



0475/10/DE
WP 177

**Stellungnahme 6/2010 zum Schutz natürlicher Personen bei der
Verarbeitung personenbezogener Daten in der
Republik Östlich des Uruguay**

vom 12. Oktober 2010

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges Beratungsgremium der EU für Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von der Europäischen Kommission, GD Justiz, Direktion C (Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro Nr. MO-59 06/036.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, insbesondere auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe b,

gestützt auf die Geschäftsordnung der Arbeitsgruppe, insbesondere auf die Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

Am 20. Oktober 2008 übermittelte die Vertretung der Republik Östlich des Uruguay (im Folgenden „Uruguay“) bei der Europäischen Union der Europäischen Kommission ein Schreiben mit dem amtlichen Ersuchen der Regierung Uruguays um Einleitung des Verfahrens zur Klärung der Frage, ob Uruguay ein angemessenes Schutzniveau bezüglich der Übermittlung personenbezogener Daten aus der EU/dem EWR gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG zum Schutz personenbezogener Daten (im Folgenden „die Richtlinie“) aufweist.

Zur Prüfung der Frage, ob Uruguay ein angemessenes Schutzniveau bietet, forderte die Kommission einen Bericht des *Centre de Recherches Informatique et Droit* (CRID) der Universität Namur an. In diesem ausführlichen Bericht wird untersucht, inwieweit das Rechtssystem Uruguays unter dem Aspekt der Beschaffenheit der Gesetzgebung und der Verfügbarkeit von Mechanismen zur Anwendung von Rechtsvorschriften zum Schutz personenbezogener Daten den einschlägigen Anforderungen entspricht. Diese Aspekte waren bereits in der Arbeitsunterlage „Übermittlung von personenbezogenen Daten in Drittländer: Anwendung von Artikel 25 und 26 der EU-Datenschutzrichtlinie“ dargelegt worden, das von der gemäß Artikel 29 der Richtlinie eingesetzten Datenschutzgruppe am 24. Juli 1998 (Dokument WP12) angenommen worden war. Für die uruguayischen Behörden äußerte sich das Kontrollorgan für die Regulierung und Kontrolle personenbezogener Daten (URCDP) mit Zustimmung seines Exekutivrats am 11. Februar 2010 zu den in diesem Bericht aufgeworfenen Fragen.

Dieser Bericht wurde zusammen mit den Bemerkungen der uruguayischen Behörden von einer eigens hierfür gebildeten Untergruppe der Artikel 29 Datenschutzgruppe geprüft, die der Datenschutzgruppe vorschlug, den uruguayischen Behörden ein Schreiben ihres Vorsitzenden zu übermitteln. Dieses Schreiben beinhaltet zunächst eine positive Einschätzung der Datenschutzregelung in Uruguay (die im Wesentlichen über das Gesetz Nr. 18 331 vom 11. August 2008 über den Schutz personenbezogener Daten und den „Habeas data“-Rechtsbehelf – LPDP [nach den spanischen Initialen] und die entsprechende Durchführungsverordnung vom 31. August 2009 – DPDP erfolgt). Darüber hinaus wurden die Behörden auf die Aspekte hingewiesen, zu denen weitere Klarstellungen erforderlich werden könnten.

Die uruguayischen Behörden übermittelten der Artikel 29 Datenschutzgruppe einen ausführlichen Bericht des Kontrollorgans URCDP, dem der Exekutivrat des Kontrollorgans am 23. Juni 2010 zugestimmt hatte und der die Antworten auf die in dem Schreiben aufgeworfenen Fragen enthält. Außerdem legten sie verschiedene Unterlagen zur Stand des Datenschutzes in Uruguay einschließlich des Jahresberichts dieses Gremiums für 2009 und des Tätigkeitsberichts für die Zeit bis zum 31. Mai 2010, verschiedener vom Exekutivrat getroffener Entscheidungen sowie maßgeblicher rechtlicher Entscheidungen zum Thema Datenschutz vor.

Der Bericht wurde den Mitgliedern der Untergruppe im September 2010 erneut vorgelegt, die ihn unter besonderer Berücksichtigung der im Schreiben der Datenschutzgruppe an die uruguayischen Behörden angesprochenen Fragen prüften. Nach Prüfung der vorstehend genannten Unterlagen kann die Untergruppe der Datenschutzgruppe nun ihren Analysebericht vorlegen.

2. DIE GESETZESLAGE ZUM DATENSCHUTZ IN URUGUAY

In der Verfassung der Republik Östlich des Uruguay von 1967 sind das Recht auf Privatsphäre und der Schutz personenbezogener Daten nicht ausdrücklich anerkannt. Allerdings trifft dieser oberste Rechtsakt in dieser Hinsicht keine sehr klare Aussage, denn in Artikel 72 der Verfassung heißt es, dass „neben den in der Verfassung aufgeführten Rechten, Pflichten und Garantien weitere zum Tragen kommen können, die mit der menschlichen Persönlichkeit verbunden sind oder sich aus der republikanischen Staatsform ergeben“.

Des Weiteren heißt es in Artikel 332 der Verfassung, dass „die Grundsätze dieser Verfassung, in denen die Rechte natürlicher Personen anerkannt werden, sowie die Grundsätze, nach denen öffentlichen Behörden Rechte zuerkannt und Pflichten auferlegt werden, auch ohne einschlägige Durchführungsverordnungen zur Anwendung kommen sollten. In diesem Fall wird auf Rechtsgrundlagen, die sich aus ähnlichen Gesetzen ergeben, sowie auf die allgemeinen Rechtsgrundsätze und die allgemein anerkannte Rechtsdogmatik zurückgegriffen“.

Daher bestätigt die Datenschutzgruppe, dass mit diesen beiden offenen Klauseln anerkannt wird, dass es persönliche Grundrechte gibt, die in der uruguayischen Verfassung nicht ausdrücklich anerkannt sind. Diese Schlussfolgerung bestätigt sich erneut durch die Tatsache, dass in Artikel 1 des Gesetzes Nr. 18 331 über den Schutz personenbezogener Daten und den „Habeas data“-Rechtsbehelf (LPDP) eindeutig erklärt wird, dass „der Mensch ein Recht auf den Schutz personenbezogener Daten hat. Demnach ist dieses Recht in Artikel 72 der Verfassung der Republik enthalten“.

Demnach ist das Grundrecht auf den Schutz personenbezogener Daten wie vom Rechtssystem Uruguays anerkannt im neuen Datenschutzgesetz LPDP geregelt, das am 11. August 2008 verkündet wurde. Es ersetzt das frühere Gesetz über den Schutz personenbezogener Daten, das für Geschäftsberichte bestimmt war sowie den „Habeas data“-Rechtsbehelf von 2004. Somit ist nun für die Regelung des Datenschutzes in allen Tätigkeitsbereichen allein das LPDP maßgeblich. In Artikel 3 ist der Grundsatz verankert, dass „die Vorschriften dieses Gesetzes auf personenbezogene Daten Anwendung finden, die in einem Medium aufgezeichnet werden, wodurch ihre Weiterverarbeitung wahrscheinlich wird, und auf jede Art von Weiterverwendung, der diese Daten im öffentlichen oder privaten Sektor zugeführt werden können“.

Zur weiteren Ausführung der Bestimmungen des neuen Datenschutzgesetzes LPDP hat die Regierung der Republik Uruguay am 31. August 2009 die Durchführungsverordnung zum Datenschutz (DPDP) erlassen. In der Präambel dieser Verordnung heißt es, dass „es angebracht ist, das nationale Rechtssystem auf diesem Gebiet an das vergleichbare Rechtssystem anzupassen, das von den meisten Ländern anerkannt wird, im Wesentlichen an das System, das die europäischen Länder mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr eingeführt haben“.

In dieser Verordnung werden einige Bestimmungen des LPDP verdeutlicht und unter Regulierungsaspekten weiter vertieft. Die Datenschutzgruppe hält es insbesondere für erforderlich, auf die Bestimmungen, die mit dem räumlichen Anwendungsbereich des LPDP, der Sicherheit, der Ausübung von Rechten auf Zugang zu, Aktualisierung von und Löschung von Daten zusammenhängen, sowie auf die einzelnen Regulierungsvorschriften für Organisation, Befugnisse und Funktionsweise des Kontrollorgans näher einzugehen, das die Bezeichnung Stelle für die Regulierung und Kontrolle personenbezogener Daten (URCDP) trägt.

Abschließend weist die Datenschutzgruppe darauf hin, dass die Unterlagen, die die uruguayischen Behörden in Beantwortung des ihnen übermittelten Schreibens vorgelegt haben, die Zustimmung des Exekutivrats des Kontrollorgans URCDP enthalten, womit dieser erklärt, *„darauf hinzuwirken, dass das Außenministerium beim Europarat die zu dieser Entscheidung notwendigen Verfahren gemäß Artikel 23 des Übereinkommens 108 des Europarats (Straßburger Übereinkommen) und des Zusatzprotokolls vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten einleitet“*.

3. GEWÄHRLEISTET DAS URUGUAYISCHE DATENSCHUTZRECHT EINEN ANGEMESSENEN SCHUTZ PERSONENBEZOGENER DATEN?

Die Datenschutzgruppe weist darauf hin, dass sich ihre Bewertung der Angemessenheit des uruguayischen Datenschutzrechts zum Schutz personenbezogener Daten im Wesentlichen auf das Gesetz Nr. 18 331 vom 13. August 2008 über den Schutz personenbezogener Daten und den „Habeas data“-Rechtsbehelf (LPDP) sowie die zu diesem Gesetz erlassene Durchführungsverordnung vom 31. August 2009 (DPDP) stützt.

Die Grundsätze dieses Gesetzes wurden mit den wesentlichen Bestimmungen der Richtlinie unter Berücksichtigung des Berichts der Arbeitsgruppe WP12 verglichen. Dieser Bericht geht auf eine Reihe von Grundsätzen ein, die einen „Kern“ von *„inhaltlichen“ Grundsätzen für den Datenschutz und die „Verfahrens-/Anwendungsanforderungen“ bilden, deren Einhaltung als Mindestvoraussetzung für einen angemessenen Datenschutz betrachtet werden könnte*.

3.1 Anwendungsbereich des Datenschutzrechts

Objektiv betrachtet wird mit Artikel 3 des LPDP und wortgleich mit Artikel 2 des DPDP der Grundsatz festgelegt, dass diese Regelung „auf personenbezogene Daten Anwendung findet, die in einem Medium aufgezeichnet werden, wodurch ihre Weiterverarbeitung wahrscheinlich wird, und auf jede Art von Weiterverwendung, der diese Daten im öffentlichen oder privaten

Sektor zugeführt werden“. Gleichzeitig sind die Vorschriften zum Datenschutz gemäß Artikel 2 gegebenenfalls auch auf juristische Personen anzuwenden.

Die Datenschutzgruppe begrüßt die Klarstellungen der uruguayischen Behörden zu ihren Bedenken, das Gesetz könnte keine Anwendung auf „Datenbanken“ finden, „die im Wege von Sondergesetzen geschaffen und reguliert werden“.

Darauf hatten die uruguayischen Behörden geantwortet, dass die erwähnten Sondergesetze, für die sie eine Reihe von Beispielen angeführt haben, ein anspruchsvolleres Datenschutzsystem beinhalten als das allgemeine Datenschutzgesetz. Dieses wird auf jeden Fall aufgrund des zuvor genannten Artikels 322 der Verfassung der Republik stets zusätzlich auf Sachverhalte Anwendung finden, die nicht im Wege eines Sondergesetzes geregelt sind.

Zum räumlichen Anwendungsbereich des Gesetzes begrüßt die Datenschutzgruppe, dass das DPDP ausdrücklich einen Artikel zu diesem Thema enthält, der sich im Grunde inhaltlich mit der Regelung in Artikel 4 der Richtlinie deckt. Dadurch ist implizit die Einhaltung der Grundprinzipien und insbesondere des Prinzips der Beschränkung der Anzahl der nachfolgenden Übermittlungen gewährleistet.

Somit ist nach dem vorstehend erwähnten Artikel 3 davon auszugehen, dass die Verarbeitung personenbezogener Daten mit dem LPDP konform ist, wenn

- die Verarbeitung durch Datenbanken oder für die Verarbeitung Verantwortliche erfolgt, die in Uruguay niedergelassen sind, und ihrer Tätigkeit in Uruguay nachgehen, wobei ihre Rechtsform unerheblich ist;
- die Datenbank oder der für die Verarbeitung Verantwortliche nicht in Uruguay niedergelassen ist, die Daten aber mittels eines Mediums innerhalb dieses Landes verarbeitet werden.

Des Weiteren ist folgende Ausnahme für den zweiten Fall vorgesehen: „In Fällen, in denen die vorstehend genannten Medien ausschließlich für Übermittlungszwecke verwendet werden, sofern die Datenbank oder der für die Verarbeitung Verantwortliche einen Vertreter mit Wohnsitz und ständigem Aufenthaltsort in dem der Kontrollbehörde unterstehenden Hoheitsgebiet benennt, um den einschlägigen rechtlichen Verpflichtungen im Regulierungsbereich nachkommen zu können“.

Daher ist die Datenschutzgruppe bezogen auf die zuvor genannten Klarstellungen der Ansicht, dass der Anwendungsbereich der uruguayischen Gesetzgebung zum Datenschutz mit dem der Richtlinie vergleichbar ist.

3.2. Inhaltliche Grundsätze

a) Wesentliche Grundsätze

1) Der Zweckbindungsgrundsatz: Die Daten sollten zu einem bestimmten Zweck verarbeitet werden und danach nur weiterverwendet oder übermittelt werden, wenn dies mit dem Übermittlungszweck nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel bilden die in Artikel 13 der Richtlinie beschriebenen Gründe, aus denen Beschränkungen in einer demokratischen Gesellschaft nötig sein könnten.

Die Datenschutzgruppe konnte mit Genugtuung feststellen, dass dieser Grundsatz im LPDP explizit in Artikel 5 Buchstabe c enthalten ist, wo ausdrücklich festgelegt ist, dass sich die öffentlichen oder privaten für die Verarbeitung Verantwortlichen und grundsätzlich alle, die mit personenbezogenen Daten Dritter umzugehen haben, in ihrem Handeln an den Zweckbindungsgrundsatz zu halten haben.

In Artikel 6 des Datenschutzgesetzes heißt es, dass „keine Datenbank zur Verletzung der Menschenrechte verwendet werden noch im Konflikt mit den Gesetzen oder den guten Sitten stehen darf“. In Artikel 8 wird ergänzend hinzugefügt, dass „die zur Verarbeitung bestimmten Daten nicht zu anderen Zwecken als denen, für die sie erhoben wurden, bzw. nicht zu Zwecken verwendet werden dürfen, die mit ihrer Erhebung unvereinbar sind“.

Die einzige Ausnahme von diesem Grundsatz bildet folgende Bestimmung: „In den Durchführungsvorschriften werden Fälle und Verfahren festgelegt, in denen personenbezogene Daten ausnahmsweise angesichts ihres historischen, statistischen oder wissenschaftlichen Wertes und in Einklang mit einschlägigen spezifischen Rechtsvorschriften gespeichert werden dürfen, selbst wenn es zu diesem Zeitpunkt dafür keine Notwendigkeit oder keinen Anlass gibt“. In Artikel 37 des DPDP ist das Verfahren für die Genehmigung der Datenspeicherung zu historischen, statistischen oder wissenschaftlichen Zwecken festgelegt. Die Datenschutzgruppe geht davon aus, dass diese Ausnahmeregelung mit der in Artikel 6 Absatz 1 Buchstabe b der Richtlinie vergleichbar ist.

Desgleichen heißt es in Artikel 11 des LPDP, dass „natürliche oder juristische Personen, die rechtmäßig Informationen aus einer Datenbank beziehen, in der Daten verarbeitet werden, verpflichtet sind, diese so zu verwenden, dass ihre Vertraulichkeit gewahrt bleibt und sie ausschließlich zu den üblichen Zwecken ihrer geschäftlichen oder allgemeinen Tätigkeit zu verwenden, wobei jede Weitergabe dieser Informationen an Dritte untersagt ist“.

Daher ist die Datenschutzgruppe der Ansicht, dass das uruguayische Recht diesem Grundsatz gerecht wird.

2) Der Grundsatz der Datenqualität und der Verhältnismäßigkeit: Daten sollten sachlich richtig und gegebenenfalls in aktuellem Zustand aufbewahrt werden. Die Daten sollten angemessen, relevant und verhältnismäßig bezogen auf den Zweck sein, zu dem sie übermittelt und anschließend verarbeitet werden.

Nach Ansicht der Datenschutzgruppe scheint dieser Grundsatz in Artikel 7 des LPDP mit dem sog. „Grundsatz der sachlichen Richtigkeit“ abgedeckt zu sein, der auch als eines der Hauptleitprinzipien des Datenschutzrechts in Artikel 5 Buchstabe b aufgeführt ist.

Der vorstehend genannte Artikel 7 besagt, dass „personenbezogene Daten, die zum Zweck der Verarbeitung erhoben werden, sachlich richtig, angemessen, unparteilich und nicht unverhältnismäßig bezogen auf den Zweck sein sollten, zu dem sie erhoben werden. Die Daten dürfen nicht mit unfairen, betrügerischen, missbräuchlichen Mitteln oder mittels Erpressung noch in einer gesetzwidrigen Weise erhoben werden“.

Des Weiteren verlangt das LPDP, dass „Daten sachlich richtig und gegebenenfalls in aktualisierter Form“ erhoben werden sollten, und dass „Daten, die sich als sachlich unrichtig oder falsch herausstellen, vom für die Verarbeitung Verantwortlichen zu löschen, ergänzen oder durch sachlich richtige, wahrheitsgemäße und aktualisierte Daten zu ersetzen sind, sobald sich der Verantwortliche dieser Situation bewusst wird. Außerdem sind alle überholten Daten nach den Vorschriften dieses Gesetzes zu löschen“.

Artikel 8 des LPDP schließlich besagt, dass „Daten zu löschen sind, sobald sie nicht mehr zu dem Zweck ihrer Erhebung notwendig oder relevant sind“.

Die Arbeitsgruppe berücksichtigt dabei auch die Erläuterungen der uruguayischen Behörden zur Vermutung der Rechtmäßigkeit der Verarbeitung gemäß Artikel 9 Buchstabe c des LPDP, wo es heißt, dass „eine vorherige Einwilligung nicht erforderlich ist (...) wenn es sich um Listen mit Daten zu natürlichen Personen handelt, die sich auf Name und Vorname, Personalausweisnummer, Staatsangehörigkeit, Anschrift und Geburtsdatum beschränken. Im Falle von juristischen Personen entsprechen diese Angaben der Firmenbezeichnung, dem Markennamen, der Steuernummer des Steuerpflichtigen, der Anschrift, der Telefonnummer und den Namen der zuständigen Personen“.

In diesem Zusammenhang haben die uruguayischen Behörden klargestellt, dass die Vermutung der Rechtmäßigkeit, die mit diesem Grundsatz etabliert wird, unter keinen Umständen anders als im Einklang mit den Grundsätzen der Rechtmäßigkeit, Verhältnismäßigkeit und Zweckbindung auszulegen ist. Selbst wenn demnach keine vorherige Einwilligung der betroffenen Person erforderlich ist, kann der für die Datenverarbeitung Verantwortliche die in diesem Artikel genannten Daten nur weiterverarbeiten, wenn diese Verarbeitung mit den ausdrücklich festgelegten rechtmäßigen Zwecken in Einklang steht und sofern die genannten Daten angemessen, relevant und nicht unverhältnismäßig bezogen auf die genannten Zwecke sind und es außer der Einhaltung beider Grundsätze keine weitere Rechtmäßigkeitsvermutung gibt.

Angesichts dieser Erläuterungen geht die Datenschutzgruppe davon aus, dass im uruguayischen Datenschutzrecht auch die Grundsätze der Verhältnismäßigkeit und der Datenqualität abgedeckt sind.

3) Der Grundsatz der Transparenz: Die betroffenen Personen sollten über den Zweck, zu dem ihre Daten verarbeitet werden sowie die Identität des für die Verarbeitung Verantwortlichen im Drittland und über jeden anderen Aspekt informiert werden, der für die Gewährleistung einer fairen Behandlung erforderlich ist. Die einzigen zulässigen Ausnahmen sind in den Artikeln 11 Absatz 23 und Artikel 13 der Richtlinie vorgegeben.

Die Datenschutzgruppe geht davon aus, dass die Pflicht zur Information der betroffenen Person über die Verarbeitung ihrer Daten von Artikel 13 des LPDP abgedeckt ist, wonach die betroffenen Personen im Fall der Erhebung personenbezogener Daten zu ihrer Person zuvor ausdrücklich, sachlich richtig und unmissverständlich über folgende Aspekte zu informieren sind:

- zu welchem Zweck die Daten verarbeitet werden sowie mögliche Empfänger oder Arten von Empfängern;

- das Bestehen einer elektronischen oder anders gearteten Datenbank und die Identität und Anschrift des für die Verarbeitung Verantwortlichen;
- ob die Antworten auf den übermittelten Fragebogen zwingend vorgeschrieben oder freiwilliger Art sind, insbesondere bezüglich sensibler Daten;
- die Folgen der Auskunftserteilung, der Verweigerung der Auskunft oder der Angabe unrichtiger Daten;
- dass die betroffene Person von ihrem Recht auf Zugang, Berichtigung oder Löschung von Daten Gebrauch machen kann.

Desgleichen bestätigt die Datenschutzgruppe, dass die betroffene Person auch bei einer Verarbeitung mit ihrer Einwilligung gemäß Artikel 9 des LPDP und Artikel 5 des DPDP zu informieren ist. In diesem letztgenannten Artikel heißt es, „wenn für die Erhebung und Verarbeitung von Daten die Einwilligung der betroffenen Person erforderlich ist, ist diese so zu informieren, dass ihr unmissverständlich bewusst ist, zu welchem Zweck die Daten verwendet werden und welche Art von Verarbeitung durch die Datenbank erfolgt oder von dem für die Verarbeitung Verantwortlichen vorgenommen wird. Andernfalls ist die Einwilligung null und nichtig“.

Die Datenschutzgruppe berücksichtigt in diesem Zusammenhang auch die Klarstellungen der uruguayischen Behörden zur Pflicht der Unterrichtung der betroffenen Person in allen Fällen. Obwohl der Wortlaut von Artikel 13 den Eindruck erwecken könnte, dass sich die Verpflichtung zur Unterrichtung der betroffenen Person nur auf die Fälle bezieht, in denen die betroffene Person die Daten freiwillig und mit ihrer Einwilligung bereitstellt, verweisen die uruguayischen Behörden darauf, dass dies eine absolute und bedingungslose Verpflichtung ist, die unabhängig von dem Grund besteht, mit dem die Datenverarbeitung gerechtfertigt wird. Die Pflicht zur Information der betroffenen Person besteht in allen Fällen ungeachtet der Frage, ob die personenbezogenen Daten von der betroffenen Person oder von einem Dritten angefordert werden oder ob die Verarbeitung mit Einwilligung der betroffenen Person oder aus einem anderen rechtmäßigen Grund erfolgt.

Darüber hinaus stellen die uruguayischen Behörden klar, dass die betroffene Person auch bei der Weitergabe von Daten und ihrer Erlangung über Dritte nach Artikel 13 des LPDP zuvor von der Person oder Stelle, die die Daten weitergibt, auch über die Weitergabe der Daten und über die Empfänger zu informieren ist.

4) Der Grundsatz der Sicherheit: Der für die Verarbeitung Verantwortliche hat angemessene technische und organisatorische Maßnahmen zum Schutz vor den mit der Verarbeitung verbundenen Risiken zu treffen. Daten dürfen nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeitet werden. Dies gilt für alle unter der Aufsicht des Verantwortlichen arbeitenden Personen einschließlich der für die Verarbeitung zuständigen Person.

Die Datenschutzgruppe weist darauf hin, dass der Grundsatz der Sicherheit in Artikel 5 Buchstabe e des LPDP aufgeführt ist.

Artikel 10 des Datenschutzgesetzes führt diesen Grundsatz näher aus. Dort heißt es, dass „der für die Verarbeitung Verantwortliche oder Nutzer der Datenbank alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit und der Vertraulichkeit der personenbezogenen Daten zu treffen hat. Mit diesen Maßnahmen soll vermieden werden, dass Daten geändert werden, verloren gehen oder unbefugt konsultiert oder verarbeitet werden. Außerdem soll sich feststellen lassen, ob Informationen - sei es durch menschliche Eingriffe oder aufgrund des verwendeten technischen Mittels - absichtlich oder ungewollt weitergegeben werden“. Weiter heißt es: „Personenbezogene Daten dürfen nicht in Datenbanken aufbewahrt werden, die nicht den Anforderungen der technischen Integrität und Sicherheit genügen“.

Des Weiteren heißt es in Artikel 7 des DPDP, dass „sowohl der für die Verarbeitung Verantwortliche als auch die Person, die für die Datenbank oder die Verarbeitung zuständig ist, für den Schutz der verarbeiteten personenbezogenen Daten zu sorgen hat, indem die am besten geeigneten technischen und organisatorischen Maßnahmen zur Gewährleistung ihrer Integrität, Vertraulichkeit und Verfügbarkeit ergriffen werden“, wobei der für die Verarbeitung Verantwortliche ganz im Sinne der Definition der Richtlinie zu verstehen ist.

Die Datenschutzgruppe stellt des Weiteren fest, dass Artikel 8 des DPDP die Verpflichtung zur Information der betroffenen Personen für den Fall enthält, dass gegen die Sicherheitsbestimmungen verstoßen wurde. Dort heißt es: „Wenn die für die Datenbank oder die Verarbeitung Verantwortlichen feststellen, dass in einer Phase der Verarbeitung gegen die Sicherheitsbestimmungen verstoßen wurde und dies wahrscheinlich mit erheblichen Auswirkungen auf die Rechte der betroffenen Person verbunden sein dürfte, haben sie diese über diesen Sachverhalt zu informieren“.

Abschließend hat sich die Datenschutzgruppe mit der Regelung der Pflicht zur Wahrung der Vertraulichkeit und Geheimhaltung gemäß Artikel 11 des LPDP befasst und anhand aller dazu vorliegenden Angaben festgestellt, dass das uruguayische Recht dem Sicherheitsgrundsatz im Sinne des Dokuments WP12 entspricht.

5) Recht auf Zugang zu und Berichtigung von Daten und auf Widerspruch: Eine betroffene Person muss Anspruch auf eine Kopie aller sie betreffenden personenbezogenen Daten sowie auf Berichtigung sachlich unrichtiger Daten haben. In bestimmten Fällen sollte der Einzelne auch das Recht auf Widerspruch gegen die Verarbeitung von ihm betreffenden Daten haben. Die einzigen Ausnahmen von diesen Rechten sollten sich auf die in Artikel 13 der Richtlinie genannten Fälle beschränken.

Bezüglich des Rechts auf Zugang sieht Artikel 14 des LPDP vor, dass „jede von der Erfassung personenbezogener Daten betroffene Person, deren Identität anhand eines Ausweisdokuments oder einer entsprechenden Vollmacht nachgewiesen werden konnte, Anspruch auf alle personenbezogenen Daten hat, die über sie in einer öffentlichen oder privaten Datenbank aufbewahrt werden. Das Recht auf Zugang kann nur alle sechs Monate kostenlos in Anspruch genommen werden, es sei denn, mit diesem Recht auf Zugang ist ein legitimes Interesse in Einklang mit dem Rechtssystem geweckt worden“.

Derartige Auskünfte „sind binnen fünf Arbeitstagen ab dem Zeitpunkt des Auskunftersuchens zu erteilen. Wird innerhalb dieses Zeitraums keine Auskunft erteilt oder wird die Auskunft aus nach diesem Recht ungerechtfertigten Gründen verweigert, besteht Anspruch auf Rechtsbehelf gemäß dem „Habeas data“-Grundsatz. Des Weiteren heißt es, dass

„die Auskunft in klarer nicht verschlüsselter Form und gegebenenfalls mit einer Erläuterung versehen in einer Sprache unter Verwendung allgemein üblicher Begriffe zu erteilen ist, die für eine Bevölkerung mit durchschnittlicher Bildung zugänglich ist“.

Artikel 14 besagt des Weiteren, dass „die Auskunft umfassend zu sein hat und sich auf die gesamte Datei zu der betroffenen Person zu beziehen hat, auch wenn sich das Auskunftersuchen nur auf einen Aspekt ihrer personenbezogenen Daten bezieht. Die Auskunft sollte auf keinen Fall Informationen enthalten, die sich auf Dritte beziehen, selbst wenn zwischen diesen und der betroffenen Person ein Zusammenhang besteht“, und „dass die Auskunft schriftlich, in elektronischer Form, telefonisch, per Bild oder auf jede geeignete Weise, die der Auskunfterteilende für angebracht hält, erteilt werden kann“.

Anhand der von den uruguayischen Behörden gelieferten Klarstellungen geht die Datenschutzgruppe davon aus, dass die betroffene Person ihr Ersuchen auf Auskunft ungeachtet des Wortlauts von Artikel 9 Buchstabe d des DPDP nicht zu begründen braucht. Es genügt hierzu, dass sie sich ausweisen kann. Die Datenschutzgruppe verweist insbesondere auf die URCDP-Vereinbarung vom 18. Juni 2010, in der es heißt, dass *„zur Wahrnehmung des Rechts auf Zugang zu den Daten gemäß Artikel 14 des Gesetzes Nr. 18 331 über den Schutz personenbezogener Daten und den „Habeas data“-Rechtsbehelf, der für die Datenbank Verantwortliche bei einem Auskunftersuchen einer betroffenen Person allein darauf zu achten hat, dass diese Person sich ausweist“*.

Bezüglich der weiteren Rechte der betroffenen Personen besagt Artikel 15 des LPDP, dass „jede natürliche oder juristische Person Anspruch auf Berichtigung, Aktualisierung, Aufnahme oder Löschung ihrer in einer Datenbank gespeicherten personenbezogenen Daten hat, wenn sich bestätigt, dass bei den sie betreffenden Informationen ein Fehler unterlaufen ist oder eine Eintragung falsch war oder unterlassen wurde“.

Das Gesetz besagt weiter, dass „der für die Datenbank oder Datenverarbeitung Verantwortliche derartige Angaben spätestens binnen fünf Arbeitstagen nach Eingang des Ersuchens der betroffenen Person im Wege der dazu erforderlichen Eingriffe zu berichtigen, auf den neuesten Stand zu bringen, aufzunehmen oder zu löschen hat oder gegebenenfalls die Gründe dafür nennt, weshalb er dies nicht für möglich hält“. Dies führt zu der Feststellung, dass „die betroffene Person, sofern der für die Datenbank oder die Datenverarbeitung Verantwortliche seinen Verpflichtungen nicht oder nicht innerhalb der genannten Frist nachkommt, Anspruch auf Durchsetzung ihres Rechts unter Nutzung des „Habeas data“-Grundsatzes hat, der Teil dieses Gesetzes ist.

Die Datenschutzgruppe nimmt die Klarstellungen zum DPDP zur Kenntnis und befasste sich dann zunächst mit den Begriffsbestimmungen in den Artikeln 10 bis 12.

Gemäß Artikel 10 ist das Recht auf Berichtigung wie folgt definiert: „Unter Recht auf Berichtigung ist das Recht der betroffenen Person zu verstehen, sachlich unrichtige oder unvollständige Daten berichtigen zu lassen“. Artikel 11 beinhaltet folgende Definition für das Recht auf Aktualisierung von Daten: „Unter Recht auf Aktualisierung ist das Recht der betroffenen Person zu verstehen, zum Zeitpunkt der Ausübung des Rechtes sachlich unrichtige Daten berichtigen zu lassen“. Artikel 12 enthält folgende Definition für das Recht auf Aufnahme von Daten: „Unter dem Recht auf Aufnahme von Daten ist das Recht der betroffenen Person zu verstehen, sie betreffende Daten in eine Datenbank aufnehmen zu lassen, wenn sie ein berechtigtes Interesse daran nachweisen kann“.

Des Weiteren ist das Recht auf Löschung von Daten in Artikel 13 folgendermaßen formuliert: „Unter dem Recht auf Löschung von Daten ist das Recht der betroffenen Person zu verstehen, Daten, deren Verwendung durch Dritte rechtswidrig ist oder sich als unangemessen oder unverhältnismäßig herausgestellt hat, löschen zu lassen“.

Im Zusammenhang mit der Durchführungsverordnung (DPDP) erkennt die Datenschutzgruppe die Elemente an, auf die das CRID in seinen beiden Berichten über die Angemessenheit des Datenschutzes in Uruguay und insbesondere in den Addenden zur Umsetzung des DPDP hinweist, und geht demnach davon aus, dass das uruguayische Recht das Recht auf Widerspruch im Sinne des Artikels 14 der Richtlinie im Wege der Regulierung des Rechts auf Löschung anerkennt.

In Bezug auf Ausnahmen zur Wahrnehmung dieser Rechte stellt die Datenschutzgruppe fest, dass diejenigen Ausnahmen mit den Grundsätzen des Datenschutzes vereinbar sind, die auf die Notwendigkeit der Aufbewahrung von Informationen aus historischen, statistischen oder wissenschaftlichen Gründen zurückzuführen sind und in Einklang mit dem geltenden Recht stehen, oder die auf die Fortsetzung eines Vertragsverhältnisses zwischen dem für die Datenverarbeitung Verantwortlichen und der betroffenen Person zurückzuführen sind, aufgrund dessen die Verarbeitung der Daten gerechtfertigt ist.

Des Weiteren ist die Datenschutzgruppe der Ansicht, dass die Ausnahmen gemäß Artikel 26 des LPDP zur Berücksichtigung der „Gefährdung, die sich für die Verteidigung des Landes oder die öffentliche Sicherheit, den Schutz der Rechte und Freiheiten Dritter oder notwendige laufende Ermittlungen ergeben könnte“, mit denen in Artikel 13 der Richtlinie vergleichbar sind. Die Datenschutzgruppe berücksichtigt dabei insbesondere, dass im Gesetz selbst in Artikel 26 vorgesehen ist, dass „jede betroffene Person, der die Wahrnehmung ihrer in den vorangegangenen Absätzen genannten Rechte ganz oder teilweise verweigert wird, sich an das Kontrollorgan wenden kann, das darüber zu entscheiden hat, ob diese Verweigerung rechtmäßig oder rechtswidrig ist“.

6) Beschränkungen bei der Weitergabe an andere Länder: Personenbezogene Daten dürfen vom Bestimmungsdrittland nur dann an ein anderes Land übermittelt werden, wenn dieses ebenfalls ein angemessenes Datenschutzniveau aufweist. Die einzigen zulässigen Ausnahmen sollten jene bleiben, die in Artikel 26 Absatz 1 der Richtlinie aufgeführt sind.

Die Datenschutzgruppe stellt fest, dass das Konzept der internationalen Übermittlung von Daten im uruguayischen Recht mit dem der Mitgliedstaaten vergleichbar ist, da es nicht nur auf den Datentransfer an einen für die Verarbeitung Verantwortlichen in einen anderen Staat, sondern auch auf Fälle abstellt, in denen die Daten an einen Verarbeiter übermittelt werden.

Dieses Konzept ist von den Begriffsbestimmungen für den Export und Import von Daten in Artikel 4 Buchstaben e und f des DPDP abgeleitet. Ein Exporteur wird dort eigens als „eine natürliche oder juristische öffentliche oder private Person“ definiert, „die im uruguayischen Hoheitsgebiet niedergelassen ist und personenbezogene Daten in Einklang mit den Bestimmungen dieser Verordnung an ein anderes Land übermittelt“, und ein Importeur ist definiert als „eine natürliche oder juristische öffentliche oder private Person, die im Zuge eines internationalen Datentransfers Daten aus einem anderen Land als für die Verarbeitung Verantwortlicher, Verarbeiter oder Dritter erhält“.

Artikel 23 des LPDP legt als allgemeine Regel für Datentransfers fest, dass „die Übermittlung personenbezogener Daten an Länder oder internationale Organisationen, die nach den Standards des internationalen oder regionalen Rechts kein angemessenes Datenschutzniveau aufweisen, untersagt ist“. In den letzten beiden Absätzen dieses Artikels heißt es ergänzend, dass „die Regulierungs- und Kontrollstelle für den Schutz personenbezogener Daten (URCDP) unbeschadet der Bestimmungen des ersten Absatzes dieses Artikels eine oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland bewilligen kann, das kein angemessenes Datenschutzniveau aufweist, wenn der für die Verarbeitung Verantwortliche angemessene Schutzmaßnahmen zum Schutz der Privatsphäre, der Rechte und Freiheiten von natürlichen Personen und der Wahrnehmung ihrer jeweiligen Rechte zusagen kann. Derartige Schutzmaßnahmen können sich aus angemessenen Vertragsklauseln ableiten“.

Daher stellt die Datenschutzgruppe fest, dass diese Bestimmungen zur Regulierung von internationalen Datentransfers mit denen in Artikel 25 Absatz 1 und Artikel 26 Absatz 2 der Richtlinie vergleichbar sind.

Artikel 23 des LPDP enthält außerdem zwei Listen mit Ausnahmen zu diesen besonderen Bewilligungen. Die Datenschutzgruppe ist der Ansicht, dass die zweite dieser Listen mit den Ausnahmen in Artikel 26 Absatz 2 der Richtlinie vergleichbar ist, da die folgenden Fälle aufgeführt werden, in denen keine besondere Bewilligung zum Datentransfer erforderlich ist:

- wenn die betroffene Person ihre eindeutige Zustimmung zu dem beabsichtigten Datentransfer gegeben hat;
- wenn die Übermittlung der Daten für die Ausführung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder für die Umsetzung vor-vertraglicher Maßnahmen auf Ersuchen der betroffenen Person erforderlich ist;
- wenn die Übermittlung der Daten für den Abschluss oder die Ausführung eines Vertrags oder für einen im Interesse der betroffenen Person noch zu unterzeichnenden Vertrag zwischen dem für die Verarbeitung Verantwortlichen und einem Dritten erforderlich ist;
- wenn die Übermittlung der Daten zur Wahrung eines wichtigen öffentlichen Interesses notwendig oder rechtlich erforderlich oder zur Anerkennung, Ausübung oder Verteidigung eines Rechts in einem gerichtlichen Verfahren erforderlich ist;
- wenn die Übermittlung der Daten zur Wahrung entscheidender Interessen der betroffenen Person erforderlich ist;
- wenn die Übermittlung der Daten von einem Register aus erfolgt, das den gesetzlichen oder verwaltungsrechtlichen Auftrag hat, Informationen für die Öffentlichkeit bereitzustellen und von der breiten Öffentlichkeit oder jeder Person konsultiert werden kann, die ein legitimes Interesse nachweisen kann, vorausgesetzt, die gesetzlichen Anforderungen dafür sind in jedem Fall erfüllt.

Die Datenschutzgruppe stellt des Weiteren fest, dass die erste Liste eine Reihe von Annahmen enthält, die allerdings nicht wörtlich mit dem in Artikel 26 Absatz 1 der Richtlinie aufgeführten Fällen übereinstimmen. Auf dieser Liste werden folgende Sachverhalte als Ausnahmetatbestände zu der besonderen Bewilligung aufgeführt:

- a) die internationale justizielle Zusammenarbeit auf der Grundlage der einschlägigen internationalen Rechtsinstrumente – Vertrag oder Übereinkommen – und je nach den Umständen des betreffenden Falls;
- b) der Austausch medizinischer Daten, wenn dieser zur Behandlung einer Person aus Gründen der öffentlichen Gesundheit oder Hygiene erforderlich ist;
- c) Banküberweisungen oder Börsengeschäfte, jeweils bezogen auf die anstehende Transaktion und in Einklang mit dem einschlägigen Recht;
- d) Vereinbarungen im Rahmen internationaler Verträge, bei denen die Republik Östlich des Uruguay Vertragspartei ist;
- e) die internationale Zusammenarbeit zwischen Geheimdiensten zur Bekämpfung des organisierten Verbrechens, des Terrorismus oder des Drogenhandels.

Die Datenschutzgruppe verweist auf ihren Bericht 4/2002 über das Schutzniveau bei personenbezogenen Daten in Argentinien und auf die Ausnahmen unter den Buchstaben b, c und d, die auf den ersten Blick den Eindruck vermitteln könnten, dass es neben den Ausnahmen in Artikel 26 Absatz 1 der Richtlinie weitere Ausnahmetatbestände geben könnte, die die Anwendbarkeit dieses Grundsatzes beeinträchtigen könnten.

Die Datenschutzgruppe begrüßt jedoch die Klarstellungen der uruguayischen Behörden dergestalt, dass diese Ausnahmen in ihrer Anwendbarkeit nicht über den von Artikel 26 Absatz 1 vorgegebenen Rahmen hinausgehen.

Somit bezieht sich die Ausnahme unter Buchstabe c auf ein Vertragsverhältnis zwischen einer Person und dem Exporteur, das für seine Erfüllung zwangsläufig eine internationale Übermittlung personenbezogener Daten erfordert.

Die Ausnahmen unter Buchstabe b und d sind grundsätzlich in dem Sinne zu verstehen, dass es in beiden Fällen um ein wichtiges öffentliches Interesse, ein für Uruguay verbindliches internationales Abkommen oder eine Frage der öffentlichen Gesundheit innerhalb des allgemeinen Konzepts des „wesentlichen öffentlichen Interesses“ geht.

In diesem Verständnis kann die Datenschutzgruppe diese Erläuterungen akzeptieren, empfiehlt jedoch weitere Maßnahmen um sicherzustellen, dass auch die uruguayischen Behörden die geprüften Vorschriften in diesem Sinne auslegen.

b) Weitere Grundsätze

Das Dokument WP12 verweist darauf, dass für bestimmte Arten der Datenverarbeitung besondere Grundsätze Anwendung finden sollten, insbesondere folgende:

1) Sensible Daten: Im Falle der Kategorie „sensible“ Daten (wie in Artikel 8 der Richtlinie aufgeführt) sollten weitere Schutzvorkehrungen getroffen werden, wie etwa die Anforderung, dass die betroffene Person ihre ausdrückliche Einwilligung zur Datenverarbeitung geben muss.

Die Datenschutzgruppe ist der Ansicht, dass dieser Grundsatz im uruguayischen Datenschutzrecht gewahrt ist.

In Artikel 4 Buchstabe e des LPDP sind sensible Daten als „personenbezogene Daten“ definiert, „aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder moralische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft oder Hinweise auf die persönliche Gesundheit und das Sexualleben erkennbar werden“. Insbesondere hinsichtlich der gesundheitsbezogenen Daten enthält Abschnitt 4 Buchstabe d des DPDP weitere Klarstellungen zur Definition dieser Daten, die mit denen des Gerichtshofs der Europäischen Union vergleichbar sind, denn dort heißt es, dass sensible Daten „Informationen sind, die den früheren, gegenwärtigen und zukünftigen körperlichen und geistigen Gesundheitszustand einer Person betreffen“. Ferner heißt es: „Dazu gehören u. a. Daten, die sich ebenfalls auf die Gesundheit von Personen beziehen, wie der prozentuelle Grad ihrer Behinderung oder genetische Angaben“.

In Artikel 18 des LPDP wird der allgemeine Grundsatz aufgestellt, dass „niemand gezwungen werden darf, sensible Daten preiszugeben. Sie dürfen nur mit ausdrücklicher schriftlicher Einwilligung der betroffenen Person verarbeitet werden“. Weiter heißt es, dass „sensible Daten aus Gründen des gesetzlich zulässigen allgemeinen Interesses oder wenn die beantragende Organisation dazu rechtlich beauftragt ist erhoben und verarbeitet werden können. Sie können auch zu statistischen oder wissenschaftlichen Zwecken verarbeitet werden, wenn kein Zusammenhang mit der betroffenen Person hergestellt wird“.

In Artikel 18 des LPDP heißt es in Bezug auf gesundheitsbezogene Daten, dass „öffentliche oder private Gesundheitseinrichtungen und Angehörige der Gesundheitsberufe, die im wissenschaftlichen Bereich arbeiten, personenbezogene Daten zur körperlichen oder geistigen Gesundheit von von ihnen betreuten oder behandelten Patienten erheben und verarbeiten können, sofern dabei die Grundsätze der Vertraulichkeit, die spezifischen Vorschriften und die allgemeinen Bestimmungen dieses Datenschutzgesetzes“ eingehalten werden. In Bezug auf die Übermittlung von gesundheitsbezogenen Daten heißt es in Artikel 17, dass die Einwilligung der betroffenen Person nicht eingeholt zu werden braucht, wenn „es sich um personen- und gesundheitsbezogene Daten handelt, die aus Gründen der öffentlichen Gesundheit und der Hygiene, Notfallsituationen oder für epidemiologische Studien erforderlich sind, sofern die Identität der betroffenen Personen im Wege angemessener Anonymisierungsmechanismen gewahrt werden kann“.

Des Weiteren untersagt Artikel 18 des LPDP „die Anlage von Datenbanken zur Speicherung von Informationen, die direkt oder indirekt sensible Daten enthalten. Ausnahmen sind Daten im Besitz von politische Parteien, Gewerkschaften, Kirchen, Glaubensgemeinschaften, Vereinigungen, Stiftungen oder anderen gemeinnützigen Einrichtungen, die diese Daten zu politischen, religiösen oder philosophischen Zwecken aufbewahren, oder Daten, die sich auf die Zugehörigkeit zu einer Gewerkschaft oder einer Rasse oder Volksgruppe, den Gesundheitszustand oder das Sexualleben beziehen und genauen Aufschluss über Partner und Mitglieder geben. Die Weitergabe solcher Daten bedarf stets der vorherigen Einwilligung der betroffenen Person“.

2) Direktmarketing: Erfolgt die Weitergabe von Daten zu Zwecken des Direktmarketing, sollte die betroffene Person jederzeit Widerspruch gegen die Verwendung ihrer Daten zu diesem Zweck einlegen können.

Die Datenschutzgruppe hält diesen Grundsatz in Artikel 21 des LPDP für abgedeckt, wo auf die Umstände hingewiesen wird, unter denen „Anschriften gesammelt, Dokumente verbreitet und Werbe-, Absatz- oder ähnliche Tätigkeiten erfolgen“.

Danach wird Folgendes festgestellt: „Wenn Daten, die zur Erstellung von bestimmten Profilen für die Absatzförderung, und zu Geschäfts- und Werbezwecken verarbeitet oder mit deren Hilfe Verbrauchsgewohnheiten ermittelt werden können, in öffentlich zugänglichen Dokumenten erscheinen oder von den betroffenen Personen selbst bereitgestellt wurden oder mit ihrer Einwilligung ermittelt wurden“ – wobei anerkannt wird, dass in allen Fällen jederzeit vom Recht auf Zugang zu den Daten Gebrauch gemacht werden kann – dann – so heißt es klar im letzten Absatz dieses Artikels – „kann die betroffene Person jederzeit beantragen, dass ihre Daten in den Datenbanken, auf die sich dieser Artikel bezieht, gelöscht oder gesperrt werden“.

3) Automatisierte Einzelentscheidung: Erfolgt die Weitergabe von Daten im Zuge einer automatisierten Einzelentscheidung im Sinne von Artikel 15 der Richtlinie, muss die betroffene Person das Recht haben, die Gründe für diese Entscheidung zu erfahren. In diesem Fall sind andere Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu ergreifen.

Die Datenschutzgruppe bestätigt, dass dieser Grundsatz ausdrücklich in Artikel 16 des LPDP anerkannt ist, der auf der allgemeinen Regel fußt, dass „jeder das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten oder anderweitigen Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens“.

Des Weiteren steht im dritten Absatz dieses Artikels ein Grundsatz, der mit dem im Dokument WP12 vergleichbar ist, denn er besagt, dass „die betroffene Person das Recht hat, vom für die Verarbeitung Verantwortlichen Aufschluss sowohl über die Bewertungskriterien als auch über das für die Verarbeitung verwendete Programm zu erhalten, das der Entscheidung in diesem Fall zugrunde lag“.

3.3. Verfahrens-/Durchsetzungsmechanismen

Die Stellungnahme der Arbeitsgruppe WP12 „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 25 und 26 der EU-Datenschutzrichtlinie“ besagt, dass zur Bewertung der Frage, ob das Rechtssystem eines Drittlandes einen angemessenen Schutz gewährleistet, zwischen den grundlegenden Zielen eines Datenschutzsystems zu unterscheiden ist. Auf dieser Grundlage ist die Vielfalt der verschiedenen in den einzelnen Ländern verwendeten Mechanismen in Form von rechtlichen und nicht-rechtlichen Verfahren zu bewerten.

Im Grunde können mit einem Datenschutzsystem drei Ziele verfolgt werden:

- möglichst weitgehende Einhaltung der einschlägigen Rechtsvorschriften;
- Bereitstellung von Unterstützung und Hilfe für die betroffenen Personen;
- Bereitstellung von Abhilfe für die betroffenen Personen im Fall der Missachtung der Vorschriften.

a) Möglichst weitgehende Einhaltung der einschlägigen Rechtsvorschriften:
 Grundsätzlich zeichnet sich ein gutes System durch für die Verarbeitung Verantwortliche aus, die ihre Pflichten genau kennen und durch betroffene Personen, die ihre Rechte und die Möglichkeiten ihrer Wahrnehmung genau kennen. Zur Gewährleistung der Einhaltung der Vorschriften sind wirksame Sanktionen und abschreckende Maßnahmen sowie Systeme wichtig, mit denen die Behörden, Prüfer und unabhängige für den Datenschutz zuständige Beamte die Einhaltung der Rechtsvorschriften direkt überprüfen können.

Die Datenschutzgruppe ist der Auffassung, dass dieses Ziel durch verschiedene Vorkehrungen des uruguayischen Rechts erfüllt wird, insbesondere:

Das Organ für die Regulierung und Kontrolle personenbezogener Daten (URCDP)

Das LPDP sieht in Artikel 31 die Schaffung eines Kontrollorgans für den Datenschutz vor, „Organ für die Regulierung und Kontrolle personenbezogener Daten“ (URCDP nach den spanischen Initialen) genannt, das ein autonomes Organ der Agentur für die Entwicklung von e-Government und der wissensbasierten Gesellschaft (AGESIC nach den spanischen Initialen) ist. Dieses autonome Organ verfügt über umfassende technische Autonomie“.

Die AGESIC umfasst zwei autonome Organe, nämlich das bereits erwähnte Kontrollorgan URCDP und das Organ für den Zugang zu öffentlichen Informationen (UAIP nach den spanischen Initialen).

Die Datenschutzgruppe nimmt die Bemerkungen der uruguayischen Behörden zur Existenz von „Regulierungsorganen“ zur Kenntnis, bei denen es sich um autonome Organe innerhalb der Organisationsstruktur des Staates handelt, die über technische Autonomie verfügen und mit ihren Befugnissen keinerlei Mandat oder Weisungen unterliegen. Diese Form der Autonomie ist im uruguayischen Recht generell für allgemeine und wirtschaftliche Regulierungsorgane ausdrücklich vorgesehen. Das Kontrollorgan URCDP ist von der Organisation her mit den Regulierungsorganen für den Telekommunikationssektor, Energiesektor oder für öffentliche Informations- und Planungszwecke vergleichbar.

Hinsichtlich der Struktur heißt es in Artikel 31 des LPDP, dass das URCDP „von einem aus drei Mitgliedern bestehenden Rat geleitet wird: dem Exekutivdirektor der AGESIC und zwei von der Exekutive bestellten Mitgliedern, die aufgrund ihres persönlichen Hintergrunds, ihrer Berufserfahrung und ihrer Kenntnisse auf diesem Gebiet ausgewählt werden, und die ihr unabhängiges Urteilsvermögen, ihre Effizienz, Objektivität und Unparteilichkeit bei der Wahrnehmung ihrer Aufgaben gewährleisten“. Die Datenschutzgruppe nimmt zur Kenntnis, dass mit dem Verweis auf die Exekutive der Staatspräsident gemeint ist und dass dieses Verfahren für die Bestellung der Mitglieder des Kontrollorgans im uruguayischen Recht verankert ist.

Dem Exekutivrat steht ein Beratendes Gremium zur Seite, das aus fünf Mitgliedern besteht:

- einer Person, die für ihren Einsatz für die Förderung und Verteidigung der Menschenrechte bekannt ist, und von der Legislative benannt wird, jedoch nicht aktives Parlamentsmitglied sein darf;
- einem Vertreter der Justiz;
- einem Vertreter der Staatsanwaltschaft;
- einem Vertreter der Wissenschaft;
- einem Vertreter des Privatsektors, der in Einklang mit den einschlägigen Vorschriften ausgewählt wird.

Hinsichtlich der Unabhängigkeit dieses Kontrollorgans hat die Datenschutzgruppe in der uruguayischen Gesetzgebung, insbesondere nach der Verabschiedung des DPDP, hinreichende Hinweise gefunden um davon ausgehen zu können, dass diese Unabhängigkeit auch für das URCDP gilt.

Zunächst heißt es im LPDP ausdrücklich, dass die Mitglieder des Exekutivrats „keine Weisungen in fachlichen Angelegenheiten erhalten“. Die uruguayischen Behörden haben dazu erklärt, dass dieser Wortlaut im weitesten Sinn zu verstehen ist.

Des Weiteren besagt Artikel 29 des DPDP, dass „sich das URCDP bei seiner Verwaltungsarbeit von den Grundsätzen der Unparteilichkeit, Zügigkeit, Effizienz und sachlichen Richtigkeit leiten lässt und dabei nach informellen Gesichtspunkten, einem angemessenen Verfahren, von Amts wegen, nach den Prinzipien von Treu und Glauben, begründeten Entscheidungen und dem Prinzip der Einfachheit vorgeht, die als Auslegungskriterien bei der Lösung von Problemen dienen, die sich bei der Bearbeitung von Einzelfällen ergeben können“.

Für die Mitglieder des Exekutivrats sieht das LPDP eine befristete Amtszeit vor, wobei die Möglichkeiten zur Amtsenthebung ausdrücklich eingeschränkt werden. So heißt es in Artikel 31, dass „mit Ausnahme des Exekutivdirektors der AGESIC alle Mitglieder des Exekutivrats für vier Jahre mit der Möglichkeit der Wiederernennung im Amt bleiben. Sie scheiden aus dem Amt nur nach Ablauf ihrer Amtszeit und Ernennung ihrer Nachfolger oder bei einer Amtsenthebung durch die Exekutive aufgrund von Inkompetenz, unterlassenem oder kriminellen Handeln unter Einhaltung eines ordnungsgemäßen Verfahrens aus“.

Die Datenschutzgruppe stellt mit Genugtuung fest, dass mit den Vorschriften des DPDP die Rolle der beiden anderen Mitglieder des Exekutivrats – neben dem Exekutivdirektor der AGESIC – gestärkt werden. Dadurch wird die Rolle des Exekutivdirektors etwas eingeschränkt, was dem Kontrollorgan ein höheres Maß an Unabhängigkeit verleiht.

In diesem Zusammenhang heißt es in Artikel 21 des DPDP, dass „im jährlichen Wechsel eines der drei Mitglieder des Exekutivrats den Vorsitz des URCDP übernimmt, mit Ausnahme des Exekutivdirektors der Agentur für die Entwicklung von e-Government und der wissenschaftlichen Gesellschaft (AGESIC). Während einer zeitweiligen Abwesenheit des Vorsitzenden des URCDP wird der Vorsitz vorübergehend von einem von der Exekutive

benannten Mitglied wahrgenommen“. Dadurch entfällt die Möglichkeit, dass der Vorsitz in diesem Organ auf den Exekutivdirektor der AGESIC entfällt.

Diese Regelung ist von besonderer Relevanz, da Artikel 24 Buchstabe a des DPDP besagt, dass die Entscheidungen des Rats per Mehrheitsbeschluss erfolgen. Ferner heißt es, dass „im Falle eines unentschiedenen Votums die betreffende Angelegenheit auf der nachfolgenden Sitzung erneut zu erörtern ist. Hat sich bis dahin nichts an der Stimmenverteilung geändert, zählt die Stimme des Vorsitzenden doppelt“. Damit wird verhindert, dass die Gegenstimme des Exekutivdirektors der AGESIC, dessen Amtszeit einer anderen Regelung als die der Mitglieder des Exekutivrats unterliegt, alleinige Grundlage einer Entscheidung des Kontrollorgans wird.

Die Datenschutzgruppe bestätigt des Weiteren, dass zu den Befugnissen des Vorsitzenden des URCDP auch die Pflicht gehört, „Maßnahmen zu ergreifen, die er in Krisensituationen für angebracht hält, diese auf der ersten Sitzung des Exekutivrats bekanntzugeben und sich anschließend an die dort gefällten Entscheidungen zu halten“.

Die Datenschutzgruppe erkennt an, dass sich die Unabhängigkeit des Kontrollorgans in der Praxis bestätigt hat, da sich an seiner Tätigkeit trotz des Regierungswechsels in Uruguay im Jahr 2009 nichts geändert hat. Dies geht auch aus den Informationen über die Tätigkeit dieses Organs in den Jahren 2009 und 2010 hervor, die die Datenschutzgruppe vom URCDP erhalten hat.

Hinsichtlich der Befugnisse des Kontrollorgans kann die Datenschutzgruppe bestätigen, dass diese mit denen in Artikel 28 der Datenschutzrichtlinie identisch sind. Artikel 34 des LPDP besagt, dass das URDPD folgende Funktionen und Befugnisse hat:

- Bereitstellung von Unterstützung und Beratung von Personen, die darauf zum Verständnis des Anwendungsbereichs dieses Gesetzes und der verfügbaren Rechtsinstrumente zum Schutz der ihnen durch dieses Gesetz gewährleisteten Rechte angewiesen sind;
- Erstellung von Regeln und Vorschriften für die Ausführung der Aktivitäten, die von diesem Gesetz geregelt werden;
- Erfassung der von diesem Gesetz erfassten Datenbanken und Führung eines permanenten Registers dieser Datenbanken;
- Überwachung, inwieweit sich die für die Datenbanken Verantwortlichen an die Vorschriften zur Integrität, sachlichen Richtigkeit und der Sicherheit von Daten halten. Dazu sollten sie in der Lage sein, die zu diesen Zwecken notwendigen Inspektionen durchzuführen;
- Anforderung von Informationen von öffentlichen und privaten Stellen, die verpflichtet sind, alle für die Verarbeitung personenbezogener Daten erforderlichen Hintergrundinformationen, Dokumentationen, Programme und sonstigen Elemente vorzulegen. In diesen Fällen hat das Kontrollorgan die Sicherheit und Vertraulichkeit der vorgelegten Informationen und Elemente zu gewährleisten;

- Abgabe von Stellungnahmen, wenn sie dazu von den jeweiligen Behörden aufgefordert wird; dies gilt auch für Anträge auf Verhängung von Verwaltungssanktionen wegen Verstößen gegen dieses Gesetz oder andere Verordnungen oder Entscheidungen über die Verarbeitung personenbezogener Daten, die unter dieses Gesetz fallen;
- im Bedarfsfall Beratung der Exekutive bei der Erarbeitung von Rechtsvorschriften, die sich ganz oder teilweise auf den Schutz personenbezogener Daten beziehen;
- kostenlose Unterrichtung der Bürger über Datenbanken, in denen personenbezogene Daten gespeichert sind, ihren Zweck und die Identität der für die Datenbanken Verantwortlichen.

Des Weiteren enthält das LPDP wie nachstehend aufgeführt spezifische Vorschriften in Bezug auf Untersuchungen, Inspektionen und Sanktionen, und auch das DPDP enthält spezifische Vorschriften für bestimmte Verfahren beim Kontrollorgan URCDP und insbesondere für die Registrierung, Verarbeitung und Bewilligung internationaler Datentransfers.

Die Datenschutzgruppe weist darauf hin, dass das URCDP von diesen Befugnissen nachweislich bei einer Reihe von Informationen Gebrauch gemacht hat, die im Zuge der in diesem Dokument beschriebenen Untersuchung der Angemessenheit des Datenschutzes vorgelegt wurden.

Aus all diesen Gründen kommt die Datenschutzgruppe an dieser Stelle zu dem Schluss, dass Uruguay über eine Aufsichtsbehörde für den Datenschutz verfügt, die die notwendige Unabhängigkeit und angemessene Vollstreckungskompetenzen aufweist, die mit denen in Artikel 28 der Richtlinie vergleichbar sind.

Umsetzung und Sanktionen

Artikel 12 des LPDP besagt, dass „der für die Datenbanken oder die Datenverarbeitung Verantwortliche für jeden Verstoß gegen die Bestimmungen dieses Gesetzes haftet“.

Gemäß Artikel 34 Buchstabe e kann das Kontrollorgan URCDP „Informationen von öffentlichen und privaten Stellen anfordern, die verpflichtet sind, alle für die Verarbeitung personenbezogener Daten erforderlichen Hintergrundinformationen, Dokumentationen, Programme und sonstigen Elemente vorzulegen. In diesen Fällen hat die Kontrollstelle die Sicherheit und Vertraulichkeit der vorgelegten Informationen und Elemente zu gewährleisten“.

In Artikel 35 des LPDP wird die Möglichkeit der Ergreifung von Zwangsmaßnahmen bei Verstößen gegen das Datenschutzrecht geschaffen. Dort heißt es, dass „das Kontrollorgan bei Verstößen gegen dieses Gesetz die folgenden Sanktionen gegen die für die Datenbanken oder die Datenverarbeitung Verantwortlichen verhängen kann:

- a) Verwarnung;
- b) Geldbuße von höchstens fünfhunderttausend indexierten Währungseinheiten;
- c) Sperrung der entsprechenden Datenbank. Die AGESIC kann den zuständigen Stellen der Justiz die Sperrung von Datenbanken für einen Zeitraum von

höchstens sechs Arbeitstagen raten, sofern ein Verstoß gegen das Datenschutzrecht nachgewiesen wurde.

Diese Befugnis des URCDP zur Verhängung von Zwangsmaßnahmen in derartigen Fällen ist ebenso in Artikel 31 des DPDP verankert, wonach das Kontrollorgan folgende Befugnisse hat:

- Durchführung von Inspektionen nach Ermessen des Exekutivrats, auf der Basis eines begründeten Beschlusses;
- Ersuchen eines zuständigen Gerichts um Ergreifung angemessener Maßnahmen, wenn die Gefahr besteht, dass Beweise verloren gehen. Das Ersuchen um derartige Maßnahmen bedarf einer begründeten Entscheidung des Exekutivrats;
- Mitteilung aller Maßnahmen an den für die Datenbank oder die Datenverarbeitung Verantwortlichen zur Kenntnisnahme. Der Verantwortliche hat sodann zehn Tage ab dem Tag nach der Mitteilung Zeit, um Abhilfe zu schaffen. Ist dieser Zeitraum verstrichen, wird der Exekutivrat mit den beanstandeten Sachverhalten befasst, der binnen 30 Tagen zu entscheiden hat. Gegen die Entscheidung kann nach den einschlägigen Rechtsvorschriften Einspruch erhoben werden.

Demnach ist die Datenschutzgruppe der Ansicht, dass das uruguayische Recht Untersuchungsbefugnisse und Sanktionsmaßnahmen vorsieht, die mit denen der Aufsichtsorgane der Mitgliedstaaten gemäß Artikel 28 der Richtlinie vergleichbar sind.

b) Bereitstellung von Unterstützung und Hilfe für betroffene Personen:

Die betroffene Person muss ihre Rechte rasch und wirksam ohne übermäßige Kosten wahrnehmen können. Dazu muss es einen institutionellen Mechanismus geben, so dass Beschwerden unabhängig untersucht werden können.

Die Datenschutzgruppe stellt fest, dass das uruguayische Recht zu diesem Zweck verschiedene Mechanismen vorsieht.

Zunächst heißt es in Artikel 34 Buchstabe a des LPDP, dass „das Kontrollorgan alle erforderlichen Maßnahmen zur Erfüllung der Ziele und der Einhaltung der Bestimmungen dieses Gesetzes ergreift“. Eine seiner Aufgaben besteht in der „Bereitstellung von Unterstützung und Beratung für die Personen, die darauf zum Verständnis des Anwendungsbereichs dieses Gesetzes und der verfügbaren Rechtsinstrumente zum Schutz der ihnen durch dieses Gesetz gewährleisteten Rechte angewiesen sind“.

Aufgrund dieser Tätigkeit kann ein Untersuchungsverfahren und gegebenenfalls ein Sanktionsverfahren eingeleitet werden, wobei das Verfahren wie im DPDP geregelt vom Kontrollorgan selbst oder auf Ersuchen einer betroffenen Partei eingeleitet werden kann.

Des Weiteren enthält Artikel 34 Buchstabe h eine weitere Aufgabe des URCDP, nämlich „die kostenlose Unterrichtung der Bürger über das Bestehen von Datenbanken mit personenbezogenen Daten, ihren Zweck und die Identität der für die Datenbanken

Verantwortlichen“ und die Regulierung der einschlägigen Registrierungsverfahren und der Verzeichnisse.

Neben diesen Aufgaben sieht das uruguayische Recht Maßnahmen zur Stärkung des Bewusstseins für das Datenschutzrecht bei den betroffenen Personen und denen vor, die diese Vorschriften einzuhalten haben.

Dies geschieht z. B. im Wege der Transparenz bei der Verbreitung der Entscheidungen und Stellungnahmen des Kontrollorgans. In diesem Zusammenhang heißt es in Artikel 25 des DPDP, dass „das URCDP alle seine Entscheidungen nach ihrer Bekanntgabe auf seiner Website veröffentlicht. Diese Veröffentlichung erfolgt unter Anwendung der einschlägigen Kriterien zur Anonymisierung der personenbezogenen Daten“.

Die Datenschutzgruppe geht davon aus, dass die zweite Möglichkeit der Unterstützung von betroffenen Personen, die über den Schutz ihrer Rechte besorgt sind, im Rahmen des „Habeas data“-Rechtsbehelfs in Kapitel VII des LPDP besteht.

So heißt es in Artikel 38 des LPDP, dass die betroffene Person in folgenden Fällen Beschwerde oder einen Antrag auf einstweilige Verfügung im Sinne des „Habeas data“-Rechtsbehelfs gegen jeden Verantwortlichen einer öffentlichen oder privaten Datenbank einreichen kann,

- wenn die betroffene Person ihre in einer Datenbank oder einem ähnlichen Speichermedium gespeicherten personenbezogenen Daten einsehen möchte und dieses Ersuchen abgelehnt wird oder der für die Datenbank Verantwortliche bei dieser Gelegenheit nicht innerhalb der gesetzlich dafür vorgesehenen Fristen auf dieses Ersuchen eingeht;
- wenn die betroffene Person den für die Datenbank oder die Datenverarbeitung Verantwortlichen um Berichtigung, Aktualisierung, Aufnahme oder Löschung von Daten ersucht und der für die Datenbank Verantwortliche diesem Ersuchen nicht innerhalb der dafür gesetzlich vorgesehenen Frist nachkommt oder dafür keine hinreichenden Gründe angibt.

Eine solche Beschwerde ist ein Rechtsbehelf, der sich rasch bearbeiten lässt und der von der betroffenen Person oder ihrem rechtlichen Vertreter oder im Fall von Verstorbenen von ihren Gesamtrechtsnachfolgern eingereicht werden kann. Er unterliegt den einschlägigen Verfahrensvorschriften, die im Einzelnen im LPDP geregelt sind.

Gemäß Artikel 43 des LPDP „sollte eine Entscheidung auf der Grundlage des „Habeas data“-Rechtsbehelfs folgende Elemente umfassen:

- Klare Angabe der Behörde oder Person, gegen die die Beschwerde erhoben wurde und gegen deren Vorgehen, Einzelhandlung oder Unterlassung die Entscheidung im Sinne des „Habeas data“-Rechtsbehelfs getroffen wird;
- präzise Reihenfolge der angemahnten Handlungen oder Unterlassungen und gegebenenfalls Angabe der Frist, während der die Entscheidung gilt;

- Angabe der Frist zur Schaffung von Abhilfe im Sinne der Entscheidung, die von einem Gericht nach den Umständen des jeweiligen Falls festzusetzen ist und die nicht länger als 15 ununterbrochen aufeinanderfolgende Kalendertage ab dem Datum der Bekanntgabe ausfallen darf.

Angesichts dieser Regelungen ist die Datenschutzgruppe wie bereits erwähnt der Ansicht, dass das uruguayische Recht hinreichende Mechanismen vorsieht, um den betroffenen Personen Hilfe und Unterstützung leisten zu können.

c) Bereitstellung angemessener Rechtsbehelfe zur Entschädigung von betroffenen Personen bei der Missachtung von Rechtsvorschriften: Dies ist ein Schlüsselement, das unbedingt zu einem System gehört, das betroffenen Personen die Möglichkeit bietet, im Wege eines Rechts- oder Schiedsverfahrens Entscheidungen zu erwirken oder gegebenenfalls Schadensersatz zu erhalten oder Sanktionen zu verhängen.

Artikel 12 des LPDP besagt, dass „der für die Datenbank Verantwortliche für jeden Verstoß gegen die Bestimmungen dieses Gesetzes haftet“.

Die Datenschutzgruppe stellt fest, dass kraft der Bestimmungen dieses Artikels und der allgemeinen Struktur des uruguayischen Zivilrechts, insbesondere seines Bürgerlichen Gesetzbuches jede betroffene Person, die aufgrund der Verarbeitung ihrer personenbezogenen Daten einen Schaden erlitten hat, Rechtsmittel zur Entschädigung einlegen kann. Diese Entschädigung kann sowohl für erlittenen materiellen als auch moralischen Schaden gewährt werden.

Daher ist die Datenschutzgruppe der Ansicht, dass diese Gewährleistung ordnungsgemäß in uruguayischen Recht verankert ist.

4. ERGEBNIS DER BEWERTUNG

Abschließend stellt die Datenschutzgruppe angesichts des vorstehenden Rechtsvergleichs fest, dass **die Republik Östlich des Uruguay** hinsichtlich des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des freien Datenverkehrs ein im Sinne von Artikel 25 Absatz 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 **angemessenes Schutzniveau gewährleistet**.

Die Datenschutzgruppe weist ferner mit Nachdruck darauf hin, dass sie im Falle eines einschlägigen Beschlusses der Kommission die Entwicklung des Datenschutzes in Uruguay und die Anwendung der in Dokument WP12 und in diesem Dokument genannten Grundsätze durch die Datenschutzbehörde (URCDP) genau mitverfolgen wird.

Brüssel, den 12. Oktober 2010

Für die Arbeitsgruppe
Der Vorsitzende
Jacob KOHNSTAMM