wenn eine Zweidrittelmehrheit der Vertreter der Vertragsparteien anwesend ist. Tritt das Änderungsprotokoll zum Übereinkommen nach Artikel 37 Absatz 2 des Protokolls in Kraft, bevor es für alle Vertragsstaaten des Übereinkommens in Kraft tritt, so ist der Übereinkommensausschuss in einer Sitzung beschlussfähig, wenn mindestens 34 Vertragsparteien des Protokolls vertreten sind.

3 Beschlüsse nach Artikel 23 erfordern eine Vierfünftelmehrheit. Beschlüsse nach Artikel 23 Buchstabe h erfordern eine Vierfünftelmehrheit einschließlich einer Mehrheit der Stimmen der Vertragsstaaten, die nicht Mitglied einer dem Übereinkommen als Vertragspartei angehörenden Organisation der regionalen Integration sind.

4 Fasst der Übereinkommensausschuss einen Beschluss nach Artikel 23 Buchstabe h, so darf die von der Überprüfung betroffene Vertragspartei nicht an der Abstimmung teilnehmen. Bezieht sich solch ein Beschluss auf eine Angelegenheit in der Zuständigkeit einer Organisation der regionalen Integration, dürfen weder die Organisation noch ihre Mitgliedstaaten an der Abstimmung teilnehmen.

5 Beschlüsse zu Verfahrensfragen erfordern eine einfache Mehrheit der Stimmen.

6 Organisationen der regionalen Integration können in Angelegenheiten, die in ihren Zuständigkeitsbereich fallen, ihr Stimmrecht im Übereinkommensausschuss mit der Zahl von Stimmen ausüben, die der Zahl ihrer Mitgliedstaaten entspricht, die Vertragsparteien des Übereinkommens sind. Macht einer dieser Mitgliedstaaten von seinem Stimmrecht Gebrauch, so darf die Organisation ihr Stimmrecht nicht ausüben.

7 Im Fall einer Abstimmung müssen alle Vertragsparteien über den Gegenstand und die Zeit der Abstimmung unterrichtet sein sowie darüber, ob die Vertragsparteien ihr Stimmrecht einzeln ausüben oder ob eine Organisation der regionalen Integration das Stimmrecht für ihre Mitgliedstaaten ausübt.

8 Der Übereinkommensausschuss kann seine Geschäftsordnung später mit einer Zweidrittelmehrheit ändern; ausgenommen sind die Abstimmungsmodalitäten, die nur durch einstimmigen Beschluss der Vertragsparteien geändert werden können und auf die Artikel 25 des Übereinkommens anzuwenden ist.

Übersetzung aus der englischen Sprache – BMI-Sprachendienst 2019/0365-wr

Europarat

Sammlung der Europaratsverträge – Nr. 223

Erläuternder Bericht zum Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (*)

Straßburg/Strasbourg, 10.X.1985

I. Einleitung

1. Seit das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, die so genannte Europaratskonvention Nr. 108 (im Folgenden „das Übereinkommen" genannt) vor 35 Jahren zur Unterzeichnung aufgelegt wurde, ist es in mehr als 40 europäischen Ländern die Grundlage für völkerrechtlich verbindlichen Datenschutz gewesen. Weit über die Küsten Europas hinaus hat das Übereinkommen die Politik und Gesetzgebung beeinflusst. In Anbetracht der immer neuen Bedrohungen für die Menschenrechte und Grundfreiheiten, insbesondere für das Recht auf Privatleben und um den aus der zunehmenden Nutzung neuer Informations- und Kommunikationstechnologien (IKT), der Globalisierung von Verarbeitungsvorgängen und dem stetig anwachsenden Strom personenbezogener Daten erwachsenden Gefahren für den Datenschutz besser gerecht zu werden und gleichzeitig die Mechanismen des Übereinkommens für Evaluierung und Fortschreibung zu stärken, wurde klar, dass das Übereinkommen modernisiert werden sollte.

2. Es herrschte breiter Konsens über folgende Aspekte des Modernisierungsprozesses: der allgemeine und technologieneutrale Charakter der Bestimmungen des Übereinkommens muss gewahrt werden; die Kohärenz und Vereinbarkeit des Übereinkommens mit anderen rechtlichen Rahmenwerken muss erhalten bleiben; der offene Charakter des Übereinkommens, dem es sein einzigartiges Potential als universeller Standard verdankt, muss bekräftigt werden. Der Wortlaut des Übereinkommens ist allgemein gehalten und kann durch ausführlichere sektorspezifische, nicht zwingende (soft-law) Texte ergänzt werden, insbesondere durch Empfehlungen des Ministerkomitees unter Beteiligung von relevanten Interessengruppen.

3. Die Modernisierungsarbeit erfolgte im breiteren Kontext verschiedener, paralleler Reformen von völkerrechtlichen Datenschutzinstrumenten sowie unter Berücksichtigung der OECD-Leitlinien 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[1] seit 1995, des Rechtsrahmens für den Datenschutz für die Asiatisch-Pazifische Wirtschaftliche Zusammenarbeit (2004) und des Internationalen Standards für den Schutz der Privatsphäre im Hinblick auf die Verarbeitung von personenbezogenen Daten[2]. Insbesondere hinsichtlich des EU-Reformpakets für den Datenschutz wurden die Arbeiten parallel ausgeführt und man ließ höchste Sorgfalt walten, um die Konsistenz zwischen beiden Rechtsrahmen sicherzustellen. Der EU-Datenschutzrahmen konkretisiert und erweitert die in dem Übereinkommen Nr. 108 enthaltenen Grundsätze des Datenschutzes und berücksichtigt den Beitritt zum Übereinkommen Nr. 108, insbesondere im Hinblick auf internationale Transfers.[3]

4. Der Beratende Ausschuss nach Artikel 18 des Übereinkommens hat einen Entwurf mit Modernisierungsvorschlägen erarbeitet, die auf der 29. Plenarsitzung (27.-30. November 2012) verabschiedet und dem Ministerkomitee vorgelegt wurden. Das Ministerkomitee hat den *Ad-hoc*-Auschuss zum Datenschutz (CAHDATA) beauftragt, die Modernisierungsvorschläge zu finalisieren. Diese Aufgabe wurden anlässlich der 3. CAHDATA-Sitzung (1.-3. Dezember 2014) abgeschlossen.

---

1 Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) und Datenschutzrichtlinie Polizei/Justiz (EU) 2016/680 (DSRL Polizei/Justiz).

2 Begrüßt von der 31. Internationalen Datenschutzkonferenz, die vom 4.-6. November 2009 in Madrid stattfand.

3 Siehe insbesondere Erwägungsgrund 105 der DSGVO.

Mit Blick auf die Finalisierung des EU-Datenschutzrahmens wurde ein weiterer CAHDATA eingesetzt, um noch offene Punkte zu klären. Auf der letzten CAHDATA-Sitzung (15.-16. Juni 2016) wurden die Vorschläge finalisiert und dem Ministerkomitee zur Prüfung und Annahme vorgelegt.

5. Dieser Erläuternde Bericht soll als Orientierungshilfe und Leitfaden bei der Anwendung der Bestimmungen des Übereinkommens dienen und zeigen, wie sich die Urheber des Übereinkommens dessen Wirkungsweise vorgestellt haben.

6. Das Ministerkomitee hat den Erläuternden Bericht gebilligt. In dieser Hinsicht ist der Erläuternde Bericht Teil des Zusammenhangs, in dem die Bedeutung bestimmter, in dem Übereinkommen verwendeter Begriffe festgestellt wird (Hinweis: siehe Artikel 31, Absätze 1 und 2 des Wiener Übereinkommens über das Recht der Verträge).

Das Protokoll wurde am 18. Mai 2018 vom Ministerkomitee angenommen. Der Anhang ist Bestandteil des Protokolls und ist ebenso rechtsverbindlich wie die anderen Bestimmungen des Protokolls.

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

(*) Dieses Dokument wird der Erläuternde Bericht zum Übereinkommen Nr. 108 in der durch das Änderungsprotokoll geänderten Fassung.

II. Erläuterungen:

7. Der Zweck dieses Protokolls ist es, das Übereinkommen des Europarats über Geldwäsche sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten (SEV Nr. 108) und das Zusatzprotokoll zum Übereinkommen bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (ETS Nr. 181) zu modernisieren und deren Anwendung zu stärken. Ab dem Tag seines Inkrafttretens gilt das Zusatzprotokoll als Bestandteil des Übereinkommens in der jeweils gültigen Fassung.

8. Die Erläuternden Berichte zum Übereinkommen Nr. 108 und seinem Zusatzprotokoll bleiben relevant insofern, als sie den historischen Zusammenhang bilden und die Entwicklung beider Instrumente zeigen. Sie können zu diesem Zweck in Verbindung mit dem aktuellen Dokument gelesen werden.

Präambel

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

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

11. Angesichts der Bedeutung des Rechts auf Schutz personenbezogener Daten in Bezug auf dessen gesellschaftliche Rolle wird in der Präambel hervorgehoben, dass die Interessen, Rechte und Grundfreiheiten der Menschen miteinander in Einklang zu bringen sind. Um die verschiedenen Interessen, Rechte und Grundfreiheiten vorsichtig in ein Gleichgewicht zu bringen, sind in dem Übereinkommen bestimmte Bedingungen und Beschränkungen für die Verarbeitung von Informationen und den Schutz personenbezogener Daten festgelegt. So ist beispielsweise das Recht auf Datenschutz im Zusammenhang mit dem Recht der freien Meinungsäußerung zu betrachten, das in Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte (SEV Nr. 5) festgelegt ist und die Meinungsfreiheit und die Freiheit, Informationen zu empfangen und weiterzugeben, einschließt. Im Übrigen bestätigt das Übereinkommen, dass die Wahrnehmung des Rechts auf Datenschutz, das nicht absolut ist, nicht allgemein herangezogen werden sollte, um den öffentlichen Zugang zu amtlichen Dokumenten zu verhindern.[4]

12. Durch die im Übereinkommen Nr. 108 festgelegten Grundsätze und Werte wird der Einzelne geschützt und gleichzeitig ein Rahmen für den internationalen Datenverkehr geschaffen. Dies ist angesichts der

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

wachsenden Bedeutung globaler Informationsflüsse in der modernen Gesellschaft besonders wichtig, um die Ausübung der Grundrechte und Grundfreiheiten zu ermöglichen und gleichzeitig Innovationen anzuregen und gesellschaftlichen und wirtschaftlichen Fortschritt zu fördern und dabei die öffentliche Sicherheit zu gewährleisten. Bei dem Verkehr von personenbezogenen Daten in einer Informations- und Kommunikationsgesellschaft müssen die Grundrechte und Grundfreiheiten des Einzelnen gewahrt bleiben. Auch bei der Entwicklung und Nutzung innovativer Technologien sollten diese Rechte beachtet werden. Dies wird dazu beitragen, Vertrauen in Innovationen und neue Technologien zu schaffen und deren Weiterentwicklung zu fördern.

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

Kapitel I - Allgemeine Bestimmungen

Artikel 1 – Ziel und Zweck

14. In Artikel 1 werden das Ziel und der Zweck des Übereinkommens beschrieben. Der Schwerpunkt liegt dabei auf dem Schutzaspekt: Jedermann muss geschützt werden, wenn seine personenbezogenen Daten verarbeitet werden.[5] Kürzlich wurde der Datenschutz als ein Grundrecht in Artikel 8 der Charta der Grundrechte der Europäischen Union und in die Verfassungen einiger Unterzeichner des Übereinkommens aufgenommen.

15. Die in dem Übereinkommen festgelegten Garantien werden auf jeden Menschen, unabhängig von seiner Nationalität oder seinem Wohnsitz, ausgedehnt. Bei der Anwendung dieser Garantien darf nicht zwischen Staatsangehörigen und Drittausländern unterschieden werden.[6] Klauseln, die den Datenschutz auf eigene Staatsangehörige oder rechtmäßig aufhältige ausländische Staatsangehörige beschränken, wären mit dem Übereinkommen unvereinbar.

Artikel 2 – Begriffsbestimmungen

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

Buchstabe a – „personenbezogene Daten“

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

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

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

[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, Ziffer 3.3 Jedermann frei von Diskriminierung (’Everyone’ without discrimination).

Bestimmungen des Übereinkommens. Bei der Bewertung, ob die getroffenen Sicherheitsvorkehrungen zur Minderung der Risiken für betroffene Personen geeignet sind, sollte die Qualität der Pseudonymisierungstechniken hinreichend Berücksichtigung finden.

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

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

Buchstaben b und c – „Datenverarbeitung“

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

Buchstabe d – „der für die Verarbeitung Verantwortliche“

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

Buchstabe e – „Empfänger“

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

nicht vollständige Dateisysteme betreffen oder zur Verknüpfung von Dateisystemen führen. Die Verarbeitung personenbezogener Daten durch die genannten Behörden sollte für die Zwecke der Verarbeitung geltenden Datenschutzvorschriften entsprechen.

Buchstabe f – Auftragsverarbeiter

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

Artikel 3 – Anwendungsbereich

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

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

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

28. Ob Tätigkeiten „rein persönliche oder familiäre Tätigkeiten" sind, hängt von den Umständen ab. Der Ausschluss gilt jedoch nicht, wenn personenbezogene Daten einer großen Zahl von Personen oder Personen, die offensichtlich außerhalb der Privatsphäre stehen, wie beispielsweise auf einer Website im Internet, zugänglich gemacht werden. Ähnlich verhält es sich mit dem Betrieb einer Kameraanlage, mit deren Hilfe Videoaufnahmen von Menschen auf einem Dauerspeichermedium, wie beispielsweise eine Festplatte, gespeichert werden, die von einer Einzelperson in ihrem Haus zum Zweck des Schutzes des Eigentums, der Gesundheit oder des Lebens der Hauseigentümer installiert wurde, die jedoch - wenn auch nur teilweise - einen Bereich des öffentlichen Raums erfasst und vom Privatbereich der die Daten auf diese Weise verarbeitenden Person nach außen gerichtet ist: Dies kann nicht als eine „rein persönliche oder familiäre Tätigkeit" angesehen werden.[7]

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

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

Kapitel II – Grundsätze für den Schutz personenbezogener Daten

Artikel 4 – Pflichten der Vertragsparteien

31. Nach diesem Artikel sind die Vertragsparteien verpflichtet, die Bestimmungen des Übereinkommens in ihr Recht aufzunehmen und ihnen in der Praxis Wirksamkeit zu verleihen. Wie dies getan wird, hängt von der

[7] Siehe Europäischer Gerichtshof, *Frantisek Rynes v. Urad*, 11. Dezember 2014, C-212/13k.

geltenden Rechtsordnung und dem für die Einbindung völkerrechtlicher Übereinkünfte gewählten Ansatz ab.

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

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

34. Wenn internationale Organisationen betroffen sind[8], so kann das Recht dieser internationalen Organisationen auch unmittelbar auf nationaler Ebene der Mitgliedstaaten dieser Organisationen angewendet werden, je nach der jeweiligen nationalen Rechtsordnung.

35. Die Effektivität der Anwendung der Maßnahmen, mit denen den Bestimmungen des Übereinkommens Wirksamkeit verliehen wird, ist von entscheidender Bedeutung. Bei der Gesamtbeurteilung der Effektivität der Umsetzung der Bestimmungen des Übereinkommens durch eine Vertragspartei sollten sowohl die Rolle der Aufsichtsbehörde (oder Behörden) als auch die den Rechtssubjekten zur Verfügung stehenden Rechtsbehelfe betrachtet werden.

36. Nach Absatz 2 müssen die Maßnahmen, mit denen dem Übereinkommen Wirksamkeit verliehen wird, von jeder Vertragspartei getroffen werden und bis zum Zeitpunkt der Ratifikation dieses Übereinkommens oder des Beitritts dazu, d. h. wenn das Übereinkommen für eine Vertragspartei verbindlich wird, in Kraft getreten sein. Mit dieser Bestimmung soll der Übereinkommensausschuss in die Lage versetzt werden zu bewerten, ob alle „notwendigen Maßnahmen“ getroffen wurden um sicherzustellen, dass die Vertragsparteien des Übereinkommens ihre Verpflichtungen einhalten und in ihrem innerstaatlichen Recht das erwartete Datenschutzniveau sicherstellen. Das Verfahren für diese Verifizierung und die dabei verwendeten Kriterien müssen in der Verfahrensordnung des Übereinkommensausschusses klar definiert sein.

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

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

39. Die Bewertung, ob eine Vertragspartei das Übereinkommen erfüllt, erfolgt durch den Übereinkommensausschuss auf der Grundlage eines objektiven, fairen und transparenten Verfahrens, das der

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

Übereinkommensausschuss festlegt und in seiner Verfahrensordnung umfassend erläutert.

Artikel 5 – Rechtmäßigkeit der Datenverarbeitung und Qualität der Daten

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

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

42. Die Einwilligung der betroffenen Person muss freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich erfolgen. Bei dieser Einwilligung muss es sich um die freie Äußerung einer bewussten Wahl handeln, die entweder durch Erklärung (schriftlich, auch auf elektronischem Wege, oder mündlich) abgegeben wird oder durch eine eindeutige bestätigende Handlung, die in diesem konkreten Zusammenhang eindeutig das Einverständnis mit der vorgeschlagenen Verarbeitung von personenbezogenen Daten anzeigt. Bloßes Schweigen, Inaktivität oder vorab validierte Formulare sollten daher nicht als Einwilligung gelten. Die Einwilligung sollte sich auf sämtliche Verarbeitungstätigkeiten beziehen, die für denselben Zweck oder dieselben Zwecke durchgeführt werden (im Falle mehrerer Zwecke sollte die Einwilligung für jeden Zweck einzeln gegeben werden). Es kann vorkommen, dass die betroffene Person unterschiedliche Entscheidungen hinsichtlich ihrer Einwilligung trifft (z. B. wenn sich die Art der Daten unterscheidet, obwohl der Zweck derselbe ist, wie beispielsweise bei Gesundheitsdaten und Aufenthaltsdaten: In solch einem Fall kann die betroffene Person der Verarbeitung von ihren Aufenthaltsdaten zustimmen, nicht jedoch der Verarbeitung ihrer Gesundheitsdaten). Die betroffene Person muss über die Auswirkungen ihrer Entscheidung aufgeklärt werden (über die Folgen der Einwilligung und den Umfang der Einwilligung). Auf die betroffene Person darf weder direkt noch indirekt Einfluss genommen oder Druck (wirtschaftlicher oder sonstiger Art) ausgeübt werden, und Einverständniserklärungen, bei denen die betroffene Person keine echte oder freie Wahl hatte oder ihr Einverständnis nicht unbeschadet ablehnen oder widerrufen konnte, sollten nicht als freiwillig abgegeben gelten.

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

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

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

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

47. Die Datenverarbeitung aus Gründen des öffentlichen Interesses sollte gesetzlich geregelt sein, etwa im

Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit, für Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Straftaten, der Strafvollstreckung, der nationalen Sicherheit, Verteidigung, für Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe, für Zwecke der Durchsetzung zivilrechtlicher Ansprüche sowie zum Schutz der richterlichen Unabhängigkeit und gerichtlicher Verfahren. Die Datenverarbeitung kann sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen, beispielsweise bei der Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen. Dies kann insbesondere bei Naturkatastrophen der Fall sein, wenn die Verarbeitung personenbezogener Daten von vermissten Personen für eine begrenzte Zeit im Rahmen der Katastrophenbewältigung notwendig sein kann, was im Einzelfall zu entscheiden ist. Auch in bewaffneten Konflikten oder anderen Gewaltlagen kann dies zutreffen.[9] Auch im Hinblick auf die Verarbeitung personenbezogener Daten durch staatliche Stellen zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften kann gelten, dass sie aus Gründen des öffentlichen Interesses durchgeführt wird.

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

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

50. Die in Buchstabe b genannte Weiterverarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt a priori als mit solchen Zwecken vereinbar, sofern andere Garantien bestehen (wie beispielsweise die Anonymisierung oder Pseudonymisierung von Daten, sofern nicht die Speicherung der identifizierbaren Form erforderlich ist; Regelung zum Berufsgeheimnis; Zugangsbeschränkungen und Regeln für die Übermittlung der Daten für die vorgenannten Zwecke, insbesondere Statistik- und Archivzwecke; sonstige technische und organisatorische Datenschutzmaßnahmen) und sofern die Verarbeitungsvorgänge grundsätzlich jede Nutzung der gewonnenen Informationen für Entscheidungen oder Maßnahmen hinsichtlich einer bestimmten Person ausschließen. „Statistische Zwecke“ bezieht sich auf statistische Erhebungen oder die Erzeugung von statistischen, aggregierten Ergebnissen. Statistiken dienen der Analyse und Charakterisierung von massenhaften oder kollektiven Phänomenen in einer zu untersuchenden Bevölkerungsgruppe.[10] Statistische Zwecke können sowohl vom öffentlichen oder privaten Sektor verfolgt werden. Die Verarbeitung von Daten für „wissenschaftliche Forschungszwecke“ dient dazu, Forscher mit Informationen zu versorgen, die zum Verständnis von Phänomenen in verschiedenen wissenschaftlichen Bereichen beitragen (Epidemiologie, Psychologie, Ökonomie, Soziologie, Sprachwissenschaft, Politische Wissenschaften, Kriminologie usw.). Dabei geht es darum, dauerhafte Grundsätze, gesetzmäßige Verhaltensweisen oder Kausalitätsmuster zu erkennen, die über die Personen hinausgehen, für die sie

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

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

gelten.[11] „Historische Forschungszwecke“ umfasst auch Forschung im Bereich der Genealogie. „Im öffentlichen Interesse liegende Archivzwecke“ kann auch ursprünglich private Archive umfassen, sofern ein öffentliches Interesse vorliegt.

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

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

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

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

Artikel 6 – Besondere Kategorien von Daten

55. Die Verarbeitung bestimmter Typen von Daten oder die Verarbeitung bestimmter Daten zur Offenlegung sensibler Informationen kann zu Eingriffen in Interessen, Rechte und Freiheiten führen. Dies ist möglicherweise der Fall, wenn ein potenzielles Risiko der Diskriminierung oder der Verletzung der Würde oder der körperlichen Unversehrtheit einer Person besteht, wenn der persönlichste Bereich einer Person, wie ihr Sexualleben oder ihre sexuelle Orientierung betroffen sind, oder wenn sich die Datenverarbeitung auf die Unschuldsvermutung auswirken könnte. Die Datenverarbeitung sollte dann nur zugelassen werden, wenn ergänzend zu den anderen Schutzbestimmungen des Übereinkommens weitere Garantien gesetzlich vorgesehen sind. Das Erfordernis geeigneter Garantien ergänzend zu den Bestimmungen des Übereinkommens schließt jedoch nicht die in Artikel 11 vorgesehene Möglichkeit aus, Ausnahmen oder Beschränkungen der Rechte einer betroffenen Person nach Artikel 9 zuzulassen.

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

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

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

und Freiheiten der betroffenen Personen.

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

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

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

61. Ist die Verarbeitung von sensiblen Daten für statistische Zwecke erforderlich, dann muss bei der Erhebung der Daten sichergestellt werden, dass die betroffenen Personen nicht identifizierbar sind. Eine Garantie im Sinne des Artikels 6 ist die Erhebung von sensible Daten für statistische Zwecke in identifizierbarer Form zu erheben (beispielsweise, um eine Wiederholungs- oder eine Longitudinalstudie durchzuführen), sollten geeignete Garantien etabliert werden.[12]

Artikel 7 – Datensicherheit

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

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

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

65. Ist es zu einer solchen Verletzung des Datenschutzes gekommen, ist der Verantwortliche für die Verarbeitung verpflichtet, die zuständige Aufsichtsbehörde über den Vorfall zu informieren, vorbehaltlich der in Artikel 11 Absatz 1 gestatteten Ausnahme. Dies ist die Mindestanforderung. Der für die Verarbeitung Verantwortliche sollte außerdem die Aufsichtsbehörden über alle getroffenen und / oder vorgeschlagenen

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

Maßnahmen informieren, die sich auf die Verletzung des Datenschutzes und deren potenzielle Folgen beziehen.

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

Artikel 8 – Transparenz der Verarbeitung

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

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

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

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

Artikel 9 – Rechte des Betroffenen

71. In diesem Artikel sind die Rechte aufgeführt, die jede Person im Hinblick auf die Verarbeitung von sie betreffenden personenbezogenen Daten ausüben können sollte. Jede Partei stellt im Rahmen ihrer Rechtshoheit sicher, dass jede betroffene Person von diesen Rechten Gebrauch machen kann, und jeder

betroffenen Person die zur Ausübung dieser Rechte nötigen rechtlichen und praktischen, angemessenen und wirksamen Mittel zur Verfügung stehen.

72. Diese sind u.a.:

- das Recht einer jeden Person, einer ausschließlich auf einer automatisierten Datenverarbeitung beruhenden Entscheidung, die sich erheblich auf sie auswirkt, nicht unterworfen zu werden, ohne dass ihre Auffassungen berücksichtigt werden (Buchstabe a),

- das Recht einer jeden Person, eine Bestätigung über die Verarbeitung von sie betreffenden personenbezogenen Daten zu erhalten und in angemessenen Abständen und ohne übermäßige Verzögerung oder Kosten Auskunft über diese Daten zu erhalten (Buchstabe b),

- das Recht einer jeden Person, auf Antrag Kenntnis über die der Datenverarbeitung zugrundeliegenden Überlegungen zu erlangen, wenn die Ergebnisse dieser Verarbeitung auf die Person Anwendung finden (Buchstabe c),

- das Recht einer jeden Person, aus sich aus ihrer Situation ergebenden Gründen gegen die Verarbeitung von sie betreffenden personenbezogenen Daten Widerspruch einzulegen, sofern der Verantwortliche nicht nachweisen kann, dass berechtigte Gründe für die Verarbeitung bestehen, welche die Interessen, Rechte oder Grundfreiheiten der Person überwiegen (Buchstabe d),

- das Recht einer jeden Person, die Berichtigung beziehungsweise Löschung von unrichtigen, falschen oder unrechtmäßig verarbeiteten Daten zu erwirken (Buchstabe e),

- das Recht jeden Person, ein Rechtsmittel einzulegen, wenn eines ihrer vorgenannten Rechte verletzt worden ist (Buchstabe f),

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

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

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

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

76. Buchstabe b: Betroffene Personen sollten Anspruch haben, von der Verarbeitung ihrer

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

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

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

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

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

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

82. Mit Buchstabe g sollen die betroffenen Personen durch das Recht auf Hilfe von einer Aufsichtsbehörde bei der Wahrnehmung ihrer Rechte aus dem Übereinkommen wirksam geschützt werden. Lebt die betroffene Person im Hoheitsgebiet einer anderen Vertragspartei, kann sie ihren Antrag über die bezeichnete Aufsichtsbehörde dieser Vertragspartei stellen. Das Unterstützungsersuchen sollte hinreichende Informationen enthalten, um die fragliche Datenverarbeitung identifizieren zu können. Dieses Recht kann gemäß Artikel 11 im Interesse eines laufenden gerichtlichen Verfahrens beschränkt werden.

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

Artikel 10 – Zusätzliche Verpflichtungen

84. Um die Wirksamkeit des Rechts auf Schutz von personenbezogenen Daten sicherzustellen, werden dem

Verantwortlichen und gegebenenfalls den Auftragsverarbeitern zusätzliche Verpflichtungen auferlegt.

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

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

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

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

89. Gemäß Absatz 3 sollen die Verantwortlichen und gegebenenfalls die Auftragsverarbeiter durch technische und organisatorische Maßnahmen sicherstellen, dass Datenschutzanforderungen so früh wie möglich berücksichtigt werden, idealerweise bereits in der Phase der Architektur- oder Systemkonzeption (Datenschutz durch Technikgestaltung). Diese Umsetzung von Datenschutzanforderungen sollte nicht nur im Hinblick auf die Technologie zur Datenverarbeitung verfolgt werden, sondern auch im Hinblick auf Arbeits- und Verwaltungsprozesse. Leicht nutzbare Funktionalitäten, die die Einhaltung von Datenschutzstandards erleichtern, sollten etabliert werden. So sollten betroffene Personen beispielsweise die Möglichkeit des sicheren Online-Zugriffs auf ihre eigenen Daten haben. Ebenso sollte es mit Hilfe leicht zu bedienender Werkzeuge für betroffene Personen möglich sein, ihre Daten zu einem anderen Diensteanbieter ihrer Wahl mitzunehmen oder ihre Daten selbst aufzubewahren (Werkzeuge zur Datenübertragbarkeit). Bei der Festlegung von technischen Anforderungen für Default-Einstellungen sollten Verantwortliche und Auftragsverarbeiter datenschutzfreundliche Konfigurationen wählen, damit durch die Nutzung von Anwendungen und Software die Rechte von betroffenen Personen nicht verletzt werden (Datenschutz by Default), insbesondere um zu verhindern, dass für den rechtmäßigen Zweck mehr Daten als nötig verarbeitet werden. Soziale Netzwerke sollten beispielsweise standardmäßig so konfiguriert werden, dass Posts oder Bilder nur innerhalb begrenzter und ausgewählter Kreise geteilt werden, und nicht im gesamten Internet.

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

Artikel 11 – Ausnahmen und Beschränkungen

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

92. Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise erfolgen, und die Daten dürfen nur für bestimmte Zwecke verarbeitet werden. Dies steht an sich der Durchführung von Maßnahmen wie verdeckten Ermittlungen oder Videoüberwachung durch die Strafverfolgungsbehörden nicht entgegen. Diese Maßnahmen können zwecks Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die nationale und öffentliche Sicherheit, getroffen werden, sofern sie gesetzlich geregelt sind und eine erforderliche und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen, bei der die berechtigten Interessen der betroffenen Person gebührend berücksichtigt werden.

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

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

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

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

97. Mit Absatz 2 wird die Möglichkeit eingeräumt, die Bestimmungen der Artikel 8 und 9 im Hinblick auf eine bestimmte Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken, die keine erkennbare Gefahr des Eingriffs in die Rechte und Grundfreiheiten von Betroffenen darstellt, zu beschränken. Dies betrifft beispielsweise die Nutzung von Daten für statistische Arbeiten sowohl im öffentlichen wie im privaten Bereich sofern die Daten in aggregierter Form veröffentlicht werden und vorausgesetzt, dass angemessene Datenschutzvorkehrungen getroffen wurden (siehe Ziffer 50).

98. Die zusätzlich zu den nach Artikel 4 Absatz 3, Artikel 14 Absätze 5 und 6 und Artikel 15 Absatz 2

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

Buchstaben a), b), c) und d) in Bezug auf Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung zulässigen Ausnahmen gelten unbeschadet der Voraussetzung einer unabhängigen und wirksamen Prüfung und Aufsicht.[14]

Artikel 12 – Sanktionen und Rechtsmittel

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

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

Artikel 13 – Erweiterter Schutz

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

Kapitel III – Grenzüberschreitender Verkehr personenbezogener Daten[15]

Artikel 14 – Grenzüberschreitender Verkehr personenbezogener Daten

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

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

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

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

---

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

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

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

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

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

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

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

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

112. Bei der Beurteilung, ob ein Datenschutzniveau angemessen ist, ist zu prüfen, ob bzw. in welchem

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

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

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

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

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

Kapitel IV – Aufsichtsbehörden[16]

Artikel 15 – Aufsichtsbehörden

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

118. In Absatz 1 wird klargestellt, dass möglicherweise Bedarf an einer oder mehreren Behörden besteht, um den besonderen Umständen unterschiedlicher Rechtssysteme (z. B. föderale Staaten) gerecht zu werden. Möglich ist auch die Schaffung spezifischer Aufsichtsbehörden, deren Tätigkeit auf einen bestimmten Sektor beschränkt ist (elektronische Kommunikation, Gesundheitswesen, öffentlicher Sektor usw.). Dies gilt auch für die Verarbeitung von personenbezogene Daten für journalistische Zwecke, wenn dies notwendig ist, um das Recht auf den Schutz von personenbezogenen Daten mit dem Recht der freien Meinungsäußerung in Einklang zu bringen. Die Aufsichtsbehörden sollten über die notwendige Infrastruktur und die notwendigen finanziellen, technischen und personellen (Juristen, IT-Spezialisten) Mittel verfügen, um unverzüglich und wirksam handeln zu können. Die Angemessenheit der Mittel sollte ständig überprüft werden. Nach Artikel 11 Absatz 3 sind,

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

unter Verweis auf Verarbeitungstätigkeiten für Zwecke der nationalen Sicherheit und der Landesverteidigung, Ausnahmen von den Befugnissen der Aufsichtsbehörden zulässig (sofern solche Ausnahmen gelten, gelten andere Absätze des Artikels 11 folglich ggf. nicht bzw. sind dadurch irrelevant). Dies gilt jedoch unbeschadet der Anforderungen bezüglich der Unabhängigkeit und Wirksamkeit von Überprüfungs- und Aufsichtsmechanismen.[17]

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

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

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

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

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

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

125. In Absatz 2 Buchstabe e geht es um die bewusstseinsfördernde Rolle der Aufsichtsbehörden. In diesem Zusammenhang scheint es besonders wichtig, dass die Aufsichtsbehörde proaktiv für die Sichtbarkeit ihrer Tätigkeiten, Aufgaben und Befugnisse sorgt. Dazu muss die Aufsichtsbehörde die Öffentlichkeit durch periodische Berichte informieren (siehe Ziffer 131). Sie kann auch Stellungnahmen und allgemeine

[17] Siehe Fußnote 14.

Empfehlungen hinsichtlich der richtigen Umsetzung von Datenschutzvorschriften abgeben oder andere Kommunikationsmittel nutzen. Sie muss darüber hinaus betroffene Personen, Verantwortliche für die Verarbeitung und Auftragsverarbeiter über ihre Rechte und Pflichten hinsichtlich des Datenschutzes informieren. Im Zuge der Förderung des Bewusstseins für Datenschutzbelange müssen die Aufsichtsbehörden den Datenschutzrechten von Kindern und anderen schutzbedürftigen Personen besondere Aufmerksamkeit widmen und sich in angepasster Form und Sprache an diese Personengruppen wenden.

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

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

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

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

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

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

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

133. Unbeschadet der Verfahrensfähigkeit von Aufsichtsbehörden vor Gericht darf durch die Intervention (oder das Versäumnis) einer Aufsichtsbehörde eine betroffene Person nicht daran gehindert werden, einen gerichtlichen Rechtsbehelf einzulegen (siehe Ziffer 124).

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

Kapitel V – Zusammenarbeit und gegenseitige Hilfeleistung

Artikel 16 – Benennung von Aufsichtsbehörden

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

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

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

Artikel 17 – Formen der Zusammenarbeit

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

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

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

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

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

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

Artikel 18 – Unterstützung von Betroffenen

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

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

146. Im Übrigen können im Ausland ansässige betroffene Personen bei der Wahrnehmung ihrer Rechte die

Unterstützung durch Botschafts- oder Konsularbeamte ihres Landes in Anspruch nehmen.

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

Artikel 19 – Garantien

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

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

Artikel 20 – Ablehnung von Ersuchen

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

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

Artikel 21 – Kosten und Verfahren

152. Die Bestimmungen dieses Artikels entsprechen jenen in anderen völkerrechtlichen Instrumenten.

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

Kapitel VI – Übereinkommensausschuss

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

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

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

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

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

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

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

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

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

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

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

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

Kapitel VII – Änderungen

Artikel 25 – Änderungen

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

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

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

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

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

Kapitel VIII – Schlussbestimmungen

Artikel 26 – Inkrafttreten

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

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

Artikel 27 – Beitritt von Nichtmitgliedstaaten oder internationalen Organisationen

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

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

Artikel 28 – Gebietsklausel

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

Artikel 29 – Vorbehalte

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

Artikel 30 – Kündigung

176. Jede Vertragspartei kann das Übereinkommen jederzeit kündigen.

Artikel 31 – Notifikationen

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

(*) Dieses Dokument wird der Erläuternde Bericht zum Übereinkommen Nr. 108 in der durch das Änderungsprotokoll geänderten Fassung.

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

Geltungsbereich des Protokolls zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten am 11. Januar 2023

Vertragsstaaten	Ratifikation		Inkrafttreten	
Albanien	22. Juli	2022		
Andorra	18. Oktober	2022		
Armenien	25. Januar	2022		
Bulgarien	10. Dezember	2019		
Deutschland	5. Oktober	2021		
Estland	16. September	2020		
Finnland	10. Dezember	2020		
Italien	8. Juli	2021		
Kroatien	18. Dezember	2019		
Litauen	23. Januar	2020		
Malta	2. November	2020		
Mauritius	4. September	2020		
Nordmazedonien	26. November	2021		
Österreich	13. Juli	2022		
Polen	10. Juni	2020		
Rumänien	9. März	2022		
Serbien	26. Mai	2020		
Spanien	28. Januar	2021		
Uruguay	5. August	2021		
Zypern	21. September	2020		

Total Anzahl an Ratifikationen: 20

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Sammlung Europäischer Verträge - Nr. 108

Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Straßburg/Strasbourg, 28.I.1981

Amtliche Übersetzung Deutschlands

Präambel

Die Mitgliedstaaten des Europarats, die dieses Übereinkommen unterzeichnen,

in der Erwägung, daß es das Ziel des Europarats ist, eine engere Verbindung zwischen seinen Mitgliedern herbeizuführen, die vor allem auf der Achtung des Vorranges des Rechts sowie der Menschenrechte und Grundfreiheiten beruht;

in der Erwägung, daß es angesichts des zunehmenden grenzüberschreitenden Verkehrs automatisch verarbeiteter personenbezogener Daten wünschenswert ist, den Schutz der Rechte und Grundfreiheiten jedes Menschen, vor allem das Recht auf Achtung des Persönlichkeitsbereichs, zu erweitern;

unter gleichzeitiger Bekräftigung, für eine Informationsfreiheit ohne Rücksicht auf Staatsgrenzen einzutreten;

in Anerkennung der Notwendigkeit, die grundlegenden Werte der Achtung des Persönlichkeitsbereichs und des freien Informationsaustausches zwischen den Völkern in Einklang zu bringen,

sind wie folgt übereingekommen:

Kapitel I – Allgemeine Bestimmungen

Artikel 1 – Gegenstand und Zweck

Zweck dieses Übereinkommens ist es, im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogner Daten geschützt werden ("Datenschutz").

Artikel 2 – Begriffsbestimmungen

In diesem Übereinkommen:

a bedeutet "personenbezogene Daten" jede Information über eine bestimmte oder bestimmbare natürliche Person ("Betroffener");

b bedeutet "automatisierte Datei/Datensammlung" jede zur automatischen Verarbeitung erfaßte Gesamtheit von Informationen;

c umfaßt "automatische Verarbeitung" die folgenden Tätigkeiten, wenn sie ganz oder teilweise mit Hilfe automatisierter Verfahren durchgeführt werden: das Speichern von Daten, das Durchführen logischer und/ oder rechnerischer Operationen mit diesen Daten, das Verändern, Löschen, Wiedergewinnen oder Bekanntgeben von Daten;

d bedeutet "Verantwortlicher für die Datei/Datensammlung" die natürliche oder juristische Person, die Behörde, die Einrichtung oder jede andere Stelle, die nach dem innerstaatlichen Recht zuständig ist, darüber zu entscheiden, welchen Zweck die automatisierte Datei/Datensammlung haben soll, welche Arten personenbezogener Daten gespeichert und welche Verarbeitungsverfahren auf sie angewendet werden sollen.

Artikel 3 – Geltungsbereich

1 Die Vertragsparteien verpflichten sich, dieses Übereinkommen auf automatisierte Dateien/Datensammlungen und automatische Verarbeitungen von personenbezogenen Daten im öffentlichen und privaten Bereich anzuwenden.

2 Jeder Staat kann bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde oder jederzeit danach durch Erklärung an den Generalsekretär des Europarats bekanntgeben:

a daß er dieses Übereinkommen auf bestimmte Arten von automatisierten Dateien/Datensammlungen mit personenbezogenen Daten nicht anwendet, und hinterlegt ein Verzeichnis dieser Arten. In das Verzeichnis darf er jedoch Arten automatisierter Dateien/Datensammlungen nicht aufnehmen, die nach seinem innerstaatlichen Recht Datenschutzvorschriften unterliegen. Er ändert dieses Verzeichnis durch eine neue Erklärung, wenn weitere Arten von automatisierten Dateien/Datensammlungen mit personenbezogenen Daten seinen innerstaatlichen Datenschutzvorschriften unterstellt werden;

b daß er dieses Übereinkommen auch auf Informationen über Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften oder andere Stellen anwendet, die unmittelbar oder mittelbar aus natürlichen Personen bestehen, unabhängig davon, ob diese Stellen Rechtspersönlichkeit besitzen oder nicht;

c daß er dieses Übereinkommen auch auf Dateien/Datensammlungen mit personenbezogenen Daten anwendet, die nicht automatisch verarbeitet werden.

3 Jeder Staat, der den Geltungsbereich dieses Übereinkommens durch eine Erklärung nach Absatz 2 Buchstabe b oder c erweitert hat, kann in dieser Erklärung bekanntgeben, daß die Erweiterung nur für bestimmte Arten von Dateien/Datensammlungen mit personenbezogenen Daten gilt; er hinterlegt ein Verzeichnis dieser Arten.

4 Hat eine Vertragspartei bestimmte Arten von automatisierten Dateien/Datensammlungen mit personenbezogenen Daten durch eine Erklärung nach Absatz 2 Buchstabe a ausgeschlossen, so kann sie nicht verlangen, daß eine Vertragspartei, die diese Arten nicht ausgeschlossen hat, das Übereinkommen auf diese Arten anwendet.

5 Ebenso kann eine Vertragspartei, die keine Erweiterung nach Absatz 2 Buchstabe b oder c vorgenommen hat, in diesen Punkten die Anwendung dieses Übereinkommens nicht verlangen von einer Vertragspartei, die eine solche Erweiterung vorgenommen hat.

6 Die Erklärungen nach Absatz 2 werden mit Inkrafttreten des Übereinkommens für den Staat wirksam, der sie abgegeben hat, wenn sie im Zeitpunkt der Unterzeichnung oder der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde abgegeben worden sind, oder drei Monate nach ihrem Eingang beim Generalsekretär des Europarats, wenn sie später abgegeben worden sind. Diese Erklärungen können ganz oder teilweise durch Notifikation an den Generalsekretär des Europarats zurückgenommen werden. Die Zurücknahme wird drei Monate nach Eingang der Notifikation wirksam.

Kapitel II – Grundsätze für den Datenschutz

Artikel 4 – Pflichten der Vertragsparteien

1 Jede Vertragspartei trifft in ihrem innerstaatlichen Recht die erforderlichen Maßnahmen, um die in diesem Kapitel aufgestellten Grundsätze für den Datenschutz zu verwirklichen.

2 Jede Vertragspartei trifft diese Maßnahmen spätestens zu dem Zeitpunkt, zu dem dieses Übereinkommen für sie in Kraft tritt.

Artikel 5 – Qualität der Daten

Personenbezogene Daten, die automatisch verarbeitet werden:

a müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden;

b müssen für festgelegte und rechtmäßige Zwecke gespeichert sein und dürfen nicht so verwendet werden, daß es mit diesen Zwecken unvereinbar ist;

c müssen den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen;

d müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein;

e müssen so aufbewahrt werden, daß der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern.

Artikel 6 – Besondere Arten von Daten

Personenbezogene Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere überzeugungen erkennen lassen, sowie personenbezogene Daten, welche die Gesundheit oder das Sexualleben betreffen, dürfen nur automatisch verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet. Dasselbe gilt für personenbezogene Daten über Strafurteile.

Artikel 7 – Datensicherung

Für den Schutz personenbezogener Daten, die in automatisierten Dateien/Datensammlungen gespeichert sind, werden geeignete Sicherungsmaßnahmen getroffen gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben.

Artikel 8 – Zusätzlicher Schutz für den Betroffenen

Jedermann muß die Möglichkeit haben:

a das Vorhandensein einer automatisierten Datei/Datensammlung mit personenbezogenen Daten, ihre Hauptzwecke sowie die Bezeichnung, den gewöhnlichen Aufenthaltsort oder den Sitz des Verantwortlichen für die Datei/Datensammlung festzustellen;

b in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermäßige Kosten die Bestätigung zu erhalten, ob Daten über ihn in einer automatisierten Datei/Datensammlung mit personenbezogenen Daten gespeichert sind, sowie zu erwirken, daß ihm diese Daten in verständlicher Form mitgeteilt werden;

c gegebenenfalls diese Daten berichtigen oder löschen zu lassen, wenn sie entgegen den Vorschriften des innerstaatlichen Rechts verarbeitet worden sind, welche die Grundsätze der Artikel 5 und 6 verwirklichen;

d über ein Rechtsmittel zu verfügen, wenn seiner Forderung nach Bestätigung oder gegebenenfalls nach Mitteilung, Berichtigung oder Löschung im Sinne der Buchstaben b und c nicht entsprochen wird.

Artikel 9 – Ausnahmen und Einschränkungen

1 Ausnahmen von den Artikeln 5, 6 und 8 sind nicht zulässig, abgesehen von den in diesem Artikel vorgesehenen.

2 Eine Abweichung von den Artikeln 5, 6 und 8 ist zulässig, wenn sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist:

a zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten;

b zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter.

3 Die Ausübung der Rechte nach Artikel 8 Buchstaben b, c und d kann durch Gesetz für automatisierte Dateien/Datensammlungen mit personenbezogenen Daten eingeschränkt werden, die Zwecken der Statistik oder der wissenschaftlichen Forschung dienen, wenn offensichtlich keine Gefahr besteht, daß der Persönlichkeitsbereich der Betroffenen beeinträchtigt wird.

Artikel 10 – Sanktionen und Rechtsmittel

Jede Vertragspartei verpflichtet sich, geeignete Sanktionen und Rechtsmittel für Verletzungen der Vorschriften des innerstaatlichen Rechts, welche die in diesem Kapitel aufgestellten Grundsätze für den Datenschutz verwirklichen, festzulegen.

Artikel 11 – Weitergehender Schutz

Dieses Kapitel ist nicht so auszulegen, als ob es die Möglichkeit begrenze oder auf andere Weise beeinträchtige, daß eine Vertragspartei den Betroffenen ein größeres Maß an Schutz als das in diesem Übereinkommen vorgeschriebene gewährt.

Kapitel III – Grenzüberschreitender Datenverkehr

Artikel 12 – Grenzüberschreitender Verkehr personenbezogener Daten und innerstaatliches Recht

1 Werden personenbezogene Daten, die automatisch verarbeitet werden oder für eine solche Verarbeitung beschafft worden sind, – mittels welcher Datenträger auch immer – über die Staatsgrenzen hinweg weitergegeben, so finden die folgenden Bestimmungen Anwendung.

2 Eine Vertragspartei darf allein zum Zweck des Schutzes des Persönlichkeitsbereichs den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei nicht verbieten oder von einer besonderen Genehmigung abhängig machen.

3 Jede Vertragspartei ist jedoch berechtigt, von Absatz 2 abzuweichen:

a soweit ihr Recht für bestimmte Arten von personenbezogenen Daten oder automatisierten Dateien/Datensammlungen mit personenbezogenen Daten wegen der Beschaffenheit dieser Arten besondere Vorschriften enthält, es sei denn, die Vorschriften der anderen Vertragspartei sehen einen gleichwertigen Schutz vor;

b um zu verhindern, daß ihr Recht dadurch umgangen wird, daß eine Weitergabe aus ihrem Hoheitsgebiet in das Hoheitsgebiet einer Nichtvertragspartei auf dem Weg über das Hoheitsgebiet einer anderen Vertragspartei erfolgt.

Kapitel IV – Gegenseitige Hilfeleistung

Artikel 13 – Zusammenarbeit zwischen den Vertragsparteien

1 Die Vertragsparteien verpflichten sich, einander bei der Durchführung dieses Übereinkommens Hilfe zu leisten.

2 Zu diesem Zweck:

a bezeichnet jede Vertragspartei eine oder mehrere Behörden und teilt deren amtliche Bezeichnung und Anschrift dem Generalsekretär des Europarats mit;

b legt jede Vertragspartei, die mehrere Behörden bezeichnet hat, die Zuständigkeit jeder Behörde fest und gibt sie in ihrer Mitteilung nach Buchstabe a an.

3 Eine bezeichnete Behörde einer Vertragspartei wird auf Ersuchen einer bezeichneten Behörde einer anderen Vertragspartei:

a Auskünfte über Recht und Verwaltungspraxis im Bereich des Datenschutzes erteilen;

b in Übereinstimmung mit dem innerstaatlichen Recht und allein zum Zweck des Schutzes des Persönlichkeitsbereichs alle geeigneten Maßnahmen treffen, um Sachauskünfte über eine bestimmte automatische Verarbeitung, die in ihrem Hoheitsgebiet durchgeführt wird, zu erteilen, jedoch mit Ausnahme der dabei verarbeiteten personenbezogenen Daten.

Artikel 14 – Unterstützung von Betroffenen, die im Ausland wohnen

1 Jede Vertragspartei unterstützt Personen, die im Ausland wohnen, bei der Ausübung der Rechte, die ihnen nach dem innerstaatlichen Recht zustehen, das die in Artikel 8 aufgestellten Grundsätze verwirklicht.

2 Eine im Hoheitsgebiet einer anderen Vertragspartei wohnende Person kann ihren Antrag über die bezeichnete Behörde dieser Vertragspartei stellen.

3 Der Antrag auf Unterstützung muß alle erforderlichen Angaben enthalten, insbesondere über:

a den Namen, die Anschrift und alle anderen für die Identifizierung des Antragstellers erheblichen Einzelheiten;

b die automatisierte Datei/Datensammlung mit personenbezogenen Daten oder den dafür Verantwortlichen, auf die sich der Antrag bezieht;

c den Zweck des Antrags.

Artikel 15 – Sicherheiten bei Hilfeleistung durch bezeichnete Behörden

1 Hat eine bezeichnete Behörde einer Vertragspartei von einer bezeichneten Behörde einer anderen Vertragspartei Auskünfte erhalten, die einem Antrag auf Unterstützung dienen oder Antwort auf ein eigenes Ersuchen geben, so darf sie diese Auskünfte nur zu den Zwecken verwenden, die dem Antrag oder Ersuchen zugrunde liegen.

2 Jede Vertragspartei sorgt dafür, daß die Personen, die der bezeichneten Behörde angehören oder in ihrem Namen handeln, durch entsprechende Verpflichtungen zur Geheimhaltung oder zur vertraulichen Behandlung dieser Auskünfte gebunden werden.

3 Es ist einer bezeichneten Behörde in keinem Fall erlaubt, nach Artikel 14 Absatz 2 im Namen eines im Ausland wohnenden Betroffenen von sich aus und ohne dessen ausdrückliche Zustimmung einen Antrag auf Unterstützung zu stellen.

Artikel 16 – Ablehnung von Ersuchen und Anträgen

1 Eine bezeichnete Behörde, an die nach Artikel 13 ein Ersuchen oder nach Artikel 14 ein Antrag gerichtet wird, kann nur ablehnen, ihnen stattzugeben, wenn:

a sie mit den Befugnissen der für die Beantwortung zuständigen Behörden auf dem Gebiet des Datenschutzes nicht vereinbar sind;

b sie den Bestimmungen dieses Übereinkommens nicht entsprechen;

c ihre Erfüllung mit der Souveränität, der Sicherheit oder der öffentlichen Ordnung der Vertragspartei, die sie bezeichnet hat, oder mit den Rechten und Grundfreiheiten der Personen, die der Gerichtsbarkeit dieser Vertragspartei unterstehen, nicht vereinbar wäre.

Artikel 17 – Kosten und Verfahren

1 Für Hilfe, welche die Vertragsparteien einander nach Artikel 13 leisten, oder für Unterstützung, die sie Betroffenen im Ausland nach Artikel 14 leisten, werden keine Auslagen oder Gebühren außer für Sachverständige und Dolmetscher erhoben. Diese Auslagen oder Gebühren werden von der Vertragspartei getragen, welche die ersuchende Behörde bezeichnet hat.

2 Der Betroffene kann nicht verpflichtet werden, für Schritte, die im Hoheitsgebiet einer anderen Vertragspartei für ihn unternommen werden, höhere Auslagen oder Gebühren zu zahlen, als von Personen erhoben werden können, die im Hoheitsgebiet der betreffenden Vertragspartei wohnen.

3 Die sonstigen Einzelheiten im Zusammenhang mit der Hilfeleistung oder Unterstützung, insbesondere hinsichtlich der Form und der Verfahren sowie der zu verwendenden Sprachen, werden unmittelbar zwischen den beteiligten Vertragsparteien festgelegt.

Kapitel V – Beratender Ausschuß

Artikel 18 – Zusammensetzung des Ausschusses

1 Nach dem Inkrafttreten dieses Übereinkommens wird ein Beratender Ausschuß eingesetzt.

2 Jede Vertragspartei ernennt einen Vertreter und einen Stellvertreter für diesen Ausschuß. Jeder Mitgliedstaat des Europarats, der nicht Vertragspartei des Übereinkommens ist, hat das Recht, sich im Ausschuß durch einen Beobachter vertreten zu lassen.

3 Der Beratende Ausschuß kann durch einstimmigen Beschluß jeden Nichtmitgliedstaat des Europarats, der nicht Vertragspartei des Übereinkommens ist, einladen, sich durch einen Beobachter in einer seiner Sitzungen vertreten zu lassen.

Artikel 19 – Aufgaben des Ausschusses

Der Beratende Ausschuß:

a kann Vorschläge zur Erleichterung oder Verbesserung der Anwendung des Übereinkommens machen;

b kann in Übereinstimmung mit Artikel 21 änderungen dieses Übereinkommens vorschlagen:

c nimmt zu jeder vorgeschlagenen änderung dieses Übereinkommens Stellung, die ihm nach Artikel 21 Absatz 3 unterbreitet wird;

d kann auf Ersuchen einer Vertragspartei zu allen Fragen im Zusammenhang mit der Anwendung dieses Übereinkommens Stellung nehmen.

Artikel 20 – Verfahren

1 Der Beratende Ausschuß wird vom Generalsekretär des Europarats einberufen. Seine erste Sitzung findet innerhalb von zwölf Monaten nach Inkrafttreten dieses Übereinkommens statt. Danach tritt er mindestens alle zwei Jahre sowie immer dann zusammen, wenn ein Drittel der Vertreter der Vertragsparteien dies verlangt.

2 Der Beratende Ausschuß ist in einer Sitzung beschlußfähig, wenn die Mehrheit der Vertreter der Vertragsparteien anwesend ist.

3 Im Anschluß an jede Sitzung unterbreitet der Beratende Ausschuß dem Ministerkomitee des Europarats einen Bericht über seine Arbeit und die Wirksamkeit des Übereinkommens.

4 In Übereinstimmung mit diesem Übereinkommen gibt sich der Beratende Ausschuß eine Geschäftsordnung.

Kapitel VI – Änderungen

Artikel 21 – Änderungen

1 Änderungen dieses Übereinkommens können von einer Vertragspartei, vom Ministerkomitee des Europarats oder vom Beratenden Ausschuß vorgeschlagen werden.

2 Der Generalsekretär des Europarats teilt jeden Änderungsvorschlag den Mitgliedstaaten des Europarats sowie jedem Nichtmitgliedstaat mit, der diesem Übereinkommen beigetreten ist oder der nach Artikel 23 eingeladen worden ist, ihm beizutreten.

3 Darüber hinaus wird jede von einer Vertragspartei oder vom Ministerkomitee vorgeschlagene Änderung dem Beratenden Ausschuß übermittelt; dieser teilt dem Ministerkomitee seine Stellungnahme zu der vorgeschlagenen Änderung mit.

4 Das Ministerkomitee prüft die vorgeschlagene Änderung und die Stellungnahme des Beratenden Ausschusses und kann die Änderung genehmigen.

5 Der Wortlaut einer Änderung, die das Ministerkomitee nach Absatz 4 genehmigt hat, wird den Vertragsparteien zur Annahme zugeleitet.

6 Eine nach Absatz 4 genehmigte Änderung tritt am dreißigsten Tag nach dem Zeitpunkt in Kraft, zu dem alle Vertragsparteien dem Generalsekretär ihre Annahme mitgeteilt haben.

Kapitel VII – Schlußklauseln

Artikel 22 – Inkrafttreten

1 Dieses Übereinkommen liegt für die Mitgliedstaaten des Europarats zur Unterzeichnung auf. Es bedarf der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.

2 Das Übereinkommen tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Mitgliedstaaten des Europarats nach Absatz 1 ihre Zustimmung ausgedrückt haben, durch das Übereinkommen gebunden zu sein.

3 Für jeden Mitgliedstaat, der später seine Zustimmung ausdrückt, durch das Übereinkommen gebunden zu sein, tritt es am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegung der Ratifikations-, Annahme- oder Genehmigungsurkunde folgt.

Artikel 23 – Beitritt von Nichtmitgliedstaaten

1 Nach Inkrafttreten dieses Übereinkommens kann das Ministerkomitee des Europarats durch einen mit der in Artikel 20 Buchstabe d der Satzung vorgesehenen Mehrheit und mit einhelliger Zustimmung der Vertreter der Vertragsstaaten, die Anspruch auf einen Sitz im Komitee haben, gefaßten Beschluß jeden Nichtmitgliedstaat des Rates einladen, dem Übereinkommen beizutreten.

2 Für jeden beitretenden Staat tritt das Übereinkommen am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegung der Beitrittsurkunde beim Generalsekretär des Europarats folgt.

Artikel 24 – Räumlicher Geltungsbereich

1 Jeder Staat kann bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde einzelne oder mehrere Hoheitsgebiete bezeichnen, auf die dieses Übereinkommen Anwendung findet.

2 Jeder Staat kann jederzeit danach durch eine an den Generalsekretär des Europarats gerichtete Erklärung die Anwendung dieses Übereinkommens auf jedes weitere in der Erklärung bezeichnete Hoheitsgebiet erstrecken. Das Übereinkommen tritt für dieses Hoheitsgebiet am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Erklärung beim Generalsekretär folgt.

3 Jede nach den Absätzen 1 und 2 abgegebene Erklärung kann in bezug auf jedes darin bezeichnete Hoheitsgebiet durch eine an den Generalsekretär des Europarats gerichtete Notifikation zurückgenommen werden. Die Zurücknahme wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von sechs Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

Artikel 25 – Vorbehalte

Vorbehalte zu diesem Übereinkommen sind nicht zulässig.

Artikel 26 – Kündigung

1 Jede Vertragspartei kann dieses Übereinkommen jederzeit durch eine an den Generalsekretär des Europarats gerichtete Notifikation kündigen.

2 Die Kündigung wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von sechs Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

Artikel 27 – Notifikationen

Der Generalsekretär des Europarats notifiziert den Mitgliedstaaten des Rates und jedem Staat, der diesem Übereinkommen beigetreten ist:

a jede Unterzeichnung;

b jede Hinterlegung einer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde;

c jeden Zeitpunkt des Inkrafttretens dieses Übereinkommens nach den Artikeln 22, 23 und 24;

d jede andere Handlung, Notifikation oder Mitteilung im Zusammenhang mit diesem Übereinkommen.

Zu Urkund dessen haben die hierzu gehörig befugten Unterzeichneten dieses Übereinkommen unterschrieben.

Geschehen zu Straßburg am 28. Januar 1981 in englischer und französicher Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist, in einer Urschrift, die im Archiv des Europarats hinterlegt wird. Der Generalsekretär des Europarats übermittelt allen Mitgliedstaaten des Europarats und allen zum Beitritt zu diesem Übereinkommen eingeladenen Staaten beglaubigte Abschriften.