ARTIKEL-29-DATENSCHUTZGRUPPE

02072/07/DE
WP 141

Stellungnahme 8/2007 zum Umfang des Schutzes personenbezogener Daten in Jersey

Angenommen am 9. Oktober 2007

STELLUNGNAHME DER GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995

zum Umfang des Schutzes personenbezogener Daten in Jersey

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[1], („die Richtlinie"), insbesondere auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe b,

gestützt auf ihre Geschäftsordnung[2], insbesondere auf Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINFÜHRUNG: DATENSCHUTZGESETZ IN JERSEY

1.1. Situation der Kanalinseln und Jerseys

Die Kanalinseln umfassen fünf Hauptinseln - Jersey, Guernsey, Alderney, Herm und Sark - und liegen vor der Nordwestküste Frankreichs in der St.-Malo-Bucht im Ärmelkanal. Sie gehören nicht zum Vereinigten Königreich und sind im Parlament des Vereinigten Königreichs in Westminster nicht vertreten. Verfassungsrechtlich sind sie in die Bailiwicks (Selbstverwaltungsgebiete) Guernsey und Jersey unterteilt.

Das Bailiwick Jersey ist ein Schutzgebiet des Vereinigten Königreichs. Das Vereinigte Königreich ist zuständig für die internationalen Angelegenheiten und die Verteidigung von Jersey. Die Insel Jersey genießt Unabhängigkeit in Bezug auf ihre internen Angelegenheiten, einschließlich des Bereichs Datenschutz. Obwohl die Behörden des Vereinigten Königreichs für alle Verhandlungen über internationale Verträge zuständig sind, erstreckt sich eine Ratifizierung durch das Vereinigte Königreich nur dann auf Jersey, wenn die Behörden des Bailiwick dies ausdrücklich verlangen.

Jersey gehört zum Zollgebiet der Europäischen Gemeinschaften. Für Handelsbeziehungen zwischen Jersey und Drittländern gelten der Gemeinsame Zolltarif, Abschöpfungen und andere Bestimmungen für Agrareinfuhren. Zwischen

---

1 ABl. L 281 vom 23.11.1995, S. 31, abzurufen unter: http://europa.eu.int/comm/internal_market/de/media/dataprot/index.htm

2 Verabschiedet auf der dritten Sitzung der Gruppe am 11.9.1996.

Jersey und der Gemeinschaft herrscht freier Warenverkehr. Gemeinschaftsvorschriften aus anderen Bereichen, einschließlich Datenschutzvorschriften, gelten allerdings nicht. Zum Zeitpunkt der Umsetzung der Richtlinie durch das Vereinigte Königreich erklärten die Behörden von Jersey, dass diese Vorschriften in Jersey nicht angewendet werden, und führten eine eigene Datenschutzregelung ein.

Gemäß Artikel 299 des Vertrags zur Gründung der Europäischen Gemeinschaft ist die Richtlinie für Jersey nicht gültig, so dass Jersey im Sinne der Artikel 25 und 26 der Richtlinie als Drittland gilt.

1.2. Geltender datenschutzrechtlicher Rahmen

Im Namen des Bailiwick wurden folgende Übereinkommen ratifiziert:
- Europäische Konvention zum Schutze der Menschenrechte und der Grundfreiheiten (EMRK)
- Internationaler Pakt über bürgerliche und politische Rechte
- Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte
- Übereinkommen der Vereinten Nationen zur Beseitigung der Rassendiskriminierung
- Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108)

Das Datenschutzgesetz von Jersey aus dem Jahr 1987, das am 11. November 1987 in Kraft trat, basierte auf dem Data Protection Act 1984 des Vereinigten Königreichs, jedoch war die Kontrollstelle, das Amt des Datenschutzbeauftragten, keine unabhängige Stelle, sondern unterstand der Regierung.

Mit dem Data Protection Law 2005 (Jersey), das dem Data Protection Act 1998 des Vereinigten Königreichs sowie den auf diesem Gesetz beruhenden abgeleiteten Rechtsvorschriften nachgebildet ist, wurden grundlegende Reformen eingeführt, um den Anforderungen der Richtlinie nachzukommen.

2. BEURTEILUNG DES DATENSCHUTZGESETZES VON JERSEY IM HINBLICK AUF EINEN ANGEMESSENEN SCHUTZ PERSONENBEZOGENER DATEN

Die Artikel-29-Datenschutzgruppe („Gruppe“) beurteilt die Angemessenheit des Datenschutzgesetzes von Jersey anhand des Data Protection Law 2005 (Jersey).

Beurteilungskriterien

Die Kriterien für die Beurteilung des Datenschutzsystems in Jersey, die im Dokument *Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU* (WP 12 5025/98)[3] der Datenschutzgruppe niedergelegt sind, lassen sich wie folgt zusammenfassen:

1. Inhaltliche Grundsätze
    - Beschränkung der Zweckbestimmung

[3] Siehe auch Europäische Kommission (Hg.), *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data*, Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 1998.

- Datenqualität und -verhältnismäßigkeit
- Transparenz
- Sicherheit
- Recht auf Zugriff, Berichtigung und Widerspruch
- Beschränkung der Weiterübermittlung in andere Drittländer
- Weitere, auf spezifische Arten der Verarbeitung anwendbare Grundsätze, wie z. B. auf i) sensible Daten, ii) Direktmarketing und iii) automatisierte Einzelentscheidungen

2. Verfahrensrechtlicher Mechanismus/Durchsetzungsmechanismus
    - Gewährleistung einer guten Befolgungsrate der Vorschriften
    - Unterstützung für einzelne betroffene Personen
    - Gewährleistung angemessener Entschädigung für die geschädigte Partei

Definition und Anwendungsbereich des Datenschutzgesetzes von Jersey (2005)

In der Präambel des Gesetzes wird dargelegt, dass es sich um eine Maßnahme handelt, um „*neue Bestimmungen für die Regelung der Verarbeitung personenbezogener Daten, einschließlich Einholung, Speicherung, Nutzung und Weitergabe solcher Daten, sowie für die dazugehörigen und damit verbundenen Zwecke zu schaffen*“.

Das Datenschutzgesetz übernimmt die folgenden Definitionen zentraler Datenschutzkonzepte:

Personenbezogene Daten

Personenbezogene Daten sind *Daten, die sich auf eine lebende natürliche Person beziehen, die identifiziert werden kann –*

a) anhand dieser Daten oder

b) anhand dieser Daten und anderer Informationen, die sich im Besitz des für die Verarbeitung Verantwortlichen befinden oder voraussichtlich in dessen Besitz kommen,

und die jede Meinungsäußerung über eine natürliche Person einschließen, die daraufhin identifiziert werden kann, sowie Angaben zu den Intentionen des für die Verarbeitung Verantwortlichen oder jeder anderen Person im Hinblick auf eine natürliche Person, die daraufhin identifiziert werden kann. [4]

Diese Definition unterscheidet sich von der Definition in der Richtlinie. Insbesondere bestimmt das Gesetz von Jersey, dass eine natürliche Person anhand der Informationen, die im Besitz des für die Verarbeitung Verantwortlichen sind oder voraussichtlich in dessen Besitz kommen, identifiziert werden kann. Im Gegensatz dazu wird in Artikel 2 der Richtlinie definiert, dass *eine Person als bestimmbar angesehen wird, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.* Laut Erwägung 26 sollten *bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt*

[4] Artikel 1.

werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Das heißt, dass Informationen, die sich auf eine natürliche Person beziehen und die Identifizierung der Person nicht durch den für die Verarbeitung Verantwortlichen, sondern einen Dritten ermöglichen, nach der Richtlinie unter den Datenschutz fallen, während nach dem Gesetz von Jersey nur diejenigen Informationen unter den Datenschutz fallen, die eine Identifizierung ermöglichen und in den Besitz des für die Verarbeitung Verantwortlichen gelangen können.

Was den Begriff „beziehen" in der Definition betrifft, so ist auf die Rechtsprechung des Vereinigten Königreichs im Fall Durant hinzuweisen. In diesem Urteil hat das Berufungsgericht (Court of Appeal) des Vereinigten Königreichs zwei Kriterien für Fälle festgelegt, in denen nicht klar ist, ob sich Daten auf eine Person beziehen und folglich personenbezogene Daten im Sinne des Datenschutzgesetzes des Vereinigten Königreichs darstellen. Es handelt sich dabei um die Frage, ob die Daten in einem „*maßgeblichen Sinne biografisch*" sind und ob sich die „*Informationen auf die betroffene Person konzentrieren*". Diese Begriffe sind ihrerseits Teil der eher allgemeinen Überlegung in Zweifelsfällen, ob es sich bei den Daten um Informationen handelt, die sich auf *die Privatsphäre der betroffenen Person auswirken*.

Angesichts der engen Verknüpfung zwischen dem Rechtssystem von Jersey und seinem englischen Gegenstück und der Besetzung des Berufungsgerichts von Jersey mit englischen Juristen ist es möglich, dass diese Entscheidung befolgt wird. Da eine solche Interpretation die Definition der personenbezogenen Daten in der Richtlinie einengt, wird der Umfang, in dem personenbezogene Daten durch die Rechtsvorschriften von Jersey geschützt werden, möglicherweise eingeschränkt.

Einschlägige Datei

Der Begriff „einschlägige Datei" entspricht gemäß der Definition des Gesetzes:

> *einer beliebigen Sammlung von Informationen, die sich auf natürliche Personen beziehen, soweit die Sammlung, auch wenn die Informationen nicht von automatisch betriebenen Geräten anhand entsprechender Anweisungen bearbeitet werden, entweder durch Verweise auf natürliche Personen oder durch Verweise auf personenbezogene Kriterien so strukturiert ist, dass spezifische sich auf eine bestimmte Person beziehende Informationen leicht zugänglich sind.*[5]

Das Gesetz von Jersey verwendet dieselbe Formulierung wie der Data Protection Act 1988 des Vereinigten Königreichs, die von der Rechtsprechung auf der Grundlage des Urteils des englischen Berufungsgerichts im Fall *Durant gegen Financial Services Authority*[6] eng ausgelegt wird. Das Berufungsgericht entschied, dass sich „eine „einschlägige Datei" im Sinne dieses Gesetzes auf ein System beschränkt: 1) *in dem die daraus bestehenden Akten so strukturiert oder referenziert sind, dass zu Beginn einer Suche deutlich angegeben wird, ob bestimmte Informationen, die personenbezogene Daten einer natürlichen Person darstellen können, in der Datei*

---

5 Artikel 1.

6 [2003] EWCA Civ 1746.

enthalten sind und wenn ja, in welcher Datei sie enthalten sind; und 2) *das als Teil seiner eigenen Struktur oder seines Referenzierungsmechanismus über ein ausreichend entwickeltes und ausführliches Mittel verfügt, um schnell anzugeben, ob und wo in einer Datei spezifische Kriterien oder Informationen über den Anwärter schnell gefunden werden können*". Diese Auslegung ist restriktiver als die Richtlinie, die eine Datei definiert als *jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird,* und die in Erwägung 27 angibt, dass der *Inhalt einer Datei nach bestimmten personenbezogenen Kriterien strukturiert sein muss, die einen leichten Zugriff auf die Daten ermöglichen.* In Fällen, in denen die Datei zwar nach bestimmten personenbezogenen Kriterien strukturiert ist und einen leichten Zugriff auf die Daten ermöglicht, aber die vom Gericht festgelegten Bedingungen nicht erfüllt sind (z. B. wenn die Informationen zu einer Person in einer Datei enthalten sind, die keine Unterverzeichnisse hat, die angeben, welche Art von Informationen enthalten sind), fallen diese Informationen nicht in den Anwendungsbereich des Gesetzes, obwohl sie von den Datenschutzvorschriften der Richtlinie erfasst werden. Angesichts der engen Verknüpfung zwischen dem Rechtssystem von Jersey und seinem englischen Gegenstück und der Besetzung des Berufungsgerichts von Jersey mit englischen Juristen ist es möglich, dass diese Entscheidung befolgt wird. Dennoch wird es eher selten vorkommen, dass derartige, wenig strukturierte manuelle Dateien von einem EU-Mitgliedstaat nach Jersey übermittelt werden. Daher kann trotz dieser Situation davon ausgegangen werden, dass das Gesetz von Jersey im Hinblick auf den Umgang mit manuellen Datensystemen ausreichenden Schutz bietet.

2.1. Inhaltliche Grundsätze

Unbedingt zu berücksichtigende Grundsätze

Der Grundsatz der Beschränkung der Zweckbestimmung verlangt, dass Daten für einen spezifischen Zweck zu verarbeiten und dementsprechend nur zu verwenden oder weiter zu übermitteln sind, soweit dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft aus einem der in Artikel 13 der Richtlinie aufgeführten Gründe notwendigen Fälle. Gemäß Artikel 9 der Richtlinie sind zur Gewährleistung der freien Meinungsäußerung ebenfalls Ausnahmen möglich.

Die Gruppe ist der Überzeugung, dass das Datenschutzgesetz von Jersey diesem Grundsatz entspricht. Im zweiten und fünften Grundsatz von Schedule (Anlage) 1, Part (Teil) 1 des Gesetzes ist vorgesehen, dass personenbezogene Daten ausschließlich für konkrete und rechtmäßige Zwecke erhoben werden und nicht in einer Weise weiterverarbeitet werden dürfen, die mit diesem bzw. diesen Zwecken nicht vereinbar sind. Des Weiteren dürfen sie nicht länger aufbewahrt werden, als für diesen bzw. diese Zwecke notwendig ist.

Der Grundsatz der Datenqualität und -verhältnismäßigkeit verlangt, dass Daten sachlich richtig und, wenn nötig, auf dem neuesten Stand gehalten werden. Die Daten sollen angemessen, relevant und nicht über den Zweck hinausgehen, für den sie übermittelt oder weiterverarbeitet werden.

Im dritten und vierten Grundsatz verlangt das Datenschutzgesetz von Jersey, dass personenbezogene Daten im Hinblick auf die Zweckbestimmungen, für die sie weiterverarbeitet werden, angemessen, geeignet und nicht exzessiv sind, und dass sie sachlich richtig und, wenn nötig, auf dem neuesten Stand gehalten werden. Die Gruppe ist der Auffassung, dass das Gesetz diesem Grundsatz entspricht.

Der Grundsatz der Transparenz verlangt, dass natürliche Personen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten müssen, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2 und 13 der Richtlinie möglich**.**

Das Gesetz wird diesem Grundsatz in Artikel 7 Absatz 1, ergänzt durch Anlage 1, Teil 2, Absatz 2 und 5, gerecht.

Im Datenschutzgesetz von Jersey sind Ausnahmen von der Anwendung des Grundsatzes der Transparenz vorgesehen. Im Allgemeinen beziehen sie sich auf die Tätigkeitsbereiche, die auch im Zusammenhang mit der Beschränkung der Zweckbestimmung beschrieben wurden und beinhalten dieselben Kriterien für die Feststellung, ob die Ausnahme für den betreffenden Zweck erforderlich ist.

Artikel 31 des Gesetzes sieht Ausnahmen für staatliche Maßnahmen zum Schutz vor öffentlichen Vermögensverlusten oder Schäden vor. Artikel 32 des Gesetzes bezieht sich auf die Veröffentlichung journalistischer, literarischer oder künstlerischer Werke von öffentlichem Interesse. Artikel 34 sieht vor, dass der Grundsatz der Transparenz nicht anzuwenden ist, wenn es sich bei den Daten um Informationen handelt, zu deren Veröffentlichung der Datenschutzbeauftragte gesetzlich verpflichtet ist. Die beiden erstgenannten Artikel dürften in den Anwendungsbereich von Artikel 13 der Richtlinie fallen. Artikel 34 entspricht hingegen nicht den Kriterien des Artikels 13. Er bezieht sich auf eine Ausnahme, die nicht als erforderliche Maßnahme zum Schutz der unter Artikel 13 genannten wichtigen öffentlichen Interessen betrachtet werden kann und nicht gerechtfertigt ist, da die Daten, die der für die Verarbeitung Verantwortliche allgemein zugänglich macht (z. B. Daten zur Rechtsstellung eines Hauses in einem öffentlichen Immobilienregister) nicht den Informationen entsprechen, die er der betroffenen Person über die *Verarbeitung* bereitstellen muss (Verantwortlicher, Zweck, Datenkategorien, Empfänger, Auskunftsrecht), und daher nicht an ihre Stelle treten können. Für die Beurteilung der Angemessenheit ist der Schutz personenbezogener Daten, die von EU-Mitgliedstaaten nach Jersey übermittelt werden, von Bedeutung, nicht jedoch die intern erfassten Daten betroffener Personen in Jersey. Umstände, unter denen Daten, die aus der EU nach Jersey übermittelt werden, anschließend in einem öffentlichen Register in Jersey veröffentlicht werden, sind kaum vorstellbar. Und selbst wenn dies der Fall wäre, gelten die Verpflichtungen nach dem Transparenzgrundsatz eher für den Übermittelnden aus der EU, als für den Empfänger in Jersey.

Anlage 7 des Gesetzes sieht Ausnahmen vor, wenn sich Daten auf den Einsatz von Streitkräften beziehen und die Einhaltung der Datenschutzbestimmungen diesen Zweck beeinträchtigen könnte. Ausnahmen sind vorgesehen im Hinblick auf Finanzdaten von Unternehmen, die ein wichtiges nationales wirtschaftliches oder finanzielles Interesse darstellen. Weitere Ausnahmen beziehen sich auf Wirtschaftsprognosen, für Verhandlungen mit der betroffenen Person verwendete

Daten und Daten, die unter eine berufliche Schweigepflicht fallen. Diese Ausnahmen erscheinen im Sinne von Artikel 13 der Richtlinie berechtigt.

Ausnahmen im Fall der Ernennung von Richtern und einer Vergabe von Orden oder Ehrenzeichen, die nur in einem engen Bereich gelten, fallen wohl nicht unter die Ausnahmen von Artikel 13 der Richtlinie.

Der Grundsatz der Sicherheit verlangt, dass der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen hat. Alle unter der Verantwortung der für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Auftragsverarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

Die Bestimmungen des Datenschutzgesetzes von Jersey entsprechen offensichtlich den in WP 12 im Hinblick auf den Grundsatz der Sicherheit festgelegten Anforderungen. Die Anforderung, dass ein für die Verarbeitung Verantwortlicher ein angemessenes Sicherheitsniveau anwendet, wird ausdrücklich dargelegt und für den Fall, dass die Verarbeitung für den Verantwortlichen durchgeführt wird, entspricht die Anforderung eines schriftlichen Vertrags, der dem Auftragsverarbeiter Pflichten auferlegt, die dem des Verantwortlichen äquivalent sind, den diesbezüglichen Anforderungen von WP 12.

Das Recht auf Zugriff, Berichtigung und Widerspruch verlangt, dass die betroffene Person das Recht hat, eine Kopie aller sie betreffenden Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muss sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten sind die in Artikel 13 der Richtlinie genannten Ausnahmen.

Was das Recht auf Zugriff anbetrifft, entspricht Artikel 7 des Datenschutzgesetzes wohl den Anforderungen von WP 12. Die dargelegten Ausnahmen vom Recht auf Zugriff dürften mit den gemäß Artikel 13 zulässigen Ausnahmen in WP 12 übereinstimmen.

Was das Recht auf Berichtigung angeht, entspricht Artikel 14 des Datenschutzgesetzes der in WP 12 festgelegten Anforderung, dass die betroffene Person ein Anrecht auf die Berichtigung unrichtiger Daten hat. Das Gesetz geht dabei noch weiter, da ein für die Verarbeitung Verantwortlicher aufgefordert werden kann, die Empfänger dieser Daten über die Berichtigung zu informieren, wenn ein Gericht dies für praktisch durchführbar hält.[7]

Das Recht auf Widerspruch ist in Artikel 10 des Datenschutzgesetzes geregelt. Danach kann eine Verarbeitung verhindert werden, bei der mit einer Schädigung oder Benachteiligung zu rechnen ist. Diese Bestimmung gibt die Anforderungen in WP 12 wieder, dass „unter bestimmten Umständen“ ein Widerspruchsrecht bestehen soll.

---

[7] Artikel 14 Absatz 5.

Die Beschränkung der Weiterübermittlung in andere Drittländer verlangt, dass weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland lediglich zulässig sind, wenn das zweite Drittland (d. h. der Empfänger der Weiterübermittlung) ebenfalls ein angemessenes Schutzniveau aufweist. Die einzigen zulässigen Ausnahmen müssen mit Artikel 26 Absatz 1 der Richtlinie übereinstimmen.

Im achten Grundsatz für den Datenschutz sieht das Gesetz von Jersey vor, dass personenbezogene Daten nicht in ein Land oder Hoheitsgebiet außerhalb des Europäischen Wirtschaftsraums übermittelt werden dürfen, wenn dieses Land oder Hoheitsgebiet kein angemessenes Schutzniveau gemäß den aufgeführten Kriterien gewährleistet.[8]

Für die Anwendung dieses Grundsatzes in Verfahren nach dem Datenschutzgesetz von Jersey sind Entscheidungen der Europäischen Gemeinschaft bezüglich Angemessenheit bzw. fehlender Angemessenheit der Verarbeitung in einem Drittland für die Behörden von Jersey verbindlich.[9]

Das Datenschutzgesetz verlangt nicht, dass bestimmte Übermittlungen außerhalb des Europäischen Wirtschaftsraums dem Datenschutzbeauftragten entweder vor oder nach der Übermittlung gemeldet werden müssen. Allerdings wird verlangt, dass der für die Verarbeitung Verantwortliche im Fall einer Meldung Informationen über die Reihe der Länder außerhalb des Europäischen Wirtschaftsraums bereitstellt, in die Übermittlungen möglich sind. Wenn bis zu zehn Länder betroffen sind, müssen sie namentlich genannt werden, wenn Übermittlungen in mehr als zehn Länder vorgesehen sind, muss in der Meldung angegeben werden, dass Übermittlungen „weltweit“ stattfinden können. Obwohl Datenübermittlungen nicht gemeldet werden müssen, kann der Datenschutzbeauftragte an den für die Verarbeitung Verantwortlichen gemäß Artikel 40 eine *enforcement notice* richten, wenn er der Ansicht ist, dass die Daten unter Umständen übermittelt wurden, unter denen ein angemessenes Schutzniveau nicht gewährleistet ist. Die Entscheidung, ob diese Anforderung erfüllt wurde oder nicht, trifft jedoch der für die Verarbeitung Verantwortliche. Vonseiten der Datenschutzbehörde erfolgen keine begleitenden sichtbaren Prüf- oder Überwachungsmaßnahmen.

Weitere Grundsätze, die auf spezifische Arten der Verarbeitung anwendbar sind:

Sensible Daten - Sind „sensible“ Kategorien von Daten betroffen (die in Artikel 8 der Richtlinie aufgeführt sind), so haben zusätzliche Garantien wie das Erfordernis zu gelten, dass die betroffene Person ausdrücklich in die Verarbeitung einwilligt. Die Definition sensibler Daten im Datenschutzgesetz von Jersey entspricht Artikel 8.

Das Datenschutzgesetz schreibt vor, unter welchen Bedingungen sensible Daten verarbeitet werden dürfen. WP 12 verlangt, dass für die Verarbeitung sensibler personenbezogener Daten zusätzliche Sicherheitsmaßnahmen mit einem besonderen Verweis auf die ausdrückliche Einwilligung der betroffenen Person getroffen werden. In Anhang 3 des Gesetzes ist aufgeführt, welche Bedingungen bei der Verarbeitung sensibler personenbezogener Daten erfüllt sein müssen.

---

8 Anhang 1, Teil 2, Absatz 13.

9 Anhang 1, Teil 2, Absatz 15.

Direktmarketing - Werden Daten zum Zwecke des Direktmarketing übermittelt, so muss die betroffene Person die Möglichkeit haben, sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke zu entscheiden.

Das Datenschutzgesetz sieht Bestimmungen für diese Option sowie die zusätzliche Sicherheit vor, dass die betroffene Person das Gericht anrufen kann, wenn der für die Verarbeitung Verantwortliche ihrer Aufforderung nicht nachkommt. Das Gesetz entspricht daher den Anforderungen von WP 12 in diesem Bereich.

Automatisierte Einzelentscheidung - Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Einzelentscheidung im Sinne von Artikel 15 der Richtlinie zu treffen, so muss die natürliche Person das Recht haben, die dieser Entscheidung zugrunde liegende Logik zu erfahren, und andere Maßnahmen müssen getroffen werden, um die berechtigten Interessen der Person zu schützen.

Die Bestimmungen des Datenschutzgesetzes scheinen ausreichend, um den Nachweis der Angemessenheit zu erbringen. Mit der Bereitstellung eines Widerspruchsrechts für die Anwendung automatisierter Einzelentscheidungen zumindest in bestimmten spezifischen Fällen geht das Gesetz über die Anforderungen von WP 12 hinaus. Es ist ebenfalls möglich, im Anschluss an eine getroffene Entscheidung deren Überprüfung vom für die Verarbeitung Verantwortlichen zu verlangen. Außerdem wird verlangt, dass die betroffene Person über die dem System zugrunde liegende Logik informiert wird.

2.2. Verfahrensrechtlicher Mechanismus/Durchsetzungsmechanismus

Nach den WP-12-Grundsätzen sind als Grundlage für die Beurteilung der Angemessenheit des Rechtssystems eines Drittlandes zunächst die Ziele des zugrunde liegenden verfahrensrechtlichen Systems für den Datenschutz zu bestimmen. Darauf aufbauend ist das Spektrum der verschiedenen in diesem Land bestehenden gerichtlichen und außergerichtlichen Verfahrensmechanismen zu bewerten.

Ziel eines Datenschutzsystems ist es, dafür zu sorgen, dass die Datenschutzvorschriften eingehalten werden, betroffene Personen Unterstützung und Hilfe bei der Wahrnehmung ihrer Rechte erhalten und bei einem Verstoß gegen die Bestimmungen angemessen entschädigt werden.

Gewährleistung einer guten Befolgungsrate der Vorschriften bedeutet, dass sich die für die Verarbeitung Verantwortlichen ihrer Pflichten deutlich bewusst sind und dass die betroffenen Personen ihre Rechte und die Mittel zu deren Wahrnehmung gut kennen. Wirksame, abschreckende Sanktionen können erheblich dazu beitragen, dass die Bestimmungen eingehalten werden; gleiches gilt natürlich für Systeme, die eine direkte Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte ermöglichen.

Die Gruppe stellt fest, dass das Datenschutzgesetz von Jersey eine Reihe von Maßnahmen vorsieht, die diesem Ziel dienen.

(a) Datenschutzbeauftragter

Das Datenschutzgesetz von Jersey sieht das Amt eines Datenschutzbeauftragten vor, der vom Parlament (States Assembly) ernannt wird, das aus einer zum Teil gewählten Kammer besteht, die sowohl als Exekutive als auch als Legislative dient. Das Amt hat den gesetzlichen Status einer Rechtspersönlichkeit. Es ist damit zum einen unabhängig von der Regierung und verfügt zum anderen über einen gesetzlichen Status, der weiter besteht, wenn die das Amt führende Person diese Tätigkeit einstellt. Der Datenschutzbeauftragte kann nur von der States Assembly entlassen werden, und die Bedingungen der Ernennung dürfen nicht als Einstellungs- oder Vertretungsvertrag zwischen den States und der ernannten Person ausgelegt werden. Die ernannte Person erhält ihre Bezüge aus den allgemeinen Steuermitteln der States.
Da der Datenschutzbeauftragte von den States, d. h. dem Parlament, ernannt wird und nur von den States entlassen werden kann, besteht kein Zweifel an der Befähigung des Datenschutzbeauftragten, seine Aufgaben in völliger Unabhängigkeit zu erfüllen.
Die Aufgaben und Befugnisse des Datenschutzbeauftragten, die das Einholen von Mitteilungen, die Beurteilung bestimmter Formen der Verarbeitung, Untersuchungsbefugnisse und Durchsetzungsbefugnisse umfassen, sind im Datenschutzgesetz von Jersey geregelt. Weitere Befugnisse sind in Artikel 51 des Gesetzes festgelegt. Die Befugnisse des Datenschutzbeauftragten scheinen eingeschränkter als die Befugnisse in Artikel 28 der Richtlinie. Zur Wahrnehmung seiner Untersuchungsbefugnisse (z. B. mit dem Ziel, Zugang zu Räumlichkeiten zu erhalten und Informationen einzuholen) ist grundsätzlich eine richterliche Anordnung erforderlich. Der für die Verarbeitung Verantwortliche hat allerdings die Möglichkeit, sich dagegen zur Wehr zu setzen. Dadurch wird die Wirksamkeit dieser Maßnahme eingeschränkt, so dass sie für Stichprobenkontrollen und Ad-hoc-Untersuchungen ungeeignet ist.

Aufgrund der Bedenken der Gruppe hinsichtlich der unzureichenden Befugnisse des Datenschutzbeauftragten bestehen gewisse Zweifel daran, dass der Datenschutzbeauftragte ein geeignetes Instrument für die Gewährleistung einer guten Befolgungsrate der Vorschriften darstellt.

(b) Vorhandensein angemessener Durchsetzungsmöglichkeiten und Sanktionen

Das Datenschutzgesetz von Jersey sieht eine Reihe von Sanktionen vor, wenn die für die Verarbeitung Verantwortlichen den gesetzlichen Anforderungen nicht nachkommen. Nach Artikel 17 ist ein Verstoß gegen die Mitteilungspflicht strafbar. Artikel 20 verlangt, dass der für die Verarbeitung Verantwortliche Änderungen an der Art oder dem Zweck der Verarbeitung mitteilen muss.

Unterstützung betroffener Personen bei der Wahrnehmung ihrer Rechte bedeutet, dass der Einzelne seine Rechte rasch und wirksam ohne überhöhte Kosten durchsetzen können muss. Dafür muss es ein Verfahren geben, das eine unabhängige Überprüfung von Beschwerden ermöglicht.

Das Datenschutzgesetz von Jersey bietet in dieser Hinsicht ein angemessenes Schutzniveau. Ohne förmliche Verfassung ist es zwar schwierig, die Unabhängigkeit eines Amtes zu garantieren, es gibt jedoch keine Nachweise über eine politische

Einflussnahme auf die Arbeit des Datenschutzbeauftragten und keinen Hinweis auf Meinungsverschiedenheiten bezüglich der Höhe der bereitgestellten Mittel.

Die Bestimmungen von Artikel 42 des Gesetzes, die einer betroffenen Person ermöglichen, den Datenschutzbeauftragten um eine Prüfung der Rechtmäßigkeit der Verarbeitung zu ersuchen, stellen eine wichtige Ergänzung zu den Rechten dar, die die betroffene Person vor Gericht geltend machen kann. Zusätzlich sieht Artikel 53 Fälle vor, in denen betroffene Personen den Datenschutzbeauftragten um Unterstützung in gerichtlichen Verfahren bitten können. In dieser Hinsicht erfüllt das Gesetz von Jersey die Anforderung, betroffene Personen bei der Wahrnehmung ihrer Rechte zu unterstützen.

Das Datenschutzgesetz hält außerdem am Datenschutzgericht (Data Protection Tribunal) als Berufungsinstanz für Entscheidungen des Datenschutzbeauftragten fest.

Die Gewährleistung einer angemessenen Entschädigung bei Verstoß gegen das Datenschutzgesetz ist ein Schlüsselelement, das eine unabhängige Schieds- oder Schlichtungsinstanz voraussetzt, das die Zahlung von Entschädigungen oder auch die Auferlegung von Sanktionen ermöglicht.

Artikel 13 des Datenschutzgesetzes sieht vor, dass eine Person, die durch einen Verstoß des für die Verarbeitung Verantwortlichen gegen eine der Vorschriften des Gesetzes geschädigt worden ist, Anspruch auf Entschädigung hat. Das Gesetz räumt außerdem Rechte in Bezug auf die Berichtigung, Sperrung und Löschung von unrichtigen Daten ein. Diese Rechte gehen über die eigentlichen Daten hinaus und umfassen jede Meinungsäußerung, die auf den unrichtigen Daten beruht. Sie werden durch Bestimmungen über strafbare Handlungen ergänzt, durch die Personen geschädigt werden können.

Die Gruppe ist der Auffassung, dass das Datenschutzgesetz von Jersey eine angemessene Entschädigung für Personen gewährleistet, die durch eine Verletzung der Datenschutzbestimmungen geschädigt worden sind.

3. ERGEBNIS

Wenn auch gewisse Zweifel bestehen, ob das Datenschutzgesetz von Jersey die Anforderungen vollständig erfüllt, die die Datenschutzrichtlinie den Mitgliedstaaten auferlegt, möchte die Gruppe doch daran erinnern, dass unter Angemessenheit nicht eine vollständige Übereinstimmung mit dem von der Richtlinie festgelegten Schutzniveau zu verstehen ist. Gewisse Bedenken bestehen in Bezug auf die Definition personenbezogener Daten und anderer Konzepte sowie hinsichtlich der Transparenz und der Befugnisse des Datenschutzbeauftragten, aber unter Berücksichtigung der Erläuterungen und Versicherungen der Behörden in Jersey hält die Gruppe diese Bedenken, was den Schutz personenbezogener Daten, die von EU-Mitgliedstaaten nach Jersey übermittelt werden, für nicht erheblich.

Ausgehend von den obigen Feststellungen kommt die Gruppe daher zu dem Schluss, dass Jersey ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 6 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 gewährleistet.

Brüssel, den 9. Oktober 2007

Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR