ARTIKEL-29-DATENSCHUTZGRUPPE

02316-02/09/DE
WP 165

Stellungnahme 6/2009 zum Umfang des Schutzes personenbezogener Daten in Israel

Annahme am 1. Dezember 2009

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

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

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. HINTERGRUND

Am 12. Juli 2007 hat die israelische EU-Mission bei der Kommission den Antrag gestellt, das Verfahren in die Wege zu leiten, damit Israel zu einem Land zu erklärt wird, das im Sinne von Artikel 25 und 26 der Richtlinie ein ausreichendes Datenschutzniveau gewährleistet.

Zur Prüfung der Angemessenheit des israelischen Datenschutzes hat die Kommission bei dem Centre de Recherches Informatique et Droit (nachstehend „CRID" genannt) bei der Universität von Namur einen Bericht in Auftrag gegeben. Das CRID hat in einem sehr ausführlichen Bericht analysiert, inwieweit der israelische Rechtsrahmen die Anforderungen für die Anwendung der Datenschutzbestimmungen für personenbezogene Daten erfüllt, die in dem Arbeitspapier „Übermittlung personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU" niedergelegt sind, das die Artikel-29-Arbeitsgruppe am 24. Juli 1998 angenommen hat (Dokument WP 12).

Die Untergruppe Safe Harbor hat den vorgenannten Bericht und die erste Antwort der israelischen Behörden auf den Bericht in einer Sitzung am 18. März 2009 diskutiert.

In jener Sitzung wurde der Arbeitsgruppe von der Untergruppe ein Brief zur Stellungnahme vorgelegt, den ihr Vorsitzender an die israelischen Behörden gedachte. In diesem Brief wird die in Israel bestehende Regelung zum Datenschutz positiv bewertet; gleichzeitig werden aber auch die Themen hervorgehoben, die einer weiteren Klärung bedürfen.

Am 2. September hat die israelische Rechts-, Informations- und Technologiebehörde (nachstehend „ILITA" genannt) im Namen der israelischen Behörden einen ausführlichen Bericht an die Arbeitsgruppe gesandt, in dem sie zu den Themen Stellung nahmen, die in dem Brief angesprochen worden waren.

Dieser Bericht wurde durch die Mitglieder der Untergruppe analysiert. Er war auch Gegenstand einer Sitzung vom 16. September 2009, in der die vorgenannten Behörden gehört wurden. In dieser Sitzung haben die Mitglieder der Untergruppe die israelischen Behörden, die durch den Leiter der ILITA und den Leiter der Justizabteilung dieser Behörde vertreten waren, zur Klärung der Fragen aufgefordert, die nach der vorangegangenen Erörterung des an die Untergruppe gesandten Berichts weiterer Klärung bedurften.

Die Untergruppe informierte die Arbeitsgruppe in der Sitzung am 12. und 13. Oktober 2009 von den Schlussfolgerungen, zu denen sie während der Sitzung vom 16. September gelangt war, und schlug die Annahme der folgenden Stellungnahme unter den in ihr genannten Bedingungen vor. Die Arbeitsgruppe nahm den Vorschlag an.

2. DATENSCHUTZGESETZE IN ISRAEL

Im Unterschied zu anderen Rechtssystemen und insbesondere zu den Rechtssystemen der Mitgliedstaaten wird das israelische Rechtssystem durch zwei Schlüsselelemente charakterisiert: erstens verfügt Israel nicht über eine geschriebene Verfassung und zweitens beruht das Recht zwar in erster Linie auf dem Common Law, weist aber dennoch Eigenschaften auf, die den Einfluss des Continental Law deutlich machen.

Das Fehlen einer geschriebenen Verfassung wird ausgeglichen durch die sogenannten „Grundgesetze", denen das Oberste Gericht Israels Verfassungsrang gegeben hat. Gleichzeitig haben einige grundlegende Grundsätze und Menschenrechte wie Gleichheit, Redefreiheit und Religionsfreiheit ebenfalls Verfassungsrang.

In diesem Rechtsrahmen ist das Recht auf Privatsphäre in Abschnitt 7 des Grundgesetzes „Menschenwürde und Freiheit" verankert. Dieser Abschnitt legt Folgendes fest:

> *(a) Alle Menschen haben ein Recht auf eine Privat- und Intimsphäre.*
> *(b) Die privaten Räumlichkeiten einer Person dürfen nicht betreten werden, sofern diese nicht zugestimmt hat.*
> *(c) Es dürfen weder private Räumlichkeiten durchsucht werden, noch Personen oder ihre persönliche Habe.*
> *(d) Die Vertraulichkeit von Gesprächen, Niederschriften oder Aufzeichnungen einer Person darf nicht verletzt werden.*

Gleichzeitig wird das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten in dem Privacy Protection Act (Datenschutzgesetz, nachfolgend „PPA" genannt) geregelt. Dieses Gesetz wurde 1981 verabschiedet und bislang neunmal geändert. Die wichtigste Änderung wurde im Jahr 2007 verabschiedet. Sie legte neue Anforderungen an die Verarbeitung personenbezogener Daten fest und regelte die Organisation, die Befugnisse und Funktionen der Kontrollbehörde für den Schutz personenbezogener Daten mit mehr Details und einer größeren Genauigkeit, als es die bestehende Gesetzgebung bis dahin getan hatte. Sie schuf eine Behörde innerhalb des Justizministeriums, nämlich die israelische Rechts-, Informations- und Technologiebehörde (ILITA), der der ehemalige Datenbankbeauftragte angehört.

Darüber hinaus wurde der als „Schoffman-Bericht" bekannte Bericht, der im Januar 2007 von einer vom Justizministerium bestellten Expertengruppe verfasst wurde, angemessen gewürdigt. In diesem Bericht wird eine Reihe von Empfehlungen für eine Änderung der Datenschutzgesetzgebung empfohlen, die derzeit für die Annahme eines neuen Datenschutz-Rechtsrahmen geprüft werden.

Schließlich wird die Datenschutzgesetzgebung im Hinblick auf das geschriebene Gesetz durch einige Beschlüsse der israelischen Regierung vervollständigt, die sich insbesondere auf die Umsetzung des PPA (z. B. bei internationalen Datenübermittlungen) und auf die Organisation und die Arbeitsweise der ILITA beziehen (z. B. in Bezug auf die Dauer des Mandats des Behördenleiters und auf die Gründe für dessen Beendigung).

Darüber hinaus teilt das israelische Rechtssystem, wie oben dargelegt, in großem Umfang Grundsätze des Common Law. Aus diesem Grund müssen Rechtsvorschriften auf jeden Fall durch Gerichtsurteile ergänzt werden, die auf der Grundlage dieser Rechtsvorschriften ergangen sind. Als Präzedenzfälle sind diese Urteile eine direkte israelische Rechtsquelle. Aufgrund des von der Gruppe geforderten Berichts, den die israelischen Behörden erstellt haben sowie aufgrund der Erklärungen der Behörde bei der Anhörung durch die Untergruppe am 16. September 2009 liegt der Arbeitsgruppe eine große Anzahl von Gerichtsbeschlüssen vor, die bei der Beurteilung berücksichtigt werden müssen.

Schließlich muss in dieser ersten Beurteilung darauf hingewiesen werden, dass Israel den internationalen Pakt über bürgerliche und politische Rechte von 1966 ratifiziert hat, auch wenn nach dem israelischen Recht die Ratifizierung eines internationalen Abkommens nicht gleichbedeutend ist mit seiner unmittelbaren Übernahme in das innerstaatliche Recht.

3. BEURTEILUNG DES DATENSCHUTZGESETZES VON ISRAEL IM HINBLICK AUF EINEN ANGEMESSENEN SCHUTZ PERSONENBEZOGENER DATEN

Die Arbeitsgruppe weist darauf hin, dass sich ihre Beurteilung der Angemessenheit des Datenschutzgesetzes in Israel auf das Gesetz Privacy Protection Act (PPA) konzentriert.

Die Bestimmungen dieses Gesetzes sowie die Rechtsprechung der Gerichte in Bezug auf den Schutz personenbezogener Daten wurden unter Berücksichtigung der Stellungnahme WP12 der Arbeitsgruppe mit den wichtigsten Bestimmungen der Richtlinie verglichen. In dieser Stellungnahme wird eine Reihe von Grundsätzen aufgeführt, die *einen „Kern" von „inhaltlichen" Grundsätzen und „verfahrensrechtlichen" bzw. mit der „Durchsetzung im Zusammenhang stehenden" Erfordernissen, deren Einhaltung als Mindestanforderung an eine Situation gilt, in der von einem angemessenen Schutzniveau gesprochen werden kann,* darstellen.

3.1 Anwendungsbereich der Datenschutzverordnungen im israelischen Recht.

Wie bereits manchmal zuvor, ist die Arbeitsgruppe auch hier der Ansicht, dass zuerst der Anwendungsbereich der Datenschutzverordnungen im israelischen Recht untersucht werden sollte, bevor im Besonderen bewertet werden kann, ob die in dem Dokument WP12 niedergelegten Grundsätze eingehalten werden.

a) Konzept personenbezogener Daten oder „Informationen".

Die Arbeitsgruppe hält es insbesondere für erforderlich, das Konzept des Begriffs „personenbezogene Informationen" aus dem PPA zu berücksichtigen und diesen in Verbindung mit dem Konzept der „personenbezogenen Daten" aus der Richtlinie zu setzen. Außerdem muss festgestellt werden, ob das israelische Recht angemessene Garantien für den Datenschutz in Bezug auf jegliche Verarbeitung bietet oder ob das genannte Gesetz nur bei vollständig oder teilweise automatisierten Datenverarbeitungssystemen Anwendung findet. Hierbei wird der durch die Richtlinie festgelegte Datenschutzrechtsrahmen berücksichtigt.

In Bezug auf das erste Thema bestätigt die Arbeitsgruppe, dass die Definition von „Information" gemäß Abschnitt 7 PPA nicht mit der Definition im Sinne der Richtlinie übereinstimmt. Das vorgenannte Gesetz stellt fest, dass *„Information für Daten zur Persönlichkeit, zum Familienstand, zu intimen Angelegenheiten, dem Gesundheitszustand, der*

wirtschaftlichen Stellung, den beruflichen Befähigungen, den Meinungen und Überzeugungen einer Person steht". Die Definition bezieht sich lediglich auf bestimmte Datenkategorien und gibt keine Hinweise darüber, ob Informationen bezüglich einer nicht identifizierten, aber identifizierbaren Person unter dem PPA geschützt wären.

Die Arbeitsgruppe berücksichtigt aber dennoch die Erklärungen, die die israelischen Behörden diesbezüglich abgegeben haben und insbesondere die vorgelegten Präzedenzfälle, die eine Ausweitung des rechtlichen Konzepts der Information implizieren, so dass es dem Konzept der „personenbezogenen Daten" im Sinne der Richtlinie ähnelt.

Diese Schlussfolgerung wird insbesondere angesichts bestimmter Urteile gezogen, wie der Entscheidung des Obersten Gerichts Israels in dem Fall *Israel gegen Bank Ha'Po'alim*, in welcher Folgendes steht: *„der Begriff Information (…) sollte Daten einschließen, die aus einer Datenbank hergeleitet werden können, die nicht nach den individuellen Namen indexiert ist"*.

Als besonders relevant betrachtet die Arbeitsgruppe zusätzlich zu den sonstigen vorgelegten Entscheidungen das Präzedenzurteil *Rani Mor gegen Ynet* des Bezirksgerichts von Haifa, dessen Schlussfolgerungen in Bezug auf IP-Adressen mit denen der Arbeitsgruppe verglichen werden können: *„das Identifizieren eines Online-Nutzers durch Veröffentlichung seiner IP-Adresse ohne vorherige Einwilligung kann ein Delikt wegen Verletzung der Privatsphäre darstellen"*.

Deshalb ist die Arbeitsgruppe in Bezug auf das Konzept der personenbezogenen Daten oder der „Informationen" für den Zweck der Anwendung der Datenschutzverordnung der Ansicht, dass die Präzedenzfälle die Bestimmungen des PPA ergänzt haben. Folglich kann aus dieser Perspektive entschieden werden, dass die Garantien dieses Gesetzes einen schützenden Rechtsrahmen bilden, der in Bezug auf das Konzept der personenbezogenen Daten dem Rechtsrahmen der Richtlinie ähnlich ist.

b) Geschützte Verarbeitungssysteme im israelischen Recht.

An dieser Stelle muss die Arbeitsgruppe auf die besondere Struktur des PPA hinweisen und insbesondere auf die ersten beiden Kapitel: während sich das erste Kapitel auf Verletzungen des Datenschutzes im Allgemeinen bezieht, regelt Kapitel 2 den Datenschutz in Datenbanken.

In Bezug auf das zweite Kapitel definiert Abschnitt 7 eine Datenbank als *„eine Sammlung von Daten, die auf magnetischem oder optischem Trägermaterial gespeichert sind und für die Computerverarbeitung gedacht sind"*. Auf diese Weise finden die Garantien im Sinne von Kapitel 2 nur in den Fällen Anwendung, in denen eine automatisierte Informationsverarbeitung stattfindet und nicht in den Fällen ohne automatisierte Verarbeitung.

Die Arbeitsgruppe nimmt die Erklärungen der israelischen Behörden zur Kenntnis, dass die Bürger gegen eine nichtautomatisierte Datenverarbeitung (oder manuelle Datenverarbeitung) durch die Garantien aus Kapitel 1 PPA geschützt sind, in dem bestimmte Grundsätze wie Zweckbindung, Geheimhaltung und Einwilligung niedergelegt sind.

Dennoch muss daran erinnert werden, dass sich der Schutz, den die Richtlinie für diese Arten der Verarbeitung gewährt, nicht nur auf die genannten Grundsätze bezieht, sondern auf die Gesamtheit des Systems und insbesondere auf die Grundsätze, die in dem Dokument WP12 aufgeführt sind. Damit das Datenschutzniveau eines bestimmten Staates in Bezug auf nichtautomatisierte Verarbeitungssysteme als ausreichend eingestuft werden kann, muss das innerstaatliche Recht dieses Staates folglich die vorgenannten Grundsätze zumindest für diese Verarbeitungssysteme anerkennen.

Aus diesem Grund kann die israelische Gesetzgebung nicht als angemessen in Bezug auf nichtautomatisierte oder manuelle Verarbeitungssysteme angesehen werden, da Kapitel 1 nicht alle der vorgenannten Grundsätze umfasst. Diesbezüglich möchte die Arbeitsgruppe darauf hinweisen, dass der „Schoffman-Bericht“ zu demselben Ergebnis kam und eine Reform des in Israel geltenden Rechtsrahmens vorschlug, in der die Gesamtheit der Datenschutzgarantien auf manuelle Verarbeitungssysteme ausgeweitet werden sollte.

Folglich ist die Arbeitsgruppe der Ansicht, dass die Analyse der Angemessenheit des Datenschutzsystems in Israel nicht die nichtautomatisierte Datenverarbeitung miteinbeziehen kann, da der genannte Rechtsrahmen die in Dokument WP12 vorgesehenen Garantien nicht gewährt.

Die Arbeitsgruppe möchte diesbezüglich auch klarstellen, dass sie der Ansicht ist, die Angemessenheitsanalyse in Bezug auf vollständig oder teilweise automatisierte Verarbeitungssysteme fortführen zu können. Deshalb sollten die internationalen Datenübermittlungen nach Israel, die durch automatisierte Systeme erfolgen und selbst diejenigen Datenübermittlungen, die zwar nicht durch automatisierte Verarbeitungssysteme erfolgt sind, aber in Israel durch automatisierte Systeme bearbeitet werden, nicht von der Angemessenheitsprüfung ausgeschlossen werden, die im Folgenden durchgeführt wird.

Folglich werden nur die internationalen Datenübermittlungen, bei denen sowohl die Übermittlung als auch die weitere Datenverarbeitung ausschließlich durch nichtautomatisierte Systeme erfolgt, von der Beurteilung ausgeschlossen, denn nur in diesen Fällen finden die Bestimmungen von Kapitel 1 PPA keine Anwendung.

Die Arbeitsgruppe ist sich der Tatsache bewusst, dass der Umfang der von der Angemessenheitsbeurteilung ausgeschlossenen Übermittlungen nur gering ist und sich nicht in großem Maße auf die abschließende Anwendung der möglicherweise getroffenen Entscheidung auswirken wird. Sie ist jedoch der Ansicht, dass es angesichts der Bestimmungen der Richtlinie von essentieller Bedeutung ist, die genannte Ausnahme zu machen. Gleichzeitig empfiehlt sie den Erlass von Vorschriften, damit in Zukunft zu erlassende Gesetze auch auf manuelle Datenbanken Anwendung finden. Dies gilt insbesondere für diejenigen Gesetze, die mit der Umsetzung des „Schoffman-Berichts“ in Verbindung stehen. Denn dann kann die Beurteilung, sofern anwendbar, auf diese Verarbeitungssysteme ausgedehnt werden.

3.2. Inhaltliche Grundsätze

Unter Berücksichtigung der vorgenannten Feststellungen wird nun die Beurteilung des Datenschutzniveaus in Israel angesichts der in Dokument WP12 aufgeführten Grundsätze vorgenommen. Begonnen wird mit einer Prüfung der aufgeführten Grundsätze, die die Gesetzgebung des Staates Israel berücksichtigen sollte.

a) Unbedingt zu berücksichtigende Grundsätze

> **1) Der Grundsatz der Beschränkung der Zweckbestimmung:** Daten sollten für einen spezifischen Zweck verarbeitet und dementsprechend nur verwendet und weiter übermittelt werden, soweit dies mit der Zweckbestimmung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft notwendigen Fälle aus einem der in Artikel 13 der Richtlinie aufgeführten Gründe.

Die Arbeitsgruppe ist der Auffassung, dass die israelische Gesetzgebung diesem Grundsatz Rechnung trägt. So legt Artikel 2 Absatz 9 PPA in allgemeinen Worten fest, dass *„die Verwendung von Informationen über die Privatangelegenheiten einer Person oder deren Übermittlung an einen Dritten für einen anderen Zweck, als den für den die Informationen erteilt wurden“* eine Verletzung der Privatsphäre darstellt.

Dieser allgemeine Grundsatz wird durch Artikel 8 Buchstabe b des vorgenannten Gesetzes noch verstärkt. Dieser legt Folgendes fest: *„Eine Person darf die Informationen in einer Datenbank, die gemäß diesem Abschnitt einer Registrierung bedarf, nur für den Zweck verwenden, für den die Datenbank eingerichtet wurde“*.

Darüber hinaus legt Artikel 9 Buchstabe b Satz 2 PPA in Bezug auf die Fälle, in denen die Datenbank bei der Kontrollbehörde registriert wurde, fest, dass der Antrag *„die Zwecke“* umfassen muss, *„für die die Datenbank eingerichtet wurde und die Zwecke, für die die Informationen verwendet werden sollen“*.

Schließlich bestätigt die Arbeitsgruppe, dass die Gerichte diese Bestimmungen auf ähnliche Weise ausgelegt haben, wie dies von der Richtlinie vorgesehen ist. Die Arbeitsgruppe berücksichtigt insbesondere das Verbot der nicht vereinbarbaren Nutzung von Finanzdaten, auf das sich das Oberste Gericht Israels in dem Fall *Datenbankbeauftragter gegen Ventura* beruft.

> **2) Der Grundsatz der Datenqualität und -verhältnismäßigkeit:** Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand gehalten werden. Die Daten sollen angemessen und relevant sein und nicht über den Zweck hinausgehen, für den sie übermittelt oder weiterverarbeitet werden.

Wird der Grundsatz der Datenqualität eng ausgelegt, ist die Arbeitsgruppe der Ansicht, dass die Verpflichtung, die Daten sachlich richtig, und wenn nötig, auf dem neuesten Stand zu halten von dem israelischen Gesetz durch die Bestimmungen zum Berichtigungsrecht eingehalten wird, auf das sich Abschnitt 14 PPA bezieht, auch wenn der Grundsatz der Datenqualität nicht als unabhängiger Grundsatz aufgeführt wird.

So erklärt Unterabschnitt a des vorgenannten Abschnitts, dass *„eine Person, die bei der Prüfung der sie betreffenden Informationen feststellt, dass diese sachlich nicht richtig, unvollständig, unklar oder nicht auf dem neuesten Stand sind, den Eigentümer der Datenbank oder wenn dieser nicht ansässig ist, den Besitzer der Datenbank dazu auffordern kann, die Informationen zu ändern oder zu löschen“*.

Die Unterabschnitte b und c beziehen sich auf die Entscheidung des Eigentümers der Datenbank. *„Wenn der Eigentümer einer Datenbank einer Aufforderung gemäß Unterabschnitt a zustimmt, führt er die erforderlichen Änderungen an den Informationen durch und teilt diese Änderungen allen Personen, die die Informationen von ihm erhalten haben, innerhalb der in den Bestimmungen festgelegten Frist mit“*.

Im Falle seiner Weigerung ist er dazu verpflichtet, dies der betroffenen Person unter Hinzufügung von Abschnitt 15 mitzuteilen *„Eine Person, die Informationen beantragt, kann in der in den Bestimmungen festgelegten Art und Weise gemäß Abschnitt 13 oder Abschnitt 13A gegen die Weigerung des Eigentümers einer Datenbank, eine Prüfung zu ermöglichen und gemäß Abschnitt 14 Buchstabe c gegen die Mitteilung der Weigerung Beschwerde beim Amtsgericht einlegen“*.

In Bezug auf den Grundsatz der Verhältnismäßigkeit, der aus Artikel 6 Absatz 1 Buchstabe c der Richtlinie abgeleitet wird, bestätigt die Arbeitsgruppe, dass dieser Grundsatz nicht ausdrücklich in der PPA anerkannt wird. Dennoch hat die Arbeitsgruppe von den israelischen Behörden mit Befriedigung Erklärungen und Präzedenzfälle entgegengenommen, die sich auf dieses Thema beziehen und die den genannten Mangel in großem Maße ausgleichen.

So betrachtet die Arbeitsgruppe die Klarstellungen als zufriedenstellend, die in Bezug auf den verfassungsrechtlichen Geltungsbereich des Grundsatzes der Verhältnismäßigkeit bei der Verarbeitung im öffentlichen Sektor gegeben wurden. Hier sieht sie das aus dem Präzedenzurteil des Obersten Gerichts in dem Fall *Acri gegen Innenminister* abgeleitete Recht als besonderes relevant an. Das Urteil wurde von den israelischen Behörden vorgelegt. Hier liegt ein ausdrücklicher Bezug zu einer Anwendung des Grundsatzes der Verhältnismäßigkeit im Sinne der Richtlinie vor.

Die Arbeitsgruppe begrüßt gleichermaßen die Klarstellungen der israelischen Behörden in Bezug auf die gesetzliche Anforderung der Verhältnismäßigkeit bei der Verarbeitung, die sich auf die Grundsätze der Angemessenheit der Maßnahme und des Guten Glaubens stützen. In diesem Zusammenhang betrachtet die Gruppe den Präzedenzfall *Eisner gegen Richmond* als besonders interessant. In dieser Entscheidung des Arbeitsgerichts von Tel Aviv wurde die Verwendung von Videokameras am Arbeitsplatz und durch Dritte eingeschränkt. Die Arbeitsgruppe sieht auch die Anwendung des Grundsatzes der Verhältnismäßigkeit im Verbraucherschutz als relevant an sowie die Gerichtsentscheidungen der zuständigen Gerichte, insbesondere des Gerichts für Standardverträge in Jerusalem, die Klauseln für ungültig erklärt haben, die den Austausch von Informationen innerhalb einer Gruppe von Handelskonzernen erlaubt haben, wie z. B. in der Rechtssache *Bank of Israel gegen First International Bank of Israel*.

Angesichts dieser Rechtsprechung ist die Arbeitsgruppe der Ansicht, dass der Grundsatz der Verhältnismäßigkeit in den meisten Fällen garantiert ist, in denen eine unverhältnismäßige Verarbeitung von personenbezogenen Daten möglich wäre. Sie glaubt insbesondere, dass der Grundsatz der Verhältnismäßigkeit ein verfassungsmäßiger Grundsatz ist, der in jedem Fall der Datenverarbeitung im öffentlichen oder privaten Sektor bei der Ausübung öffentlicher Aufgaben erfüllt werden muss.

Dennoch würde es die Arbeitsgruppe zufriedenstellender finden, wenn die israelische Gesetzgebung diesen Grundsatz ausdrücklich beinhalten würde. Als Ziel wird die Garantie angestrebt, dass Tätigkeiten im privaten Sektor, für die es noch keine Gerichtsentscheidungen

auf der Grundlage der Grundsätze der Angemessenheit und des Guten Glaubens gibt, in Zukunft auf Probleme bei der Auslegung reagieren können, die einen angemessenen Schutz der Rechte der betroffenen Personen behindern könnten. Die Arbeitsgruppe erinnert daran, dass die Aufnahme dieses Grundsatzes in das PPA eine der Schlussfolgerungen des „Schoffman-Berichts“ ist.

Ohne dass die vorgenannte Schlussfolgerung die abschließende Beurteilung des Schutzniveaus im Staat Israel beeinträchtigt, ist die Arbeitsgruppe der Ansicht, dass die zukünftigen Entwicklungen in der Rechtsetzung, insbesondere in Bezug auf die Umsetzung des „Schoffman-Berichts“, die Bestimmungen erfüllen sollten, welche die ausdrückliche Anwendung des Grundsatzes der Verhältnismäßigkeit für die Verarbeitung aller personenbezogener Daten im öffentlichen und privaten Sektor vorsehen.

> **3) Der Grundsatz der Transparenz:** natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2 und 13 der Richtlinie möglich.

Die Arbeitsgruppe ist der Ansicht, dass die Gesetzgebung in Israel dem Grundsatz in ausreichendem Umfang gerecht wird.

Abschnitt 11 PPA legt Folgendes fest:

> *„Einer Anfrage an eine Person zum Erhalt von Informationen, die in einer Datenbank gespeichert und verwendet werden sollen, muss eine Mitteilung beigefügt werden, die folgende Angaben enthält:*
> *(1) ob die Person gesetzlich dazu verpflichtet ist, die Informationen zu erteilen oder ob dies vom Willen und der Einwilligung der Person abhängt;*
> *(2) den Zweck, für den die Informationen eingeholt werden sollen;*
> *(3) der Empfänger der Informationen und der Zweck dieser Übermittlung.“*

Darüber hinaus legt Abschnitt 13A Absatz 1 PPA Folgendes fest: *„Der Eigentümer einer Datenbank, der diese am Sitz einer anderen Person (in diesem Abschnitt - der Besitzer) unterhält, ist dazu verpflichtet, die antragstellende Person unter Angabe der Adresse an den Besitzer zu verweisen und den Besitzer in Schriftform dazu aufzufordern, der antragstellenden Person die Prüfung zu ermöglichen“*. Entsprechend legt Unterabschnitt 2 Folgendes fest: *„Wenn sich der Antragsteller zuerst an den Besitzer wendet, ist dieser dazu verpflichtet, dem Antragsteller mitzuteilen, ob er Informationen über ihn besitzt und ihm darüber hinaus den Namen und die Anschrift des Eigentümers der Datenbank mitzuteilen“*.

> **4) Der Grundsatz der Sicherheit:** Der für die Verarbeitung Verantwortliche hat geeignete, den mit der Verarbeitung verbundenen Risiken entsprechende technische und organisatorische Sicherheitsmaßnahmen zu treffen. 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 Arbeitsgruppe ist der Ansicht, dass der Staat Israel diesen Grundsatz garantiert. Sie berücksichtigt insbesondere die Bestimmungen der Abschnitte 16, 17, 17A und 17B PPA.

Abschnitt 7 definiert „Sicherheit der Informationen“ als den *„Schutz der Informationsintegrität oder den Schutz der Information vor Offenlegung, Nutzung oder dem Anfertigen von Kopien ohne rechtmäßige Genehmigung“* und Abschnitt 17 fügt hinzu, dass *„sowohl der Eigentümer als auch der Besitzer und der Manager einer Datenbank für die Sicherheit der Informationen in der Datenbank verantwortlich ist“*.

Artikel 17B legt ausdrücklich fest, dass bestimmte Eigentümer einer Datenbank oder deren Auftragsverarbeiter einen Sicherheitsbeauftragten mit den entsprechenden Qualifikationen ernennen müssen, der für die Einhaltung der Sicherheitsbestimmungen verantwortlich ist.

Darüber hinaus regelt Artikel 16 die Verpflichtung zur Vertraulichkeit bei der Verarbeitung von Informationen und legt Folgendes fest: *„Niemand darf Informationen offenlegen, in deren Kenntnis er aufgrund seiner Funktion als Angestellter, Manager oder Besitzer einer Datenbank gelangt ist, es sei denn, er tut dies in Ausübung seiner Tätigkeit oder zur Umsetzung eines Gesetzes oder eines Gerichtsbeschlusses, der in einem Gerichtsverfahren ergeht. Wenn der Antrag vor Klageeinreichung gestellt wird, wird er vor dem Amtsgericht verhandelt“*. Ein Verstoß gegen diese Verpflichtung kann mit bis zu fünf Jahren Gefängnis bestraft werden.

Artikel 17A schließlich bezieht sich auf den Auftragsverarbeiter und legt Folgendes fest:

> *„(a) Eine Person, die sich im Besitz von Datenbanken verschiedener Eigentümer befindet, muss sicherstellen, dass der Zugang zu den einzelnen Datenbanken nur den Personen möglich ist, die aufgrund einer schriftlichen Vereinbarung zwischen der Person und dem Eigentümer der jeweiligen Datenbank ausdrücklich dazu befugt sind.*
> *(b) Eine Person, die sich im Besitz von mindestens fünf Datenbanken befindet, die gemäß Abschnitt 8 registriert werden müssen, muss dem Datenbankbeauftragten jährlich eine Liste der Datenbanken in ihrem Besitz vorlegen. Auf dieser Liste müssen die Namen der jeweiligen Datenbankeigentümer angeben werden sowie die Personen, die aufgrund eines Abkommens mit dem Eigentümer Zugang zu den Datenbanken haben und eine diesbezügliche eidesstattliche Erklärung sowie der Name des Sicherheitsbeauftragten gemäß Abschnitt 17B“*.
>
> 5) **Das Recht auf Zugriff, Berichtigung und Widerspruch:** Die betroffene Person hat das Recht, 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.

Abschnitt 13 a PPA legt fest, dass *„jede Person das Recht hat, entweder selbst oder durch einen Vertreter, den sie schriftlich dazu bevollmächtigt hat, alle Informationen zu prüfen, die über sie in einer Datenbank gespeichert sind. Hierzu ist auch der Vormund befugt“*. Abschnitt 13 b bestimmt, dass *„der Eigentümer einer Datenbank die Prüfung der Informationen, die eine der unter Unterabschnitt (a) genannten Person (nachstehend „den Antrag stellende Person“ genannt) beantragt, in der hebräischen, arabischen oder englischen Sprache ermöglicht“*.

In Bezug auf das Recht auf Berichtigung, legt der vorstehend bereits analysierte Abschnitt 14 a PPA Folgendes fest: *„Eine Person, die bei der Prüfung der sie betreffenden Informationen feststellt, dass diese sachlich nicht korrekt, unvollständig, unklar oder nicht auf dem neuesten Stand sind, kann den Eigentümer der Datenbank oder, wenn dieser nicht ansässig ist, den Besitzer derselben dazu auffordern, die Informationen zu ändern oder zu löschen“*.

Eine Nichterfüllung der Verpflichtungen, die dem für die Datenverarbeitung Verantwortlichen durch diese Abschnitte auferlegt werden, stellt gemäß Artikel 31 eine Straftat dar und kann gemäß Abschnitt 31B auch zu einer zivilrechtlichen Haftung gegenüber der betroffenen Person führen. Diese Abschnitte werden in einem nachfolgenden Teil der vorliegenden Stellungnahme näher untersucht.

Abschnitt 17F PPA sieht das Widerspruchsrecht in Fällen des Direktmarketing ausdrücklich vor. Dies wird nachfolgend gezeigt.

Nachdem dies aufgezeigt wurde, stellt die Arbeitsgruppe fest, dass die israelische Gesetzgebung dieses Recht nicht in einer allgemeinen Klausel festlegt. Die Arbeitsgruppe berücksichtigt jedoch, dass Daten gemäß PPA nur für einen eingeschränkten Zweck (Abschnitt 8 b und Abschnitt 2 Absatz 9) genutzt werden dürfen, über den die betroffene Person unterrichtet wurde (Abschnitt 11). Die Arbeitsgruppe vertritt folglich die Ansicht, dass die betroffene Person der Verarbeitung von Daten widersprechen kann, weil diese über die Zwecke hinausgeht, für die die Daten erhoben wurden oder weil die betroffene Person nicht ordnungsgemäß darüber informiert wurde. In einem solchen Fall wird die exzessive Verarbeitung als Verletzung der Privatsphäre gemäß Abschnitt 2 Absatz 9 PPA, als strafbare Handlung gemäß Abschnitt 31Aa Absatz 1 und als betrügerisches Vorgehen in Bezug auf die Pflicht zur Benachrichtigung gesehen, was gemäß Abschnitt 31A a Satz 3 als strafbare Handlung gilt.

Abschnitt 15 PPA legt darüber hinaus Folgendes fest: *„Eine Person, die Informationen beantragt, kann in der in den Bestimmungen festgelegten Art und Weise gemäß Abschnitt 13 oder Abschnitt 13A gegen die Weigerung des Eigentümers einer Datenbank, eine Prüfung zu ermöglichen und gemäß Abschnitt 14 Buchstabe c gegen die Mitteilung der Weigerung Beschwerde beim Amtsgericht einlegen“*.

Schließlich ist die Arbeitsgruppe davon überzeugt, dass die Ausnahmen zur Ausübung des Auskunftsrechts und folglich des Widerspruchsrechts aus Abschnitt 13 c PPA mit den Ausnahmen aus Artikel 13 der Richtlinie für die Mitgliedstaaten übereinstimmen. In diesem Sinne bewertet die Arbeitsgruppe die Rechtsprechung der Gerichte in Bezug auf die Ausübung der vorgenannten Rechte positiv und hier insbesondere das Urteil des Obersten Gerichts in dem Fall *Fischler gegen Leiter der Polizeibehörde*, in welchem der betroffenen Person das Recht zugesprochen wurde, Kenntnis über die sie betreffenden Informationen aus den Polizeiakten zu erlangen.

Deshalb vertritt die Arbeitsgruppe die Ansicht, dass die Gesetzgebung des Staates Israel die Rechte der betroffenen Personen auf Zugang zu ihren Daten, auf Berichtigung oder auf Widerspruch gegen die Verarbeitung der Daten gemäß den Anforderungen von WP12 ausreichend garantiert.

6) Beschränkungen der Weiterübermittlung in andere Drittländer: Weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland sind lediglich zulässig, 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. (Diese Ausnahmen werden in Kapitel 5 untersucht).

Die Arbeitsgruppe berücksichtigt zur Beurteilung der Einhaltung dieses Grundsatzes die Bestimmungen der Datenschutzverordnungen (Übermittlung von Datenbanken ins Ausland), die die Regierung von Israel am 17. Juni 2001 erlassen hat.

Die Verordnungen verbieten die Übermittlung von Daten an Drittländer, sofern diese Länder nicht ein Datenschutzniveau bieten, das mindestens dem Datenschutzniveau nach israelischem Recht entspricht und ausdrücklich einige grundlegende Grundsätze wie die rechtmäßige und gesetzliche Erhebung und Verarbeitung von Daten, die Zweckbindung, die Datenqualität (sachliche Richtigkeit und das Halten der Daten auf dem neuesten Stand), die Einhaltung des Informationsrechts (und gemäß dem israelischen Recht daraus folgend das Berichtigungsrecht) und die Datensicherheit aufführt.

Verordnung 2 Absatz 8 legt mehrere Fälle fest, bei denen eine gesetzliche Vermutung der Angemessenheit vorliegt. Darunter fallen einschließlich der Mitgliedstaaten die Länder, die die Konvention 108 des Europarates unterzeichnet haben sowie diejenigen, von denen *„der Datenbankbeauftragte mitgeteilt hat, dass mit der Datenschutzbehörde des Drittlandes eine Vereinbarung getroffen wurde“*.

Die Absätze 1 bis 7 der Verordnung 2 legen einige Ausnahmen zu diesen allgemeinen Bestimmungen fest:

- *„wenn die betroffene Person eingewilligt hat;*
- *wenn es nicht möglich ist, die Einwilligung einzuholen, die Datenübermittlung aber für den Schutz der Gesundheit der betroffenen Person entscheidend ist;*
- *wenn die Daten an eine [ausländische] Gesellschaft übermittelt werden, die sich im Besitz des Eigentümers der [lokalen] Datenbank befindet und dieser den Datenschutz garantiert hat;*
- *wenn der Empfänger der Daten sich dazu verpflichtet hat, für ein Datenschutzniveau zu sorgen, als ob die Daten in Israel gespeichert würden;*
- *wenn die Daten der Öffentlichkeit aufgrund einer gesetzlichen Genehmigung zugänglich sind;*
- *wenn die Datenübermittlung für den Schutz der öffentlichen Ordnung oder Sicherheit entscheidend ist;*
- *wenn die Datenübermittlung durch das israelische Gesetz gefordert wird“*.

Verordnung 3 legt den Grundsatz der Rechenschaftspflicht fest und schreibt vor, dass die die Daten übermittelnde Partei von dem Empfänger der Daten eine Garantie einholen muss, dass ausreichend Maßnahmen zum Schutz der Daten ergriffen werden und sie nicht weiter übermittelt werden.

Die Arbeitsgruppe vertritt die Ansicht, dass die dargelegten Bestimmungen dem Grundsatz der Beschränkung der Weiterübermittlung in andere Drittländer entsprechen und dass die diesbezüglichen, durch die israelische Gesetzgebung gegebenen Garantien eine angemessene

Einhaltung der Rechte der Bürger der Europäischen Union gewährleisten, deren Daten in Israel verarbeitet werden.

Dennoch erinnert die Arbeitsgruppe an die Kriterien für Ausnahmen gemäß Artikel 26 Absatz 1 der Richtlinie, die auch in dem *„Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995“* (Dokument WP114) aufgeführt sind und drängt die israelischen Behörden, Auslegungen der in der vorgenannten Verordnung 2 aufgeführten Ausnahmen in Übereinstimmung mit dem vorgenannten Dokument und der Richtlinie selbst vorzunehmen.

b) Weitere Grundsätze

Dokument WP12 verweist auf bestimmte Grundsätze, die in Bezug auf besondere Verarbeitungssysteme angewendet werden müssen. Es werden die Wichtigsten genannt:

> **1) 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.

Abschnitt 7 PPA enthält das Konzept der „sensiblen Daten“ und definiert diese wie folgt:

> *„(1) Daten zur Persönlichkeit, zu intimen Angelegenheiten, dem Gesundheitszustand, der wirtschaftlichen Stellung, den Meinungen und Überzeugungen einer Person;*
> *(2) Informationen, die der Justizminister mit der Zustimmung des Verfassungs- und Rechtsausschusses der Knesset als sensible Informationen definiert hat“*.

Die Arbeitsgruppe vertritt die Ansicht, dass die vorgenannte Liste, auch wenn sie nicht vollumfänglich mit der in Artikel 8 der Richtlinie erstellten Liste übereinstimmt, doch als ähnlich eingestuft werden kann. Sie erkennt insbesondere, dass Informationen, die sich auf Meinungen und Überzeugungen beziehen, viele der Daten umfassen, die in Artikel 8 der Richtlinie genannt werden. Darüber hinaus drängt die Arbeitsgruppe die israelischen Behörden, solche Informationen als sensible Daten anzuerkennen, die in Artikel 8 der Richtlinie aufgeführt sind und bei den in der PPA vorgesehenen Kategorien unter die Gruppe „intime Angelegenheiten“ eingeordnet werden können. Hier geht es insbesondere um Daten zur ethnischen Herkunft und zu den sexuellen Präferenzen.

Die Arbeitsgruppe stellt auch fest, dass Daten im Allgemeinen nur mit der vorherigen Einwilligung der betroffenen Person eingeholt werden dürfen. Diese Einwilligung kann nach Abschnitt 3 PPA sowohl ausdrücklich als auch implizit erfolgen. Das Erfordernis von Artikel 8 der Richtlinie wird nicht vollständig erfüllt, da Artikel 8 eine ausdrückliche Einwilligung fordert.

Diese mögliche Kluft wird jedoch durch den erwähnten Abschnitt 3 überbrückt, der fordert, dass die Einwilligung auf jeden Fall in Kenntnis der Sachlage erfolgen muss. Die Arbeitsgruppe ist der Ansicht, dass die Verarbeitung solcher Daten nur als Folge einer Handlung der betroffenen Person erfolgen kann und nicht aufgrund einer stillschweigenden Einwilligung, wenn die betroffene Person eindeutig in Kenntnis der Sachlage ist, weil ihr die in Bezug auf den Grundsatz der Transparenz verwendeten Begriffe erklärt wurden.

Aus diesem Grund geht die Arbeitsgruppe davon aus, dass selbst wenn die Verarbeitung aufgrund einer stillschweigenden Einwilligung erfolgen kann, dennoch eine vorherige Handlung durch den für die Datenverarbeitung Verantwortlichen erforderlich ist, mit der die betroffene Person über alle Folgen informiert wird, die ihre Einwilligung nach sich zieht.

Obwohl es keine Vorschrift gibt, die der in der Richtlinie vorgesehenen gleicht, ist die Arbeitsgruppe dennoch der Ansicht, dass die israelische Gesetzgebung diesen Grundsatz angemessen erfüllt.

> **2) 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.

Die Arbeitsgruppe stellt mit Befriedigung fest, dass dieser Grundsatz eindeutig durch die israelische Gesetzgebung geregelt ist, denn das PPA enthält in Kapitel 2 einen Teil, der sich ausdrücklich auf das „Direktmailing" bezieht und es definiert als *„persönliche Kontaktaufnahme mit einer Person, da diese zu einer Bevölkerungsgruppe zählt, die durch eine oder mehrere Charakteristika unter Personen ermittelt wurde, deren Namen in einer Datenbank gespeichert sind"*.

Die israelische Gesetzgebung sieht bestimmte Verpflichtungen bei der Verarbeitung der vorgenannten Daten vor. Insbesondere müssen die für die Datenverarbeitung Verantwortlichen die Datei bei der Kontrollbehörde registrieren und ein Register der Quellen führen, von denen sie die Daten erhalten haben. Darüber hinaus müssen in allen Sendungen an die betroffenen Personen bestimmte Informationen enthalten sein.

Die Arbeitsgruppe ist der Ansicht, dass der Grundsatz durch die Unterabschnitte b und e des Abschnitts 17F PPA erfüllt ist. Diese legen Folgendes fest:

> *„(b) Jedermann ist dazu befugt, den Eigentümer der Datenbank, die für das Direktmailing genutzt wird, in Schriftform dazu aufzufordern, die ihn betreffenden Informationen aus der Datenbank zu löschen.*
> *(c) Jedermann ist dazu befugt, den Eigentümer der Datenbank, die für Direktmailing-Dienste genutzt wird oder den Eigentümer der Datenbank, in der die Informationen gespeichert sind, aufgrund derer der Kontakt hergestellt wurde, in Schriftform dazu aufzufordern, die ihn betreffenden Informationen für einen begrenzten Zeitraum oder von Dauer nicht an eine Person, eine Kategorie von Personen oder bestimmte Personen zu senden.*
> *(d) Wenn eine Person dem Eigentümer der Datenbank eine Forderung gemäß Unterabschnitt b oder c übermittelt hat, handelt der Eigentümer der Datenbank entsprechend und teilt der Person dann mit, dass er ihre Forderungen erfüllt hat.*
> *(e) Wenn der Eigentümer der Datenbank die Mitteilung im Sinne von Unterabschnitt d nicht innerhalb von 30 Tagen ab Erhalt der Forderung gemacht hat, ist die Person, auf die sich die Informationen beziehen, dazu befugt, das Amtsgericht auf die vorgeschriebene Weise anzurufen, damit der Eigentümer der Datenbank angewiesen wird, entsprechend den Bestimmungen zu handeln"*.

> **3) 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 Arbeitsgruppe stellt fest, dass die israelische Gesetzgebung keine ausdrückliche Vorschrift in Bezug auf diesen Grundsatz enthält. Die Arbeitsgruppe hat jedoch mit Befriedigung die Stellungnahmen in dem Bericht des CRID und die Klarstellungen der israelischen Behörden entgegen genommen, in denen erklärt wird, dass das israelische Gesetz es den betroffenen Personen in jedem Fall ermöglicht, dieser Art von Entscheidungen zu widersprechen.

Die Arbeitsgruppe sieht diesen Grundsatz zwar derzeit als erfüllt an, drängt die israelischen Behörden aber dennoch dazu, den Grundsatz in ähnlichen Worten wie in Artikel 15 der Richtlinie in allen zukünftigen ordnungspolitischen Maßnahmen in dieser Angelegenheit ausdrücklich aufzuführen.

3.3. Verfahrensrechtliche Mechanismen/Durchsetzungsmechanismen

Nach der Stellungnahme der Arbeitsgruppe WP12 „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“ sind als Grundlage für die Beurteilung der Angemessenheit des Rechtssystem 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.

Diesbezüglich verfolgt ein Datenschutzsystem im Wesentlichen drei Ziele:

- Gewährleistung einer guten Befolgungsrate der Vorschriften,
- Unterstützung und Hilfe für einzelne betroffene Personen bei der Wahrnehmung ihrer Rechte,
- Gewährung einer angemessenen Entschädigung für die geschädigte Partei bei einem Verstoß gegen die Bestimmungen.

a) Gewährleistung einer guten Befolgungsrate der Vorschriften: Ein gutes System ist üblicherweise dadurch gekennzeichnet, 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 israelische Rechts-, Informations- und Technologiebehörde (ILITA).

In Übereinstimmung mit Abschnitt 7 PPA wurde das Amt des Datenbankbeauftragten geschaffen: *„Der Datenbankbeauftragte ist eine Person, welche die Qualifikationen für das Amt eines Amtsrichters hat und durch die Regierung mittels Mitteilung im Reshumot damit beauftragt wurde, ein wie in Abschnitt 12 beschriebenes „Register der Datenbanken“ zu unterhalten (nachstehend „das Register“ genannt“)“.*

Durch eine Entscheidung der israelischen Regierung aus dem Jahr 2006 wurde das Amt des Datenbankbeauftragten kürzlich der ILITA angegliedert. Aufgrund der vorgenannten

Entscheidung ist der für die Datenverarbeitung Verantwortliche des Datenbankregisters jetzt der Leiter der ILITA. Darüber hinaus gehören auch der Beauftragte der Zertifizierungsstelle sowie der Beauftragte der Abteilung Kreditdaten der ILITA an.

Die Durchsetzungsmöglichkeiten der ILITA werden durch Abschnitt 10 PPA geregelt. In Übereinstimmung mit oben Stehendem ist es der Arbeitsgruppe bewusst, dass diese Möglichkeiten, die per Gesetz dem Datenbankbeauftragten zustehen, der ILITA zukommen, der der Datenbankbeauftragte angegliedert wurde.

Das PPA räumt der ILITA insbesondere die Befugnis ein, die Verarbeitung unter den nachgenannten Bedingungen aufzuzeichnen und zu prüfen.

Die Arbeitsgruppe notiert die Änderungen, die die Staatsregierung kürzlich in Bezug auf die Ernennung und Entlassung des Leiters der ILITA umgesetzt hat. Die Arbeitsgruppe ist der Ansicht, dass die Änderungen dem Leiter und damit der genannten Behörde ein angemessenes Maß an Unabhängigkeit für die Zwecke einräumen, die für die der Richtlinie unterliegenden Kontrollbehörden festgesetzt wurden. Die Arbeitsgruppe berücksichtigt insbesondere, dass das Profil der bei ILITA arbeitenden Personen und ihres Leiters das von Beamten ist und nicht das von politischen Mandatsträgern.

Die Arbeitsgruppe merkt diesbezüglich an, dass gemäß der Regierungsentscheidung 4460 (HC/915) vom 8. Januar 2006 die Ernennung des Leiters der ILITA als hochrangigem Beamten vorher durch einen unabhängigen Ausschuss bewertet werden muss. Dieser Ausschuss setzt sich auf fünf Mitgliedern zusammen. Das sind Vertreter der öffentlichen Hand, der Akademie und der kontrollierten juristischen Personen, welche die Bedingungen festlegen, die der ernannte Amtsträger erfüllen muss und die Ernennung einer ausgewählten Person vorschlagen.

Darüber hinaus hat die Arbeitsgruppe mit Befriedigung festgestellt, dass nach der Regierungsentscheidung Nr. 4470 vom 8. Februar 2009 die Amtszeit des Leiters von ILITA auf sechs Jahre festgesetzt wurde. Er kann nur unter bestimmten Umständen durch einen speziellen Beamtenausschuss abgesetzt werden, dem ein ehemaliger Richter vorsitzt. Diese Vorgehensweise ähnelt derjenigen, die in Israel unter anderem für den Wettbewerbskommissar, den Leiter der Regelungsbehörde Kapitalmärkte und Versicherungen oder für den Rechnungsführer des Finanzministeriums festgelegt wurde. Außerdem bedarf jede Entscheidung zur Entlassung des Leiters von ILITA einer gerichtlichen Überprüfung, bei der angemessene Gründe vorgelegt werden müssen. Schließlich wird der Leiter von ILITA durch das israelische Arbeitsgericht einschließlich der folgenden Bestimmungen der Grundrechte geschützt: Freiheit der Beschäftigung, Grundsätze der Angemessenheit, der Verhältnismäßigkeit und des fairen Verfahrens.

Im Hinblick auf die Unabhängigkeit der ILITA berücksichtigt die Arbeitsgruppe die Erklärungen der israelischen Behörden in Bezug auf den anzuwendenden allgemeinen Haushaltsplan für Kontrollbehörden. Dieser ähnelt dem Haushaltplan für die ILITA und bestätigt, dass aufgrund der Zuteilungen der letzten paar Jahre von einem angemessenen Status der Unabhängigkeit ausgegangen werden kann.

Außerdem berücksichtigt die Arbeitsgruppe die Tatsache, dass gemäß Abschnitt 36S b PPA die Gebühren, die für die Registrierung von Datenbanken erhoben werden, der ILITA als Kontrollbehörde direkt für die ihr per Gesetz zugewiesenen Aufgaben zustehen.

Die Arbeitsgruppe berücksichtigt auch die Erklärungen der israelischen Behörden, mit denen diese die Unabhängigkeit zum Ausdruck bringen, mit der diese Behörden ihre Aufgaben ausüben. Darunter fällt auch die Durchführung von Kontrollen bei öffentlichen Stellen wie dem Büro des Generalstaatsanwalts, dem Innenministerium, dem Transportministerium, dem Verteidigungsministerium und sogar dem Finanzministerium, dem die ILITA angehört.

Schließlich ist die Arbeitsgruppe der Ansicht, dass die der ILITA zugewiesenen Kompetenzen, die sogar die Verfolgung von strafbaren Handlungen im Bereich des Datenschutzes umfassen und die Tatsache, dass die ILITA mit der Organisation der 32. Internationalen Konferenz für den Schutz der Privatsphäre und den Datenschutz beauftragt wurde, die im Oktober 2010 in Jerusalem stattfindet, die Anstrengungen verstärken, die der Staat Israel unternimmt, um die Existenz einer Behörde für den Schutz personenbezogener Daten zu garantieren und dieses Recht angemessen zu schützen.

Angesichts des oben Stehenden kommt die Arbeitsgruppe zu dem Schluss, dass der Staat Israel eine Kontrollbehörde für den Datenschutz hat, die mit der erforderlichen Unabhängigkeit und angemessenen Durchsetzungsmechanismen ausgestattet ist und den Bestimmungen aus Artikel 28 der Richtlinie annähernd entspricht.

Durchsetzungsmöglichkeiten und Sanktionen

Nachdem die ILITA eine Beschwerde untersucht hat, prüft sie deren Begründetheit. Ist sie begründet, hat die ILITA die Befugnis, dem für die Verarbeitung Verantwortlichen der Datenbank Vorschriften zur Einhaltung der Bestimmungen zu erteilen.

Abschnitt 31A PPA umfasst eine Liste der strafbaren Handlungen im Fall von Übertretungen. Es sollte angemerkt werden, dass die ILITA wie bereits gesagt, gemäß ihren Durchsetzungsbefugnissen erst selbst ermitteln und dann an einem Gericht ein Strafverfahren anhängig machen kann.

Darüber hinaus hat die ILITA die Befugnis, für die in Abschnitt 31A aufgeführten strafbaren Handlungen gemäß dem Anhang zu den Verordnungen über Ordnungswidrigkeiten (Geldbußen für Ordnungswidrigkeiten – Datenschutz) 2004, Verwaltungsgebühren zu erheben. Die Verordnungen hat der Justizminister gemäß seiner ihm durch das Gesetz über Ordnungswidrigkeiten aus dem Jahr 1985 zustehenden Befugnis erlassen. Das System der Geldbußen für Ordnungswidrigkeiten ermöglicht es dem jeweiligen Exekutivorgan, eine Geldbuße zu verhängen und es dem Beklagten zu überlassen, ob er die Buße zahlt oder ein Gerichtsverfahren anstrebt.

Zusammen mit den genannten Sanktionen, legt Abschnitt 10 f PPA Folgendes fest: *„Wenn der Besitzer oder der Eigentümer einer Datenbank eine Bestimmung dieses Gesetzes oder die darunter fallenden Vorschriften verletzt oder einem Ersuchen des Datenbankbeauftragten nicht nachkommt, hat dieser das Recht, die Eintragung der Datenbank im Register ganz oder für eine von ihm festzusetzende Zeitdauer zu streichen, voraussetzt, dass dem Eigentümer vor der Aussetzung oder Streichung die Möglichkeit auf rechtliches Gehör gegeben wurde“*.

Angesichts all dessen ist die Arbeitsgruppe der Ansicht, dass die israelische Gesetzgebung die notwendigen Elemente bereitstellt, um ein gutes Niveau bei der Einhaltung der Datenschutzregeln zu gewährleisten.

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

Die Arbeitsgruppe vertritt die Ansicht, dass dieser Grundsatz durch die israelische Gesetzgebung in ausreichendem Maße gewährleistet wird. Insbesondere Unterabschnitte d und e Satz 1 des Abschnitts 10 legen Folgendes fest:

„(d) Der Justizminister setzt mit der Zustimmung des Verfassungs- und Rechtsausschusses der Knesset durch Beschluss eine Kontrolleinheit fest, die die Datenbanken, ihre Registrierung und die ihnen zugrundeliegende Informationssicherheit überwacht. Die Größe der Einheit wird entsprechend dem Kontrollbedarf bestimmt.

(e) Der Datenbankbeauftragte steht der Kontrolleinheit vor. Er ernennt Inspektoren, die die Kontrolle im Sinne dieses Gesetzes durchführen. Niemand darf zum Inspektor ernannt werden, der nicht eine angemessene Berufsausbildung im Bereich Computerisierung und Informationssicherheit sowie eine angemessene Ausbildung im Bereich Ausübung der Befugnisse im Sinne des Gesetzes erhalten hat oder dessen Ernennung die israelische Polizei aus Gründen der öffentlichen Sicherheit widerspricht.

(e1) In der Ausübung seiner Aufgaben kann ein Inspektor –

(1) jede zuständige Person dazu auffordern, ihm Informationen und Unterlagen auszuhändigen, die sich auf die Datenbank beziehen;

(2) Räumlichkeiten betreten, bei denen er die begründete Annahme hat, dass dort eine Datenbank betrieben wird, die Räumlichkeiten durchsuchen und Gegenstände beschlagnahmen, wenn er davon überzeugt ist, dass dies erforderlich ist, um die Umsetzung dieses Gesetzes sicherzustellen und eine Verletzung seiner Bestimmungen zu verhindern; die Bestimmungen der Strafprozessordnung [Festnahme und Durchsuchung] [neue Version], 5869 – 1969 finden auf die Gegenstände Anwendung, die gemäß diesem Abschnitt beschlagnahmt wurden; Vorkehrungen für das Betreten einer Militäreinrichtung oder einer Einrichtung einer Sicherheitsbehörde im Sinne von Abschnitt 19 c werden durch den Justizminister in Beratung mit dem Minister entschieden, der der jeweiligen Sicherheitsbehörde vorsteht; in diesem Abschnitt bedeutet „Objekt“ auch Computermaterial und Datenausgabe gemäß der Definition im Computergesetz, 5765 – 1995;

(3) unbeschadet der Bestimmungen von Absatz 2 ist ein Inspektor nicht dazu befugt, Räumlichkeiten zu betreten, die nur als Wohnung genutzt werden, es sei denn, es liegt ein entsprechender Beschluss eines Richters am Amtsgericht vor“.

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

Zusammen mit den vorstehend analysierten Sanktionen in den Bereichen Verwaltung und Strafrecht, gibt Abschnitt 31B PPA Folgendes an: *„Eine Handlung oder eine Auslassung, die zu einer Verletzung der Bestimmungen der Kapitel zwei oder vier oder zu einer Verletzung der Bestimmungen dieses Gesetzes führt, gilt als Vergehen gemäß der Zivilgesetzordnung“*.

Deshalb ist die Arbeitsgruppe der Ansicht, dass das israelische Recht das Recht der betroffenen Person auf Entschädigung für eine Verletzung ihrer Rechte oder ihres Eigentums als Folge einer unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten ausreichend garantiert.

4. ERGEBNIS DER BEURTEILUNG

Ausgehend von den obigen Feststellungen kommt die Arbeitsgruppe daher zu dem **Schluss, dass Israel** 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 **ein angemessenes Schutzniveau** bei automatisierten internationalen Datenübertragungen **garantiert** sowie im Fall der nicht automatisierten Datenübertragung, bei einer weiteren automatisierten Verarbeitung auf israelischem Hoheitsgebiet.

Gleichzeitig fordert die Arbeitsgruppe die israelischen Behörden jedoch dazu auf, in Zukunft bei der Gesetzgebung, und dies gilt insbesondere für Gesetze, die mit der Umsetzung des „Schoffman-Berichts“ in Verbindung stehen, Folgendes ins Auge zu fassen:

- Die Anwendung der israelischen Gesetzgebung auf manuelle Datenbanken, damit die Beurteilung der Angemessenheit auch auf die Fälle ausgedehnt werden kann, die nicht bei den Schlussfolgerungen der vorliegenden Stellungnahme eingeschlossen sind.

- Die ausdrückliche Anwendung des Grundsatzes der Verhältnismäßigkeit auf die Gesamtheit der Verarbeitungen personenbezogener Daten im privaten Sektor.

- Eine Auslegung der Ausnahmen in der internationalen online-Datenübermittlung, die in Artikel 26 Absatz 1 der Richtlinie vorgesehen sind.

Die Arbeitsgruppe stellt abschließend fest, dass sie innerhalb des Rechtsrahmens, der aufgrund der letztendlich angenommenen Entscheidung der Kommission erstellt wird, die angenommenen Maßnahmen in Bezug auf die oben diskutierten Bereiche genau beobachten wird.

Brüssel, den 1. Dezember 2009

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK