Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter**
**EDÖB**

8. Datenschutztag

# Modernisierung und Rolle der Datenschutzkonvention des Europarates

Freitag, 24. Jänner 2014, Wien

## Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108)

Jean-Philippe Walter, Dr. iur.
Stellvertreter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten
Präsident des Beratenden Ausschusses (Übereinkommen 108)

### I. Einleitung

Am 28. Januar 2011 konnte das 30-Jahr-Jubiläum der Ratifizierung des Übereinkommens des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) im Rahmen des Datenschutztages gefeiert werden. Der Europarat und der Beratende Ausschuss des Übereinkommens 108 haben diesen Tag zum Anlass genommen, die Überarbeitung des einzigen international verbindlichen rechtlichen Instruments in diesem Bereich in Angriff zu nehmen. Die Bestimmungen des Übereinkommens und des Zusatzprotokolls haben in Bezug auf die Verarbeitung personenbezogener Daten keineswegs an Bedeutung verloren; es sind aber Anpassungen nötig, um besser auf Herausforderungen wie die Globalisierung, die technischen Entwicklungen, die multifunktionalen,

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

ortsunabhängigen technischen Anwendungen sowie die Masseneffekte der Technik reagieren zu können, weil diese Faktoren den Persönlichkeitsbereich und das Recht auf Datenschutz belasten.

Das Übereinkommen 108 ist und bleibt eine ausgezeichnete Grundlage, die es ermöglicht, den berechtigten Erwartungen sowohl von betroffenen Personen als auch von Personen, die für die Datenverarbeitung verantwortlich sind, gerecht zu werden und gleichzeitig die Wirksamkeit des Datenschutzes zu erhöhen und dafür zu sorgen, dass die wichtigsten Grundsätze besser umgesetzt werden. Erlauben Sie mir, einleitend die wichtigsten Punkte des Übereinkommens 108 und des Zusatzprotokolls in Erinnerung zu rufen:

- Das Übereinkommen ist ein Referenzwerk für zahlreiche internationale und nationale Erlasse wie die Richtlinie 95/46/EG, die eine Weiterentwicklung der Grundsätze des Übereinkommens darstellt.
- Mit dem Zusatzprotokoll ist das Übereinkommen das erste und einzige internationale Dokument mit verbindlichen Bestimmungen für den Datenschutz. Bis heute haben etwa 80 Staaten aus 5 Kontinenten den Datenschutz gesetzlich geregelt. Mehr als die Hälfte dieser Staaten sind Vertragsparteien des Übereinkommens. Dieses wurde von 45 der 47 Mitgliedsstaaten des Europarats ratifiziert, darunter auch die 28 Mitglieder der Europäischen Union.
- Das Übereinkommen enthält die Grundsätze des Datenschutzes, die auf der ganzen Welt anerkannt sind. Die rechtlichen Bestimmungen sind absolut kohärent mit anderen Texten wie den entsprechenden Richtlinien der OECD oder den Richtlinien der Vereinten Nationen.
- Das Übereinkommen ist einfach und allgemein gehalten und verfolgt einen sogenannten «technologisch neutralen Approach», damit die Aktualität der grundlegenden rechtlichen Bestimmungen erhalten bleibt, die technischen Entwicklungen aber nachvollzogen werden können, ohne dass das Schutzniveau sinkt oder dass durch die Anpassung an bestimmte Anforderungen und Situationen eine Verstärkung des Schutzes ausgeschlossen wird.

- Die Anwendung des Übereinkommens ist horizontaler Art. Es umfasst sämtliche automatisierte Verarbeitungen von personenbezogenen Daten aus dem privaten und dem öffentlichen Bereich, einschliesslich durch Justiz- und Polizeibehörden und den Nachrichtendienst.
- Durch die Vereinbarkeit des Rechts mit der Achtung des Persönlichkeitsbereichs und der Informationsfreiheit (insbesondere das Recht auf freien, grenzüberschreitenden Datenverkehr) garantiert das Übereinkommen in den existierenden Rechtssystemen ein hohes Schutzniveau und gewährleistet grundsätzlich den freien Datenverkehr zwischen den Teilnehmerstaaten. Gleichzeitig verlangt das Zusatzprotokoll ein angemessenes Schutzniveau beim Datenverkehr mit Ländern, die das Übereinkommen nicht unterzeichnet haben.
- Das Übereinkommen regelt die Zusammenarbeit zwischen den Vertragsparteien und die Unterstützung der betroffenen Personen, unabhängig von deren Staatsangehörigkeit oder Wohnort. Es sorgt durch den Beratenden Ausschuss für eine multilaterale Zusammenarbeitsplattform.
- Das Übereinkommen wurde unter Mitwirkung von Nichtmitgliedstaaten des Europarats erarbeitet (USA, Kanada, Australien und Japan) und ist damit kein rein europäisches Dokument. Der Beitritt steht auch Drittstaaten offen, was ein weltweites Potenzial eröffnet. So ist im August 2013 Uruguay als erster Nichtmitgliedstaat des Europarats dem Übereinkommen und dem Zusatzprotokoll beigetreten; der Beitritt Marokkos steht demnächst bevor.

## II. Die Ziele der Überarbeitung

Die oben erwähnten Punkte dienten für die laufenden Arbeiten als Orientierungshilfe. Damit sollen die nachstehenden Ziele verfolgt werden:

- Die Herausforderungen für die Privatsphäre, die aufgrund der Verwendung von Informations- und Telekommunikationstechnologien entstehen, müssen angegangen werden.

- Das Recht auf Datenschutz im Sinne eines bei der Ausübung anderer grundlegender Rechte und Freiheiten unverzichtbaren Grundrechts soll bei der Verarbeitung personenbezogener Daten gestärkt werden. Es geht insbesondere darum, den Menschen einen adäquateren Umgang mit den Daten, die sie betreffen, zu ermöglichen und die Wahrung der Menschenwürde bei der Verarbeitung von Personendaten zu garantieren.
- Das Recht auf Datenschutz soll mit der Ausübung anderer Grundrechte und Freiheiten vereinbar werden, insbesondere mit der Freiheit der Meinungsäusserung, die in der Welt des Internets eine ganz andere Dimension erhalten hat, und mit dem Recht auf Zugang zu amtlichen Dokumenten.
- Die Mechanismen zur Umsetzung und Kontrolle des Übereinkommens sollen gestärkt werden.
- Der allgemeine Charakter und die technologische Neutralität der Bestimmungen sollen gewahrt werden. Gleichzeitig soll das Dokument aber in gewissen Bereichen durch spezifische sektorielle Bestimmungen ergänzt werden.
- Die Kohärenz und die Vereinbarkeit mit dem Recht der Europäischen Union müssen gewährleistet sein.
- Der globale Anspruch und der offene Charakter des Übereinkommens sollen gewahrt und gestärkt werden.

Auf der Grundlage dieser Ziele hat das Büro des Beratenden Ausschusses ein Projekt vorbereitet, das vom Beratenden Ausschuss anlässlich der 29. Vollversammlung im November 2012 verabschiedet wurde.[1] Dieses Projekt wird zurzeit vom zwischenstaatlichen Ad-hoc-Komitee (CAHDATA) geprüft, das den Text fertigstellen und ein Protokoll zur Änderung des Übereinkommens vorbereiten muss.

[1] www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2904Rev4_F_Convention%20108%20modernis%C3%A9e%20version%20F.pdf

## III. Das Projekt in groben Zügen

### 1. Gegenstand und Zweck

Unter Artikel 1 soll der Zweck des Übereinkommens klarer geregelt werden. Konkret geht es darum, jeder natürlichen Person, die der Gerichtsbarkeit einer Vertragspartei untersteht, unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnort, das Recht auf den Schutz personenbezogener Daten zu gewähren, um die Wahrung ihrer anderen Grundrechte und Freiheiten, insbesondere das Recht auf einen Persönlichkeitsbereich bei der Datenverarbeitung, garantieren zu können. Mit dieser Formulierung schafft das Übereinkommen keine rechtlichen Hierarchien, sondern ruft in Erinnerung, dass die Verarbeitung von personenbezogenen Daten andere Menschenrechte tangiert, und dass deren Einhaltung mit der Gewährleistung des Datenschutzrechts einhergeht. Dieses Recht ist mit sämtlichen anderen Grundrechte und Freiheiten verknüpft, ja, es verstärkt sie. Es ist somit die Basis, auf der sämtliche Grundrechte und Freiheiten beruhen, die bei der Verarbeitung personenbezogener Daten betroffen sind. Es darf aber nicht als absolutes Vorrecht betrachtet werden, sondern ist vielmehr in Bezug auf seine Funktion in der Gesellschaft zu verstehen.[2] Nach dem Verhältnismässigkeitsprinzip darf dieses Recht nicht so ausgeübt werden, dass die Ausübung anderer Menschenrechte verhindert wird, sondern es geht darum, die verschiedenen existierenden Rechte miteinander vereinbar zu machen.

### 2. Geltungsbereich und Begriffsbestimmungen

Im Vergleich zum geltenden Recht sieht der Änderungsentwurf vor, den Geltungsbereich auf sämtliche automatisierten und nicht automatisierten Verarbeitungen von Personendaten, die der Gerichtsbarkeit einer Vertragspartei unterstehen, auszudehnen. Datenverarbeitungen im öffentlichen und privaten Bereich, einschliesslich durch Justiz- und Polizeibehörden, Armee und Nachrichtendienst, sind weiterhin abge-

[2] Siehe Erwägungsgrund 139 des Entwurfs zur europäischen Verordnung; vgl. Urteil der Gerichthofs der Europäischen Union, C-92/09 und C-93/09 *Volker et Markus Schecke*[2010] CJE I-0000, §§ 48, 50 et 86

deckt. Die manuelle Verarbeitung wird insofern integriert, als die Daten Teil eines Ganzen sind, dessen Struktur es erlaubt, die Daten von bestimmten Personen nach definierten Kriterien zu suchen. Zurzeit ist diese Art von Verarbeitung nur abgedeckt, wenn ein Mitgliedstaat den Geltungsbereich selbst um die manuelle Verarbeitung erweitert. Die Verarbeitung von Daten durch die dafür verantwortlichen Personen untersteht der Gerichtsbarkeit einer Vertragspartei, wenn zwischen dem Hoheitsgebiet der Vertragspartei und der Verarbeitung ein genügend enger Zusammenhang besteht. Selbst wenn dies nicht explizit aus dem Wortlaut hervorgeht, ist es – wie der Verordnungsentwurf der Europäischen Union zeigt – möglich, unter dem Ausdruck «der Gerichtsbarkeit einer Vertragspartei unterstehen» auch Verarbeitungen zu subsumieren, die von Tätigkeiten (z.B. Verhaltensanalysen) oder Dienstleistungen gegenüber Personen im Hoheitsgebiet einer Vertragspartei herrühren, wenn diese Verarbeitungen von Personen ausgeübt werden, die nicht unter die Gerichtsbarkeit einer Vertragspartei des Übereinkommens fallen.

Das Übereinkommen sollte jedoch nicht mehr auf Datenverarbeitungen angewendet werden, die von natürlichen Personen ausschliesslich für persönliche oder private Zwecke dienen. Dieser Ausschluss will verhindern, dass natürlichen Personen, die in ihrer Privatsphäre Daten ohne kommerzielle oder berufliche Zwecke verarbeiten, unverhältnismässige Auflagen gemacht werden. Dabei handelt es sich um private Tätigkeiten wie das Sammeln von Bildern, das Führen von Listen mit Namen von Freunden oder Familienangehörigen, Korrespondenz usw. Dem Phänomen der sozialen Netzwerke, Blogs und anderer Internetdienste, bei denen persönliche Informationen in rein privatem Rahmen geteilt werden, ist in diesem Zusammenhang besondere Beachtung zu schenken. Es ist schwierig, einschränkende Kriterien festzulegen: Zurzeit lautet der Grundsatz, dass das Übereinkommen uneingeschränkt umgesetzt wird, sobald Personen ausserhalb des persönlichen oder privaten Bereichs Zugang zu persönlichen Daten haben. Nach einem Urteil Zürcher Obergerichts ist sogar eine Veröffentlichung auf Facebook, die nur dem Freundeskreis zugänglich ist, als öffentlich zu betrachten: «Nach der Rechtsprechung gelte grundsätzlich alles als öffentlich, was nicht im privaten Rahmen erfolge. In privatem Rahmen erfolge eine Äusserung

nur, wenn sie an den Familien- oder Freundeskreis gerichtet sei oder an ein Umfeld, das durch persönliche Beziehungen oder ein besonderes Vertrauen geprägt sei.»[3] Die Veröffentlichung in einem sozialen Netzwerk bietet keine solchen Garantien. Der vorgeschlagene Ausschluss gilt nicht für Personen, die für die Datenverarbeitung zuständig sind, oder für Auftragsverarbeiter, welche die nötigen Mittel zur Verfügung stellen, um personenbezogene Daten für solche persönlichen oder privaten Zwecke zu verarbeiten.

Das Übereinkommen sieht keine Möglichkeit vor, Vorbehalte zu machen. Die Vertragsparteien haben jedoch die Möglichkeit, mittels einer Erklärung gegenüber dem Generalsekretariat des Europarats gewisse automatisierte Datensammlungen mit personenbezogenen Daten vom Geltungsbereich auszuschliessen. Diese Möglichkeit darf nicht als verstecktes Mittel interpretiert werden, um dennoch Vorbehalte anzubringen. Die Staaten sollen vielmehr die Möglichkeit haben, Verarbeitungen, die zur Zeit der Ratifizierung noch nicht dem Datenschutz unterworfen waren, die aber zu einem späteren Zeitpunkt davon erfasst wurden, vom Übereinkommen auszuklammern. Dabei kann es sich nicht um eine dauerhafte Lösung handeln. Der Ausschuss schlägt vor, diese Möglichkeit, die in den 1980er-Jahren sinnvoll war, heute aber nicht mehr gerechtfertigt ist, nicht länger vorzusehen.

Was die Begriffsbestimmungen betrifft, so sind diese zu aktualisieren. Als erstes wird der Begriff der «bestimmbaren Person» präzisiert. So ist eine Person nicht bestimmbar, wenn ihre Identifizierung mit einem zu grossen zeitlichen oder anderen Aufwand verbunden ist. Mit «bestimmbar» sind nicht nur die zivilen Bestandteile der Identität eines Individuums gemeint, sondern auch, was diese Person von anderen Personen unterscheiden kann. Dies ist mit Hilfe einer Identifikationsnummer, von Lokalisierungsdaten, einem Online-Identifikator (z.B. IP-Adresse) oder anderen Informationen möglich, die zur physischen, physiologischen, genetischen oder psychischen Identität zählen.

[3] Tagesanzeiger vom 26. Nov. 2013

Ausserdem wird der Begriff der Datensammlung nicht mehr verwendet. Der Begriff des «Verantwortlichen für die Datei/Datensammlung» wird ersetzt durch den Begriff «für die Verarbeitung verantwortliche Person». Ausserdem wird die Aufzählung durch die Begriffe «Auftragsverarbeiter» und «Empfänger» ergänzt. Im Gegensatz zum europäischen Projekt hat der Beratende Ausschuss die Definitionen «genetische Daten» und «biometrische Daten» nicht aufgenommen, da man – meines Erachtens zu Recht – der Meinung war, dass diese Begriffe dem Wandel der Zeit unterliegen. Es wäre darum verfrüht, sie in einem Rechtstext zu definieren. Es ist jedoch nicht auszuschliessen, dass das CAHDATA diese beiden Begriffe einführt und sich dabei an die Arbeit des Komitees des Europarats über die Bioethik anlehnt.

## 3. Pflichten der Vertragsparteien

Das Übereinkommen wird nicht direkt angewendet. Nach Artikel 4 trifft jede Vertragspartei in ihrem innerstaatlichen Recht die erforderlichen Massnahmen, um die Bestimmungen anzuwenden. Dies hat spätestens dann zu geschehen, wenn das Übereinkommen in Kraft tritt. Zurzeit gibt es keine Möglichkeit, zu kontrollieren, ob die Massnahmen wirklich getroffen wurden und ob sie auch greifen. Der Beratende Ausschuss schlägt deshalb vor, in Zukunft einerseits zu fordern, dass die Massnahmen vor der Ratifizierung oder dem Beitritt getroffen werden. Andererseits soll der «Beitrittskandidat» ebenfalls vor der Ratifizierung oder dem Beitritt beweisen, dass er die Massnahmen getroffen hat und dass sie wirksam sind. Mit der Ratifizierung oder dem Beitritt erklären sich die Vertragsparteien damit einverstanden, dass der Ausschuss die Einhaltung der Verpflichtungen überprüfen kann. Sie müssen eine solche Überprüfung ausserdem aktiv unterstützen. Dies ist ein wichtiger Schritt, um die Wirksamkeit des Datenschutzes und das Engagement der Vertragsparteien, sich an die Verpflichtungen des Übereinkommens zu halten, zu verstärken.

## 4. Grundsätze für den Datenschutz

Artikel 5 des Übereinkommens regelt die Grundsätze für den Datenschutz: Rechtmässigkeit, Treu und Glauben, Zweckmässigkeit, Verhältnismässigkeit und Richtigkeit. Diese Grundsätze reichen an sich aus, um die unterschiedlichen Verarbeitungen von Personendaten abzudecken. Der Beratende Ausschuss hält es aber für nötig, das Verhältnismässigkeitsprinzip nach Artikel 5 Buchstabe c des Übereinkommens zu stärken und den Text entsprechend zu ergänzen. Die von dieser Bestimmung betroffenen Daten «müssen den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen». Das Verhältnismässigkeitsprinzip muss aber auch für die Verarbeitung und im Speziellen für die Wahl der Mittel und der Methoden gelten. Die Verarbeitung muss verhältnismässig, also geeignet und erforderlich sein, um den verfolgten rechtmässigen Zweck zu erreichen, und sie muss ein ausgewogenes Gleichgewicht zwischen den vorhandenen öffentlichen und privaten Interessen sowie den Grundrechten und Freiheiten, um die es geht, darstellen. Es sind diejenigen Mittel der Verarbeitung zu wählen, die am wenigsten in die Grundrechte und Freiheiten eingreifen. Dieser Grundsatz muss zu jedem Zeitpunkt gewährleistet sein, und er wird ergänzt durch den Grundsatz der Datenbeschränkung, wonach Datensammlung und -verarbeitung auf das absolut notwendige Minimum zu begrenzen sind.

Zurzeit regelt das Übereinkommen nicht, welche Zwecke eine Verarbeitung legitimieren. Es sieht lediglich allgemein vor, dass jede Verarbeitung von Daten rechtmässig sein muss. Der Änderungsentwurf enthält eine neue Bestimmung, die besagt, dass Daten nur dann verarbeitet werden dürfen, wenn die betroffene Person informiert wurde und freiwillig eingewilligt hat, oder wenn die Verarbeitung auf einer anderen gesetzlich geregelten Grundlage beruht. Um die Anpassungsfähigkeit und den allgemeinen Charakter des Übereinkommens zu gewährleisten, werden die Einzelheiten, welche Gründe als rechtmässig gelten, nicht näher geregelt. Die Gründe nach Artikel 7 der Richtlinie 95/46/EG sind damit aber auf jeden Fall abgedeckt. Dabei geht es insbesondere um Fälle, in denen eine Datenverarbeitung nötig ist, um einen

Vertrag (oder vorvertragliche Massnahmen) zu erfüllen, um lebenswichtige Interessen der betroffenen Person zu schützen, oder um Fälle, in denen schwerwiegende gesetzliche Gründe die Verarbeitung rechtfertigen.

Die Einwilligung sollte, sofern sie verlangt wird, unabhängig von der Art der Daten zumindest klar und eindeutig sein. Diese Änderung wird dadurch gerechtfertigt, dass es insbesondere in der virtuellen Welt offenbar nötig ist, jede Zweideutigkeit betreffend die Gültigkeit der Einwilligung auszuräumen. Besonders wichtig ist dies bei Online-Datenverarbeitungen. Eine gültige Einwilligung bedingt eine ausdrückliche und bestätigende Handlung der betroffenen Person. Dabei ist Schriftlichkeit nicht nötig: Daraus lässt sich ableiten, «dass die für die Datenverarbeitung Verantwortlichen als Folge der Forderung nach einer Einwilligung ohne jeden Zweifel, de facto dazu angehalten werden, Verfahren und Mechanismen anzuwenden, die keinen Zweifel daran lassen, dass die Einwilligung erteilt wurde. Dies kann entweder eine ausdrückliche Handlung der Person sein oder eine Handlung der Person, aus der die Einwilligung eindeutig geschlossen werden kann.»[4] Die Einführung einer solchen Bestimmung zur ausdrücklichen Einwilligung ist noch offen und wird nicht von allen Seiten gutgeheissen. Ein Kompromiss ist eventuell durch die Verwendung des Begriffs der *eindeutigen Einwilligung* möglich. Schliesslich muss die Einwilligung im Sinne des Grundsatzes von Treu und Glauben jederzeit widerrufbar sein.

## 5. Besonders schützenswerte Personendaten

Was besonders schützenswerte Personendaten betrifft, so wird am Grundsatz des Verarbeitungsverbots festgehalten, sofern innerstaatlich keine ausreichenden Schutzmechanismen vorhanden sind. Der Änderungsentwurf präzisiert die nötigen Garantien in ihren Grundzügen. Diese Garantien dienen dazu, den Risiken – insbesondere dem Risiko der Diskriminierung – vorzubeugen, welche die Verarbei-

[4] Stellungnahme Artikel 29 - Datenschutzarbeitsgruppe 15/2011 zur Definition von Einwilligung, S. 28, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf#h2-3

tung von besonders schützenswerten Personendaten für die Interessen, und die Grundrechte und Freiheiten der betroffenen Person darstellt.

Mit dem Änderungsentwurf wird der Katalog der besonders schützenswerten Daten überarbeitet und um folgende Arten von Daten ergänzt: genetische Daten, biometrische Daten sowie Daten betreffend die Zugehörigkeit zu einer Gewerkschaft, Strafverfolgungen und -urteile, Widerhandlungen und strafrechtliche Massnahmen. Die Bestimmung unterscheidet zwischen Personendaten, die per se besonders schützenswert sind (z.B. genetische Daten), und Personendaten, die durch die Verwendung zu besonders schützenswerten Daten werden, z.B. Daten über den ethnischen Ursprung oder politische Überzeugungen. In dieser zweiten Kategorie liegt der Schwerpunkt auf dem Verarbeitungszweck. So ist das Speichern einer Fotografie in einer Datensammlung nicht zwingend als kritisch zu betrachten, wenn das Ziel der Verarbeitung nicht darin liegt, durch die Analyse der Fotografie bestimmte Informationen zu gewinnen. Der Vorschlag, Daten als besonders schützenswert einzustufen, die durch die Verarbeitung ein hohes Risiko für die Interessen und die Grundrechte und Freiheiten der betroffenen Person (insb. Diskriminierung) darstellen, wurde nicht weiterverfolgt. Der Vorschlag hätte es ermöglicht, gewisse Verarbeitungen nicht nur aufgrund der Art der Daten, sondern auch unter Berücksichtigung des Zwecks und der Umstände der Verarbeitung als besonders schützenswert einzustufen. Eine gewisse Rechtsunsicherheit wäre jedoch die Folge gewesen. Nach Artikel 11 des Übereinkommens kann eine Vertragspartei die Liste besonders schützenswerter Daten erweitern, deren Verarbeitung für die betroffene Person möglicherweise ein erhöhtes Risiko darstellt.

## 6. Datensicherheit

Was die Datensicherheit betrifft, sieht der Änderungsentwurf neu vor, dass Verletzungen des Datenschutzes gemeldet werden müssen. Diese Pflicht geht weniger weit als der europäische Verordnungsentwurf und ist auf signifikante Fälle begrenzt, d.h. Datenschutzverletzungen, welche die grundlegenden Rechte und Freiheiten der

betroffenen Personen stark beeinträchtigen könnten. Die Meldung muss zumindest gegenüber den zuständigen Kontrollbehörden erfolgen. Im Gegensatz zum EU-Verordnungsentwurf sieht der Entwurf des T-PD keine Pflicht vor, auch die betroffenen Personen zu informieren. Die Aufzählung der Gründe wird für die für die Datenverarbeitung verantwortlichen Personen jedoch ein Anreiz sein, in schwerwiegenden Fällen Meldung zu erstatten. Ausserdem können die Kontrollbehörden im Rahmen ihrer Zuständigkeiten die Verantwortlichen dazu auffordern. Diese Lösung lässt genügend Spielraum, um jede Situation einzeln zu beurteilen.

## 7. Transparenz der Verarbeitung

Der Änderungsentwurf sieht vor, dass die Transparenz der Verarbeitung garantiert werden muss. Die für die Verarbeitung verantwortliche Person muss ein Minimum an Information liefern, insbesondere zur Identität, zum gewöhnlichen Aufenthaltsort oder zu ihrem Sitz, zum Zweck der Verarbeitung, zu den Adressaten der Daten, zur Dauer der Aufbewahrung und zu den Möglichkeiten der betroffenen Personen, ihre Rechte auszuüben. Bei Bedarf muss sie zusätzliche Informationen liefern, wenn diese nötig sind, um eine loyale Verarbeitung zu gewährleisten. Dabei geht es zum Beispiel um Informationen zu möglichen Weitergaben von Daten in Drittländer oder zur Ausrichtung einer Datensammlung (auf Pflicht oder Freiwilligkeit basierend). Im Gegensatz zum europäischen Recht und im Sinne des allgemeinen Charakters des Übereinkommens regelt der Entwurf nicht, wann die Information zu erfolgen hat. Damit die betroffenen Personen aber informiert ihre Rechte geltend machen und bei Bedarf eine gültige Einwilligung geben können, muss die Information so früh wie möglich erfolgen, das heisst spätestens bei der Datenbeschaffung, wenn die Daten bei der betroffenen Personen eingeholt werden. Werden die Daten nicht bei den betroffenen Personen eingeholt, so ist dies zum Zeitpunkt der Erfassung oder innerhalb nützlicher Frist erforderlich, spätestens jedoch bei der erstmaligen Weitergabe. Die Art der Information ist von den Umständen der Verarbeitung abhängig. Sie erfolgt aktiv und in geeigneter Form, zum Beispiel über eine Webseite oder ein Informationsschreiben. Die Information erfolgt zudem in angemessener Weise. Dies kann allgemein

oder individuell sein, je nach den Umständen und der Art der Verarbeitung. So muss nicht informiert werden, wenn die Person schon im Besitz der betreffenden Information ist und die Umstände der Verarbeitung sich nicht verändert haben. Werden die Daten bei Dritten erhoben, so ist die für die Verarbeitung verantwortliche Person nicht zur Information verpflichtet, wenn ein Gesetz die Verarbeitung ausdrücklich vorsieht, soweit das Gesetz ausreichend bestimmt und detailliert ist. Weiter entfällt die Informationspflicht, wenn es der verantwortlichen Person nicht möglich ist (materiell oder rechtlich) oder die Information mit einem unverhältnismässigen Aufwand verbunden ist. Ausnahmen von Artikel 9 des Übereinkommens sind auch möglich, wenn es um die Staatssicherheit oder um die Vorbeugung oder Verhinderung von strafrechtlichen Handlungen geht.

## 8. Rechte der betroffenen Personen

Die Rechte der betroffenen Personen werden ebenfalls gestärkt, damit sie eine bessere Kontrolle über ihre Daten ausüben können und um das Recht auf Wahrung der menschlichen Würde und der Nichtdiskriminierung zu garantieren.

### 8.1. Auskunftsrecht und andere Rechte

Beim Auskunftsrecht sieht der Änderungsentwurf vor, dass die Liste der Informationen, die der betroffenen Person gegeben werden müssen, wenn sie um Auskunft ersucht, erweitert wird. Abgesehen von den Informationen, welche die für die Verarbeitung verantwortliche Person unter dem Transparenzgebot liefern muss, sind auch Informationen über die Herkunft der Daten zu liefern. Ausserdem hat die betroffene Person das Recht, über den Hintergrund der Verarbeitung von Daten, die gegen sie vorliegen oder verwendet werden, informiert zu werden. Diese neue Bestimmung ist besonders bei der Erstellung von Profilen wichtig, welche in der Regel automatisch generiert werden[5], und mit einer anderen neuen Regelung zu verbinden: Daten, die

[5] Siehe dazu die Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammen-

eine Person massgeblich betreffen oder die für sie rechtliche Auswirkungen haben, dürfen nicht für Entscheidungen verwendet werden, wenn der Entscheid nur aufgrund einer automatisierten Verarbeitung erfolgt und die betroffene Person ihren Standpunkt nicht darlegen konnte.

Der Änderungsentwurf sieht zudem vor, dass das Übereinkommen explizit das Recht enthält, sich der Verarbeitung von personenbezogenen Daten jederzeit widersetzen zu können, es sei denn, die verantwortliche Person bringe wichtige Gründe vor, welche die Verarbeitung rechtfertigen. Diese Gründe müssen schwerer wiegen als die Interessen sowie die Grundrechte und Freiheiten der betreffenden Person. Der Ausschuss hat jedoch darauf verzichtet, explizit ein (digitales) Recht auf Vergessen einzuführen. Er ist der Ansicht, dass die vorhandenen Garantien (Aufbewahrungsdauer, Recht auf Berichtigung oder Löschung) in Verbindung mit dem Widerspruchsrecht für einen ausreichenden Schutz sorgen. Schliesslich muss die betroffene Person Rekurs einlegen können, wenn die ihr zustehenden Rechte nicht eingehalten werden, und die Datenschutzbehörden haben die nötige Unterstützung zu gewährleisten.

### 8.2. Einschränkungen

Wir sollten uns bewusst sein, dass diese Rechte von betroffenen Personen nicht uneingeschränkt ausgeübt werden können. Nach Artikel 9 des Übereinkommens gibt es Möglichkeiten zur Einschränkung, wenn dies gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist:

- zum Schutz der nationalen und der öffentlichen Sicherheit, zur Wahrung höherer wirtschaftlicher und finanzieller Interessen des Staates und zur Verhütung und Verfolgung von strafrechtlichen Widerhandlungen;
- zum Schutz der betroffenen Person und der Rechte und Freiheiten Dritter; vor allem das Recht auf freie Meinungsäusserung und Informationsfreiheit. Aber

hang mit Profiling
https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282010%2913&Language=lanGerman&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 .

auch das Fernmeldegeheimnis, das Geschäftsgeheimnis, das Handelsgeheimnis und andere gesetzlich geschützte Geheimnisse sind abgedeckt.

Einschränkungen sind auch für Verarbeitungen von Daten denkbar, die zu statistischen oder wissenschaftlichen Zwecken verwendet werden, sofern die Rechte und Freiheiten betroffener Personen dadurch nicht beeinträchtigt werden. Die Ausnahmen nach Artikel 9 betreffen nicht nur die Ausübung der Rechte von betroffenen Personen, sondern auch bestimmte Grundsätze und die Informationspflicht.

Das Übereinkommen 108 sieht keine Möglichkeit vor, Vorbehalte zu machen, und es wird in allen Bereichen angewendet, in denen personenbezogene Daten verarbeitet werden. Nach Artikel 9 ist es jedoch möglich, bei einigen Bestimmungen Ausnahmen zu machen, wenn dies in einer demokratischen Gesellschaft für die oben erwähnten Ziele nötig ist und wenn dies in einem Gesetz vorgesehen ist. Es geht dabei nicht darum, das Übereinkommen einzuschränken und Möglichkeiten zu schaffen, Vorbehalte zu machen, sondern darum, gewisse Grundsätze anzupassen oder einzuschränken oder gewisse Rechte zu begrenzen, um aufgrund von höheren Ansprüchen bestimmte rechtmässige Handlungen vornehmen zu können, die ohne grösseren Eingriff in die Grundrechte und Freiheiten nicht möglich wären. Im Gegensatz zum geltenden Übereinkommen sind keine Ausnahmen zu Artikel 6, der die besonders schützenswerten Personendaten regelt, mehr möglich. Es wird aber noch geprüft, in welchem Masse es zulässig sein soll, Ausnahmen von den Grundsätzen wie Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit und Zweckmässigkeit vorzusehen. Tendenziell geht es in Richtung einer Bestimmung, die es ermöglicht, diese Grundsätze bereichsspezifisch anzupassen.

## 9. Pflichten beim Datenschutz

Die Revision des Übereinkommens muss auch die Verantwortung der Personen stärken, die Daten verarbeiten oder verarbeiten lassen. Der Änderungsentwurf enthält somit den Grundsatz, dass die für die Verarbeitung verantwortliche Person das

Recht auf Datenschutz während jeder Verarbeitungsphase einhalten und alle Massnahmen – auch im Fall von Auftragsverarbeiter – treffen muss, um die Datenschutzbestimmungen umzusetzen. Diese Pflicht erstreckt sich auch auf die Wahl der für die Verarbeitung verwendeten Mittel. Insbesondere müssen Technologien verwendet werden, die die Einhaltung der Grundrechte und Freiheiten gewährleisten. Der Entwurf sieht neu auch die Pflicht der für die Verarbeitung verantwortlichen Person bzw. des Auftragsverarbeiters vor, die möglichen Auswirkungen einer Verarbeitung auf die Rechte und Freiheiten der Einzelpersonen zu analysieren. Die für die Verarbeitung verantwortliche Person muss die Verarbeitung der Daten so konzipieren, dass das Risiko einer Beeinträchtigung des Rechts auf Datenschutz ausgeschlossen oder auf ein Minimum reduziert wird. Sie muss interne Mechanismen umsetzen, die es ermöglichen, den betroffenen Personen und den Datenschutzbehörden zu zeigen, dass bei der Verarbeitung der Daten die geltenden Bestimmungen eingehalten werden. Bei diesen Massnahmen wurde zum Beispiel an die Ernennung eines internen Datenschutzbeauftragten gedacht.

Schliesslich schlägt der Beratende Ausschuss vor, zu verlangen, dass Produkte und Dienstleistungen zur Verarbeitung von personenbezogenen Daten die Implikationen des Datenschutzrechts von Anfang an berücksichtigen und die Konformität der Verarbeitung von Daten mit Blick auf das anwendbare Recht erleichtern müssen (Privacy by design, Privacy by default).

Diese Pflichten und speziell auch die Analyse der Auswirkungen, die bei jeder Verarbeitung von personenbezogenen Daten mit einbezogen werden muss, müssen den möglichen Risiken für die Interessen sowie die grundlegenden Freiheiten und Rechte der betroffenen Personen angemessen sein. Sie müssen insbesondere auch die Art der Verarbeitung oder der Daten, die Anzahl betroffener Personen, die Personenkategorien und die verwendeten Technologien berücksichtigen. Die Grösse des Unternehmens (für die Verarbeitung verantwortliche Person oder Auftragsverarbeiter) und das Volumen der verarbeiteten Daten können in einem gewissen Masse ebenfalls berücksichtigt werden.

## 10. Grenzüberschreitender Datenverkehr

In Artikel 12 des Änderungsentwurfs, der den grenzüberschreitenden Datenverkehr regelt, werden Artikel 12 des geltenden Übereinkommens und Artikel 2 des Zusatzprotokolls zusammengeführt. Es handelt sich um eine zentrale Bestimmung des Übereinkommens, deren Ziel es ist, einerseits den freien Informationsaustausch zwischen den Vertragsparteien grundsätzlich zu ermöglichen, soweit sie ein hohes Datenschutzniveau gewährleisten können. Dies wird erreicht, indem im innerstaatlichen Recht die nötigen Massnahmen getroffen werden, um das Übereinkommen umzusetzen. Andererseits legt der Artikel die Regeln fest, die bei der Übermittlung von Daten an Empfänger gelten, die nicht der Rechtshoheit einer Vertragspartei unterstehen, um den betroffenen Personen bei der Verarbeitung personenbezogener Daten einen angemessenen Schutz zu gewährleisten. Leider wird der grenzüberschreitende Datenverkehr im Änderungsentwurf nicht definiert. Man spricht nur von der Übermittlung von Daten an einen Empfänger, der einer anderen Rechtshoheit untersteht als der Absender. Ob damit auch der Fall abgedeckt ist, wenn Daten Personen ausserhalb der Rechtshoheit der übermittelnden Person weitergegeben oder zugänglich gemacht werden, wird nicht beantwortet. Die Frage, ob die Übermittlung auch die Verbreitung von Daten über das Internet einschliesst, bleibt ebenfalls offen. Es ist in der Tat nicht unrechtmässig, Daten, die im Internet vorhanden sind, der Regelung zum Datenverkehr zu unterstellen, wenn man den Kontrollverlust und die hohen damit verbundenen Risiken berücksichtigt, die bei der Veröffentlichung über diesen Kanal entstehen können. Artikel 12 regelt jedoch nur den Datenexport und nicht den Import.

Der Änderungsentwurf nimmt die Regelung von Artikel 12 auf, wonach die Weitergabe von Daten an einen Adressaten unter der Rechtshoheit einer anderen Vertragspartei aus rein datenschutzrechtlichen Gründen nicht verboten oder mit einer Genehmigung verknüpft werden darf. Der Grundsatz des freien Datenverkehrs zwischen Vertragsparteien, die einen gleichwertigen Datenschutz gewährleisten, ist je-

doch nicht absolut. Der Haken daran ist folgender: Die Möglichkeit, dass eine Vertragspartei sich an verbindliche harmonisierte und gemeinsame Schutzregeln hält, ist Staaten vorbehalten, die einer regionalen internationalen Organisation angehören. Mit anderen Worten geht es bei dieser Bestimmung darum, den Angemessenheitsmechanismus der EU zu erhalten und zu vermeiden, dass Daten einfach so an Personen einer Vertragspartei übermittelt werden, die nicht Mitglied der EU ist und die einer Angemessenheitsfeststellung nicht folgen könnte. Diese Differenzierung hat bei gewissen Staaten ausserhalb der EU bzw. Europas Kritik ausgelöst. Sie könnte sich negativ auf die Attraktivität des Übereinkommens bei Staaten auswirken, die nicht Mitglied des Europarats sind, die dem Übereinkommen aber möglicherweise beitreten würden. Um dieses Risiko zu reduzieren, ist zu wünschen, dass der Beitritt zum Übereinkommen bei der Anerkennung der Angemessenheit ein wichtiger Faktor ist. Eine Absichtserklärung der EU in diesem Sinne wäre gegenüber Drittstaaten ein positives Zeichen. Ein erster Schritt ist mit der Mitteilung vom 29. November 2013 der Kommission an das europäische Parlament und den Rat betreffend Datenübermittlungen zwischen der EU und den USA erfolgt. Die Kommission äussert sich darin dahingehend, dass der Beitritt eines Drittstaates zum Übereinkommen zu fördern sei.[6] Ausserdem ist es wichtig, dass in Brüssel und Strassburg dieselben Kriterien zur Beurteilung des Datenschutzes gelten und dass im Rahmen des Übereinkommens ein Folgemechanismus (Kontrollsystem) eingeführt wird. Die Kriterien, die von der Gruppe nach Artikel 29 definiert werden, um die Angemessenheit anzuerkennen, folgen weitgehend den Grundsätzen des Übereinkommens und sind bestimmt eine gute Basis für die Arbeiten des Komitees.

Untersteht der Empfänger nicht der Rechtshoheit einer Vertragspartei, so können die Daten in der Regel nur weitergegeben werden, wenn ein angemessenes Schutzniveau garantiert ist. Dieses Niveau muss garantieren, dass die Menschenrechte durch die Globalisierung und die Art des grenzüberschreitenden Datenverkehrs nicht beeinträchtigt werden. Es kann durch rechtliche Bestimmungen, die für den Empfänger gelten, geregelt werden, zum Beispiel durch rechtliche Grundlagen im Bereich des

[6] Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows, st17067/13

Datenschutzes. Es können auch standardisierte oder auf den Einzelfall bezogene rechtliche Massnahmen abgeleitet werden wie Vertragsklauseln, interne Regeln oder ähnliche verbindliche, wirksame und rekursfähige Massnahmen. Diese können von der Person festgelegt werden, die die Daten weitergibt oder die den Zugang zu den Daten ermöglicht – oder von der Person, die die Daten empfängt. Der Änderungsentwurf sieht vor, dass die Datenschutzbehörden über im Einzelfall festgelegte Massnahmen informiert werden müssen. Die Datenschutzbehörden können verlangen, dass die Wirksamkeit und die Qualität der Massnahmen nachgewiesen werden müssen. Sie können bei Bedarf die Datenweitergabe aufschieben, verbieten und oder mit Auflagen versehen. Sie können auch verlangen, dass die Massnahmen im Zusammenhang mit einer bestimmten Weitergabe überprüft werden. Die Weitergabe von Daten an Personen in Staaten, die das Übereinkommen unterzeichnet haben, die aber nicht Mitglied der EU sind und die noch keine Angemessenheitsfestellung besitzen, muss durch standardisierte oder im Einzelfall festzulegende Massnahmen begleitet werden.

Fehlt ein angemessenes Datenschutzniveau, so ist es möglich, die Daten unter bestimmten Voraussetzungen weiterzugeben oder zur Verfügung zu stellen. Die Weitergabe kann mit der Einwilligung der betroffenen Person erfolgen. Diese muss vorher über die Risiken informiert sein, die mit dem Fehlen angemessener Garantien verbunden sind. Es können auch Daten weitergegeben werden, wenn besondere Interessen der betroffenen Person dies erfordern, zum Beispiel, um lebenswichtige Interessen von ihr zu schützen. Und es können Daten weitergegeben werden, wenn überwiegende berechtigte Interessen vorhanden sind, vor allem wenn es sich dabei um wichtige gesetzlich vorgesehene öffentliche Interessen und Massnahmen handelt, die in einer demokratischen Gesellschaft notwendig sind. Hierbei geht es vor allem um die Notwendigkeit der Zusammenarbeit zwischen Justiz- und Polizeibehörden in strafrechtlichen Verfahren. Wenn kein angemessenes Datenschutzniveau gegeben ist, dürfen solche Weitergaben nicht regelmässig stattfinden, sondern müssen auf besondere Situationen beschränkt sein.

Der Änderungsentwurf sieht in Artikel 9 die Möglichkeit vor, dass die Vertragsparteien durch gesetzliche Bestimmungen Ausnahmen betreffend den grenzüberschreitenden Datenverkehr vorsehen können, wenn die Ausnahmen in einer demokratischen Gesellschaft notwendig sind, um das Recht auf freie Meinungsäusserung und auf Informationsfreiheit zu schützen. Solche Ausnahmen können sich insbesondere im Zusammenhang mit der Verbreitung von Daten im Internet für die Ausübung dieser beiden grundlegenden Freiheiten als nötig erweisen.

## 11. Aufsichtsbehörden

Der Änderungsentwurf befasst sich auch mit der Frage der Aufsichtsbehörden. Er nimmt Artikel 1 des Zusatzprotokolls auf und ergänzt die bestehenden Befugnisse der Behörden, Ermittlungen durchzuführen sowie Klagen anzustrengen bzw. den zuständigen Justizbehörden Verstösse gegen innerstaatliche Rechtsvorschriften zur Kenntnis zu bringen, durch die Pflicht, involvierte Personen zu sensibilisieren, zu informieren und auszubilden (betroffene Personen, für die Verarbeitung verantwortliche Personen, Auftragsverarbeiter usw.). Ausserdem ist vorgesehen, dass die Behörden Beschlüsse fassen und Sanktionen aussprechen können. Der Entwurf präzisiert zudem, dass die Aufsichtsbehörde bei der Ausübung ihrer Rechte und Pflichten unabhängig sein muss. Insbesondere bei der Wahrnehmung ihrer Aufgaben und der Ausübung ihrer Rechte ist die Aufsichtsbehörde weisungsfrei. Weder die ernennende noch eine andere Behörde ist befugt, Anweisungen zu erteilen. Um ihre Aufgaben und Rechte wirksam wahrnehmen zu können, muss die Aufsichtsbehörde überdies über angemessene personelle, technische und finanzielle Mittel und über die nötigen Infrastrukturen verfügen. Der Entwurf äussert sich auch explizit zur Zusammenarbeit zwischen den Aufsichtsbehörden. Diese müssen, wo nötig, zur Erfüllung ihrer Aufgaben zusammenarbeiten, indem sie insbesondere Informationen über Datenverarbeitungen in ihrem Hoheitsgebiet, über ihre Rechte oder über administrative Abläufe austauschen. Die Zusammenarbeit muss auch die Koordination ihrer Ermittlungen und ihres Einschreitens sowie die Führung gemeinsamer Aktivitäten umfassen. Die Institutionalisierung der Zusammenarbeit zwischen den Aufsichtsbehörden ist unver-

zichtbar, um der Globalisierung bei der Verarbeitung von Personendaten zu begegnen. Dies ist notwendig, um die Wirksamkeit des Datenschutzrechts zu erhöhen. Der Entwurf sieht vor, dass sich die Aufsichtsbehörden mittels Konferenzen oder in Netzwerken organisieren können, um diese Koordinationsaufgabe gut wahrnehmen zu können. Damit keine neue Struktur geschaffen werden muss, könnte in Zukunft die europäische Konferenz der Datenschutzbeauftragten diese Aufgabe wahrnehmen. Die Zusammenarbeit zwischen den Vertragsparteien, die zurzeit unter den Artikeln 13 ff. des Übereinkommens geregelt ist, obliegt in Zukunft den Aufsichtsbehörden. Dies betrifft auch die Unterstützung von Betroffenen bei der Ausübung ihrer Rechte. Schliesslich wurde die Datenverarbeitung durch die Justizbehörden geklärt. Die Aufsichtsbehörde darf nicht auf die Unabhängigkeit der Rechtsprechung Einfluss nehmen und ist demnach nicht zuständig für Verarbeitungen, die durch die Justizbehörden bei der Ausübung ihrer richterlichen Funktionen vorgenommen werden. Für andere Verarbeitungen ist sie jedoch zuständig.

## 12. Beratender Ausschuss

Das Übereinkommen setzt einen Beratenden Ausschuss ein, um die Anwendung zu unterstützen und zu verbessern. Der Ausschuss spielt bei der Auslegung des Übereinkommens, dem Informationsaustausch zwischen den Vertragsparteien und der Entwicklung des Datenschutzrechts eine wichtige Rolle. Der Entwurf sieht vor, die Rolle und die Kompetenzen des Ausschusses zu stärken. Es wird sich nicht mehr nur um einen beratenden Ausschuss handeln, da dieser auch befugt sein wird, zu evaluieren und die Kontrolle sicherzustellen. Deshalb ist vorgesehen, die Bezeichnung anzupassen. Aus dem Beratenden Ausschuss wird das Konventionskomitee. Dieser kann sich insbesondere zum Datenschutzniveau eines Staates oder einer internationalen Organisation äussern, bevor dieser oder diese dem Übereinkommen beitritt. Er kann auch die Konformität der Regeln des innerstaatlichen Rechts einer Vertragspartei und die Wirksamkeit von Massnahmen, die getroffen wurden, prüfen (Vorhandensein einer Aufsichtsbehörde, Kompetenzen, Rekurse), insbesondere um das Datenschutzniveau festzustellen. Er kann auch evaluieren, ob die rechtlichen

Bestimmungen zum Datenverkehr ausreichen, um ein angemessenes Datenschutzniveau zu gewährleisten. Zur Einschätzung dieses Niveaus muss im internen Reglement des Ausschusses das Prüfverfahren festgelegt werden. Zudem kann er Modelle für standardisierte rechtliche Massnahmen ausarbeiten. Und zu guter Letzt wird er eine wichtige Rolle spielen, wenn es darum geht, Schwierigkeiten, die bei der Anwendung des Übereinkommens auftreten, einvernehmlich zu lösen.

## IV. Schlussfolgerung

Die Überarbeitung des Übereinkommens gehört zu den Prioritäten des Europarates. Nach der Verabschiedung durch den Beratenden Ausschuss anlässlich der 29. Vollversammlung im November 2012, wird der Entwurf jetzt vom CAHDATA geprüft. Dieser Ausschuss besteht aus den Mitgliedstaaten des Europarates, Uruguay, den Beobachterstaaten des Europarats, und einigen Ländern, die eingeladen sind, dem Übereinkommen beizutreten. Die europäische Kommission sowie Vertreterinnen und Vertreter aus Wirtschaft und Gesellschaft sind an den Arbeiten beteiligt. Der Ausschuss muss auf Basis des T-PD ein Änderungsprotokoll zum Übereinkommen vorbereiten. Der Entwurf sollte im Laufe des Jahres 2014 fertig gestellt werden und dem Ministerkomitee zur Verabschiedung und den Vertragsparteien zur Genehmigung unterbreitet werden.

Mit dieser Überarbeitung, wird die Wirksamkeit des Übereinkommens erhöht, insbesondere durch die Einführung eines Ablaufs zur Prüfung der Konformität des innerstaatlichen Rechts der Vertragsparteien mit den Bestimmungen des Übereinkommens, und durch die Möglichkeit, dessen Umsetzung zu kontrollieren. Das Übereinkommen wird bei der Weiterentwicklung des universellen Rechts auf Datenschutz mehr denn je eine wichtige und zentrale Rolle spielen. Es bildet im Hinblick auf ein globales Datenschutzrecht eine solide Grundlage und bietet Drittstaaten durch den Beitritt die Möglichkeit, die Angemessenheit des rechtlichen Anspruchs anzuerkennen. Zum gegenwärtigen Zeitpunkt, wo unsere Grundrechte und Freiheiten zugunsten der Sicherheit geschwächt werden, und angesichts der gross angelegten Über-

wachungen in diesem Bereich, muss der rechtliche Rahmen des Datenschutzes in Europa und auf der ganzen Welt dringend gestärkt werden. Die Verabschiedung eines aktualisierten und weltoffenen Übereinkommens stellt dabei einen wichtigen Schritt dar.