ARTICLE 29 DATA PROTECTION WORKING PARTY

02316/09/EN
WP 165

Opinion 6/2009 on the level of protection of personal data in Israel

Adopted on 1 December 2009

The Working Party on the protection of individuals with regard to the processing of personal data

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "the Directive") and in particular Article 29 and Article 30 (1) (b) thereof,

Having regard to the Rules of Procedure of the Working Party, and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. BACKGROUND

On 12 July 2007, the Israeli Mission to the European Union requested the Commission to launch the procedure to declare Israel as a country that ensures an adequate level of protection for the purposes provided for in Articles 25 and 26 of the Directive.

In order to examine Israel's adequacy, the Commission requested the Centre de Recherches Informatique et Droit (hereinafter “CRID”) from Namur University to produce an extensive report which analysed the extent to which the Israeli regulatory system fulfilled the requirements for the application of the personal data protection regulations set out in the Working Document “Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection Directive”, adopted by the Working Party set up under Article 29 of the Directive on 24 July 1998 (document WP12).

The aforementioned report, together with the preliminary response to the same from the Israeli authorities, was discussed by the Safe Harbour Subgroup during a meeting held on 18 March 2009.

At that meeting, the Subgroup submitted to the Working Party for an opinion a proposal that its President should send a letter to the Israeli authorities which, while positively assessing the existing data protection scheme in Israel, would emphasize those issues that required further clarification.

On 2 September 2009, the Israeli authorities sent, through the Israeli Law, Information and Technology Authority (hereinafter "ILITA"), an extensive report to the Working Party, in which they responded to the issues raised in the said letter.

This report has been analysed by the members of the Subgroup, and was also the subject of a meeting to hear the aforementioned authorities, which was held on 16 September 2009. During that meeting, the members of the Subgroup requested the Israeli authorities, represented by the Head of ILITA and the Head of its Legal Department, to clarify those issues that, following the earlier discussion of the report sent to the Subgroup, still needed further clarification.

The Subgroup informed the Working Party, during its meeting held on 12 and 13 October 2009, of the conclusions reached at the meeting of 16 September, and proposed the adoption of the present Opinion, under the terms contained herein. The proposal was approved by the Working Party at the aforementioned meeting.

2. LAW ON DATA PROTECTION IN ISRAEL

The Israeli legal system is characterized by two key elements which distinguish it from other legal systems and, in particular, from those of the Member States: firstly, Israel does not have a written Constitution; secondly, although its system may be considered as fundamentally linked to those systems that are based on Common Law, it also includes certain characteristics which point to the influence of Continental Law.

The absence of a written Constitution is complemented by the existence of the so called "Basic laws" which have been given constitutional status by the Supreme Court of Israel. At the same time, certain basic principles and fundamental human rights, such as equality, freedom of speech or freedom of religion, also have constitutional status.

Within this framework, the right to privacy is included under section 7 of the Basic Law: Human Dignity and Liberty, which establishes the following:

> *(a) All persons have the right to privacy and to intimacy.*
> *(b) There shall be no entry into the private premises of a person who has not consented thereto.*
> *(c) No search shall be conducted on the private premises of a person, nor in the body or personal effects.*
> *(d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.*

At the same time, the right to privacy and to the protection of personal data is regulated by the Privacy Protection Act (hereinafter the "PPA"), passed in 1981 and subject to amendments on nine subsequent occasions. The most relevant amendment was passed in 2007 and it established new requirements for the processing of personal data, and regulated the organization, powers and functions of the supervising authority in matters of personal data protection in greater detail and with greater precision than the existing legislation up to that date, creating an Authority within the Ministry of Justice - namely the Israeli Law, Information and Technology Authority (ILITA) - which includes the previous Database Registrar.

In addition, due attention has to be paid to a report drafted in January 2007 by a Committee of Experts appointed by the Ministry of Justice, known as the "Schoffman Report", which made a set of recommendations for amending the data protection legislation which are currently being considered for the purposes of adopting a new data protection framework.

Lastly, the data protection legislation is complemented, with respect to the written law, by several decisions adopted by the Israeli Government, specifically with regard to the implementation of the PPA (for example, on international data transfers) as well as to the organization and functioning of ILITA (for example, with respect to the duration and causes for the termination of the mandate of the head of ILITA).

Furthermore, as indicated previously, the Israeli legal system shares, to a great extent, the principles that are characteristic of the Common Law systems. This is why written regulatory provisions must, in any event, be supplemented by the judgments adopted in accordance with them, which have the value of precedent and directly form part of the Israeli sources of law. The report requested by the Committee and issued by the Israeli authorities, as well as the statements made by the latter during the hearing held by the Subgroup on 16 September 2009, have provided the Working Party with a large number of judicial resolutions which have to be taken into consideration in the assessment to be conducted by the Working Party.

Lastly, in this preliminary assessment, it must be pointed out that Israel has ratified the International Covenant on Civil and Political Rights of 1966, although in Israeli law, ratification of an International Agreement does not mean that it is directly incorporated into domestic law.

3. ASSESSMENT OF THE DATA PROTECTION LAW OF ISRAEL AS PROVIDING ADEQUATE PROTECTION OF PERSONAL DATA

The Working Party points out that its assessment on the adequacy of the Law on data protection in Israel focuses on the Privacy Protection Act (PPA).

This Act's provisions, as well as the case law made by the courts with regard to the protection of personal data, have been compared with the main provisions of the Directive, taking into account opinion WP12 of the Working Party. This opinion lists a number of principles which constitute *a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate*.

3.1 Scope of the regulating rules on data protection within the Israeli law.

As on certain previous ocassions, the Working Party believes that it is necessary, before proceeding to the specific assessment of the fulfilment of the principles settled in the document WP12, to examine the scope of application of the regulation on data protection within Israeli law.

a) Concept of personal data or "information".

In particular, the Working Party believes that it is necessary to take into account the concept of the term "personal information" referred to in the PPA and its link to the concept of "personal data" provided in the Directive. Likewise, it will be necessary to determine whether Israeli law establishes the appropriate safeguards on data protection in relation to any processing or if the said regulation is only applicable to total or partial automated processing systems, taking into account the framework of protection established through the Directive.

In relation to the first issue, the Working Party confirms that the definition of "information" referred to in section 7 of the PPA is not similar to the definition set out in the Directive. Thus, the aforementioned rule states that "*information means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person"*. The definition refers solely to certain data categories and does not allow to know if information regarding a non-identified but identifiable person would be protected under the PPA.

Nonetheless, the Working Party takes into account the explanations given on this issue by the Israeli authorities and, in particular, the judicial precedents provided by them which imply an extension of the legal concept of information, making it similar to the concept of *"data of a personal nature"* within the meaning of the Directive.

In particular, this conclusion is reached in view of certain rulings, such as the one pronounced by Israel´s Supreme Court in the case of *Israel v. Bank Ha'Po'alim*, which states that *"the term information (...) should include data that can be derived from a database which is not indexed according to individual names"*.

The Working Party, in addition to the rest of the rulings provided, considers as especially relevant the case-law arising out of the judgment *Rani Mor v. Ynet* of the District Court of Haifa, referring to the IP address, where the conclusion reached can be assimilated to that held by the Working Party, by indicating that *"Identifying an online user by disclosing his or her IP address without consent may constitute a tort of infringement of privacy"*.

Therefore, with regard to the concept of personal data or "information" for the purpose of the application of the regulation on data protection, the Working Party believes that the case law has supplemented what was established by the PPA, making it possible from this perspective to consider the safeguards offered by this Law as constituting a protective framework, as regards the concept of personal data, similar to the one provided by the Directive.

b) Protected processing systems in Israeli law.

The Working Party has to refer at this point to the special structure of the PPA and, in particular, its first two Chapters: Chapter 1 refers to breaches of privacy in general, while Chapter 2 regulates the protection of privacy in databases.

With respect to the second chapter, Section 7 of the PPA defines a database as *"a collection of data, kept by a magnetic or optic means and intended for computer processing"*. In this way, the system of guarantees established in Chapter 2 will be applicable only to those cases in which there is an automated processing of information and not in those cases where there is no such automated processing.

The Working Party takes note of the explanations given by the Israeli authorities, to the effect that citizens would be protected against non-automated data processing (or manual processing) by the safeguards enshrined in Chapter 1 of the PPA, where certain principles are reflected, such as the limitation of the purpose, secrecy and consent.

Nonetheless, it is worth recalling that the protection which the Directive conferson these types of processing relates not only to the abovementioned principles, but to the totality of its system and, in particular, to the principles contained in document WP12. For this reason, in order to be able to consider that the level of data protection of a certain State with regard to non-automated processing systems is adequate, it would be necessary for the domestic law of the said State to recognize, at least in respect of these processing systems, the aforementioned principles.

For this reason, since Chapter 1 does not include the abovementioned principles in their entirety, it is not possible to consider the Israeli legislation as adequate with regard to non-automated or manual processing systems. In this connection, the Working Party would like to recall that the "Schoffman Report" reached the same conclusion, proposing a reform of the legal framework in force in Israel to extend the totality of the data protection safeguards to include manual processing systems.

Thus, the Working Party believes that the analysis of the adequacyof the system of data protection in Israel cannot refer to the non-automated processing of data, since the said framework does not establish the safeguards envisaged in document WP12.

To this end, the Working Party also wishes to make it clear that it believes it could continue its adequation analysis with regard to total or partially automated processing systems. Therefore, it should not be considered as excluding from the adequation examination, which will be carried out from this point, those international data transfers to Israel that are made through automated means or those that, even if they have not been carried out through the said means, refer to data that are subsequently going to be the subject of automated processing in the State of Israel.

Therefore, only those international data transfers whereby the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means will be excluded from this assessment, since it is only in such cases that the provisions of Chapter 1 of the PPA do not apply.

The Working Party is aware that the volume of transfers excluded from the adequation assessment will be residual, and will not significantly affect the application of the Decision that may ultimately be adopted; however, it believes it is essential to make the said exception in the light of the Directive´s provisions. At the same time, it recommends the adoption of provisions that envisage the application of Israeli legislation to manual databases as part of the legislative developments to be carried out in the future, and in particular in those related to the implementation of the “Schoffman Report”, with the aim of being able to expand its assessment, where applicable, to include these processing systems.

3.2. Principles related to the content

Taking the above statements into consideration, we will now proceed to assess the level of data protection in Israel, in the light of the principles contained in document WP12, starting with the study of the principles with which the legislation of the State of Israel should comply.

a) Fundamental Principles

1) The purpose limitation principle: data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive.

The Working Party believes that Israeli legislation respects this principle. Thus, in general terms, Article 2 (9) of the PPA states *that "using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given"* is a breach of privacy.

This general principle is even reinforced by Article 8 (b) of the Law, which provides that *"a person shall not use information in a database that requires registration under this section except for the purpose for which the database was established"*.

Furthermore, for those instances in which the database has been registered with the supervisory authority, Article 9 (b) (2) of the PPA says that the request must include *"the purposes for which the database was established and the purposes for which the information is intended"*.

Finally, the Working Party confirms that the Courts of Justice have interpreted these rules in similar terms to those envisaged by the Directive. In particular, it takes into consideration the prohibition of incompatible use of financial data referred to by Israel´s Supreme Court in the case *Database Registrar v. Ventura*.

> **2) The data quality and proportionality principle:** data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

With regard to the principle of quality in the strict sense, the Working Party believes that, even though it is not listed as an independent principle, the obligation of keeping the exact data and, if appropriate, keeping them up to date, is recognized by Israeli law through the regulation on the right to rectification referred to in Section 14 of the PPA.

Thus, Subsection (a) of the said Section states that *"A person who, on inspecting any information about himself finds that it is not correct, not complete, not clear or not up to date may request the owner of the database or, if such owner is a non-resident, the possessor thereof to amend or delete the information"*.

Subsections (b) and (c) refer to the decision of the owner of the database. Therefore, *"Where the owner of a database agrees to a request under subsection (a), he shall make the necessary changes in the information and shall notify them to every person who received the information from him within a period prescribed by regulations"*.

In case of refusal, the owner must communicate it to the data subject, adding Section 15 whereby *"a person requesting information may, in the form and manner prescribed by regulations, appeal to the Magistrate's Court against refusal by the owner of a database to enable inspection under section 13 or section 13A and against notice of refusal under section 14(c)"*.

With regard to the principle of proportionality derived from Article 6(1)(c) of the Directive, the Working Party confirms that this principle is not specifically recognized in the PPA. Nonetheless, the Working Party satisfactorily receives explanations and case law provided in relation to this issue by the Israeli authorities, which to a large extent enable the said deficiency to be offset.

Thus, the Working Party considers as satisfactory the clarifications given with respect to the constitutional scope of the proportionality principle when the processing is carried out in the public sector. In particular, it considers as especially relevant the law of precedent derived from the judgement by the Supreme Court pronounced in the case *Acri v. Minister of Interior,* provided by the Israeli authorities, where there is an express reference to the undertaking of the proportionality principle in the terms provided by the Directive.

In the same way, the Working Party welcomes with satisfaction the clarifications given by the Israeli authorities with regard to the legal requirement of proportionality in the processing, based on the principles of reasonableness of the measure and good faith. In this sense, it considers particularly interesting the precedent established by the case *Eisner v. Richmond,* which restricted the use of videocameras at the workplace and by others following a ruling by the National Labour Court in Tel Aviv. The Working Party also considers relevant the application of the proportionality principle in consumer protection and the court resolutions in which the competent courts, and in particular the Standard Contract Court in Jerusalem, have invalidated clauses that allowed the exchange of information within business groups, as in the case *Bank of Israel v. First International Bank of Israel*.

In light of this case-law, the Working Party believes that the proportionality principle is guaranteed in most of the instances in which it would be possible to apply a disproportionate processing to personal data and, in particular, that the proportionality principle is a constitutional principle that must be observed by any data processing carried out within the public sector or within the private sector when performing public tasks.

Nonetheless, the Working Party believes it would more satisfactory if Israeli legislation explicitly included this principle, with the aim of guaranteeing that the activities that lie within the private sector and tare different from those for which there are already court rulings based on the principles of reasonability and good faith, will be able to deal in the future with problems of intepretation that could hinder the adequate protection of the rights of the individuals involved. In this connection, the Working Party recalls that the inclusion of this principle within the PPA is contained in the conclusions of the "Schoffman Report".

In this way, without the aforementioned conclusion affecting the final assessment regarding the level of protection of the State of Israel, the Working Party believes that the future legislative developments and, in particular, those related to the implementation of the "Schoffman Report", should adopt the provisions that envisage the express application of the principle of proportionality in relation to the totality of personal data processing carried out by the public and private sectors.

> **3) The transparency principle:** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2)3 and 13 of the Directive.

The Working Party believes that the legislation of the State of Israel complies sufficiently with this principle.

Section 11 of the PPA provides that:

> *"A request to a person for information with a view to the keeping and use thereof in a database shall be accompanied by a notice indicating*
> *(1) whether that person is under a legal duty to deliver that information or whether its delivery depends on his volition and consent;*
> *(2) the purpose for which the information is requested;*
> *(3) to whom the information is to be delivered and the purposes of such delivery."*

Furthermore, in accordance with section 13A (1) of the PPA *"The owner of a database who keeps it at the place of another person (in this section - the possessor) shall refer the person making the request to the possessor, with his address, and order the possessor, in writing, to enable the person making the request the inspection"*. Likewise, according to subsection (2) *"Where the person making the request applies to the possessor first, the possessor shall inform him if he possesses information about him, and also the name and address of the owner of the database"*.

> **4) The security principle:** Technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

The Working Party believes that the State of Israel guarantees this principle, taking specifically into account the provisions of sections 16, 17, 17A and 17B of the PPA.

Section 7 defines "information security" as the "*protection of the integrity of the information, or protection of the information from being exposed, used or copied, without lawful permission"* and Section 17 adds that *"A database owner, possessor or manager, are each responsible for the information security in the database"*.

Article 17B specifically establishes that certain owners of a database or its processors must appoint a security supervisor with the appropriate qualifications, who will be responsible for the security obligations.

In addition, Article 16 regulated the confidentiality obligation in the processing of information by establishing that *"No person shall disclose any information obtained by him by virtue of his functions as an employee, manager or possessor of a database save for the purpose of carrying out his work or implementing the Law or under a court order in connection with a legal proceeding; where the request is made before a proceeding has been instituted, it shall be heard in the Magistrate's Court"*. Failure to comply with this obligation may result in a prison sentence of up to five years.

Finally, Article 17A of the PPA refers to the processor, providing the following:

> *"(a) A person who possesses databases of different owners shall ensure that access to each database is provided only to persons who are expressly authorized to do so by written agreement between the person and the owner of the said database.*
> *(b) A person who possesses at least five databases that require registration under section 8 shall deliver annually to the Registrar a list of the databases in his*

possession, indicating the names of the owners of the databases, verified by affidavit that, in respect of each of the databases, the persons entitled to access to the database were determined by agreement between the person and the owner, and the name of the security supervisor, as referred to in section 17B."

5) **The rights of access, rectification and opposition:** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights must be in line with Article 13 of the Directive.

Section 13 (a) of the PPA establishes that "*every person is entitled to inspect, either himself or through a representative authorized by him in writing or his guardian, any information about him kept in a database"*, `providing Section 13 (b) that "*the owner of a database shall enable, at the request of a person referred to in subsection (a) (hereinafter "person making the request") inspection of the information, in the Hebrew, Arabic or English language"*.

With regard to the right of rectification, section 14 (a) of the PPA, already analysed above, establishes that *"A person who, on inspecting any information about himself finds that it is not correct, not complete, not clear or not up to date may request the owner of the database or, if such owner is a non-resident, the possessor thereof to amend or delete the information"*.

Failure to comply with the obligations imposed on the controllers by virtue of these sections constitutes a criminal offence under Article 31 and could also give rise to a civil liability vis-à-vis the data subject under section 31B. These sections will be studied in more detail later in the present opinion.

With regard to the right to object, section 17F of the PPA expressly establishes such right in relation to direct marketing activities, as will be seen further on.

Having said this, the Working Party confirms that the Israeli legislation does not establish this right through a general clause. Nonetheless, it takes into account that, according to the PPA, data can be collected only for a limited purpose (sections 8(b), 2(9)), of which the data subject has been informed (sec. 11). Hence, the Working Party considers that a data subject can oppose the processing of the data on the grounds that it exceeds the purposes for which the data was collected, or that he was not properly informed thereof. In such a case, the excessive processing is considered a violation of privacy under sec. 2(9) of the PPA, a criminal offence under sec. 31A(a)(1), and misrepresentation of the notice requirement, which is a criminal offence under sec. 31A(a)(3).

Section 15 of the PPA additionally establishes that "*a person requesting information may, in the form and manner prescribed by regulations, appeal to the Magistrate's Court against refusal by the owner of a database to enable inspection under section 13 or section 13A and against notice of refusal under section 14(c)"*.

Lastly, the Working Party believes that exemptions to the exercise of the right to access, and therefore to rectify, provided in section 13 (c·) of the PPA are consistent with those contained in Article 13 of the Directive for the Member States. In this sense, the Working Party positively values the case law derived from the law courts in relation to the exercise of the aforementioned rights and, in particular, the case law contained in the ruling pronounced by

the Supreme Court in the case of *Fischler v. Chief of Police,* in which the data subject was granted the right to know the information about himself contained in the police files.

Therefore, the Working Party believes that the legislation of the State of Israel sufficiently guarantees the rights of the data subjects to access their data, request the rectification or object to the processing thereof, according to the terms contained in document WP12.

> **6) Restrictions on onward transfers:** further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the Directive (These exemptions are examined in Chapter Five).

For the purpose of assessing compliance with this principle, the Working Party takes into consideration the provisions of Privacy Protection (Transfer of Databases Abroad) Regulations adopted by the Government of Israel on 17 June 2001.

The regulations prohibit the transfer of data to third countries, unless those countries provide a level of data protection which is not less than that laid down in Israeli law, and specifically refers to several basic principles, such as lawful and legal collection and processing of data, purpose limitation, data quality (accuracy and keeping data up to date), respect for the right of access (and subsequently, according to Israeli legislation, rectification), and data security.

Regulation 2 (8) specifies several cases that could be considered as a legal presumption of adequacy, including Member States, those countries that are a Party to Convention 108 of the Council of Europe or those for which *"the Registrar of Databases announced that an agreement has been achieved with a privacy agency of the third country"*.

Paragraphs (1) to (7) of Regulation 2 specify several exemptions to these general rules:

- *"if the data subject consented.*
- *if it is impossible to have the consent, and it is crucial to transfer the data to protect the person's health.*
- *if the data is transferred to a [foreign] corporation held by the owner of the [local] database, and he has guaranteed the data protection.*
- *if the receiver of the data has undertaken the obligation to provide data protection as if it were kept in Israel.*
- *if the data is available to the public under a statutory authorization.*
- *if the transfer is crucial to protect public order of safety.*
- *if the transfer of data is required by Israeli law."*

Regulation 3 states the accountability principle, which provides that the transferring party should arrange for the receipt of a guarantee from the receiver of the data that sufficient measures are undertaken to secure the data, and that such data are not further transferred.

The Working Party also believes that the rules that have been set out comply with the principle of restriction of further data transfers to third countries and that the guarantees provided by the Israeli legislation on this issue make it possible to guarantee adequate respect for the rights of citizens of the European Union whose data are being processed in Israel.

Nonetheless, the Working Party would like to recall the criteria for the interpretation of exemptions established by Article 26(1) of the Directive and contained in its "*Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*" (document WP114) and it urges the Israeli authorities to carry out any interpretation of the exemptions contained in rule 2, previously mentioned, in accordance with the criteria included in the said document and in the Directive itself.

b) Supplementary principles

Document WP12 refers to certain principles that must be applied to specific processing systems, in particular the following:

> **1) Sensitive data -** where 'sensitive' categories of data are involved (those listed in Article 8 of the Directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

Section 7 of the PPA includes the concept of "sensitive data", defining it as:

> *"(1) data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person;*
> *(2) information that the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, is sensitive information.";*

The Working Party believes that, although the above list does not fully coincide with the one established under Article 8 of the Directive, it may be regarded as similar. In particular, the WP understands that information which refers to opinions and beliefs includes much of the data mentioned in the said Article. In addition, the Working Party urges the Israeli authorities to consider as sensitive, not least because it belongs to the "*intimate affairs*" category, such information which refers to the data listed in Article 8 of the Directive that could not be included under the other categories envisaged by the PPA and, in particular, the data related to ethnic origin or sexual preferences.

The Working Party also confirms that, in general, data may only be collected with the prior consent of the data subject, which - according to section 3 of the PPA - may be either express or implicit. This possibility does not fully meet the requirements of Article 8 of the Directive, which states that the consent must be explicit.

However, this possible gap is overcome by the abovementioned section 3, which requires that, in any event, the consent has to be informed. In this way, the Working Party believes the processing of such data may only be carried out as a consequence of an action from the data subject and not as a result of the direct giving of consent if the subject has been clearly informed of the terms explained when referring to the principle of transparency.

For this reason, even when the processing may derive from implicit consent of the data subject, the Working Party believes that a prior action from the controller is necessary, aimed at enabling the data subject to learn of all the consequences of the action involved in him giving this consent.

Therefore, even though there is no rule similar to the one envisaged in the Directive, the Working Party believes the Israeli legislation adequately meets this principle.

2) Direct marketing - where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt out' from having his/her data used for such purposes at any stage.

The Working Party satisfactorily confirms that this principle is clearly regulated by the Israeli legislation, since the PPA contains a Part within its Chapter 2 specifically aimed at "direct mailing" defined as "*contacting a person personally, based on his belonging to a group of the population that is determined by one or more characteristics of persons whose names are included in a database*".

The Israeli legislation contains specific obligations in the event of the processing of the said data. In particular, the controllers must register the file with the supervisory authority and keep an up-to-date register of the sources from which they obtained the data. Furthermore, there are specific information requirements that must be included in all deliveries addressed to the data subjects.

With regard to the principle itself, the Working Party believes that it is met by subsections (b) and (e) of section 17F of the PPA, which establish the following:

"(b) Every person is entitled to demand, in writing, of the owner of the database used for direct mailing that the information relating to him be deleted from the database.
(c) Every person is entitled to demand, in writing, of the owner of the database used for direct-mailing services or of the owner of the database containing the information based on which the contact was made, that the information relating to him not be delivered to a person, to a type of persons or to specific persons, for either a limited period of time or permanently.
(d) Where a person informed the owner of the database of his demand as specified in subsections (b) or (c), the owner of the database shall act in accordance with the demand and notify the person, in writing, that he acted accordingly.
(e) Where the owner of the database did not give notice as specified in subsection (d) within 30 days from the day of receipt of the demand, the person whom the information is about may apply to the Magistrate's Court in the manner prescribed by regulations, to order the owner of the database to act as specified."

3) Automated individual decision: where the purpose of the transfer is the taking of an automated decision within the meaning of Article 15 of the Directive, the individual should have the right to know the logic underlying this decision, and other measures should be taken to safeguard the individual's legitimate interest.

The Working Party confirms that Israeli legislation does not contain any express provision with regard to this principle. However, it satisfactorily receives comments contained in the report issued by the CRID and the clarifications carried out by the Israeli authorities in the sense that the Israeli law, in any event, enables the data subject to object to the adoption of these types of decisions.

In any event, without prejudice to considering this principle as met at this point in time, the Working Party urges the Israeli authorities to explicitly contemplate this principle in similar terms to Article 15 of the Directive in all future regulatory measures to be adopted regarding this matter.

3.3. Procedure/Application mechanisms

The opinion issued by the Working Party WP12 "Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive" indicates that, in order to provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the range of different judicial and non-judicial procedural mechanisms used in third countries.

In this respect, the objectives of a data protection system are essentially threefold:

- To deliver a good level of compliance with the rules.
- To provide support and help to individual data subjects in the exercise of their rights.
- To provide appropriate redress to the injured party where rules are not complied with.

a) To deliver a good level of compliance with the rules: a good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for the rules, as can systems of direct verification by authorities, auditors, or independent data protection officials.

The Israeli Law, Information and Technology Authority (ILITA).

Pursuant to Section 7 of the PPA, a Database Registrar is created, whereby the *"Registrar means a person who has the qualifications to be appointed judge of a Magistrate's Court, and was appointed by the Government, by notice in Reshumot, to keep a "Register of Databases" (hereinafter referred to as "the Register") as prescribed in section 12"*.

This Registrar has been currently integrated, by virtue of a decision from the Government of Israel in 2006, in ILITA, which was created under the aforementioned decision so that the controller of the Database Register is, in turn, the Head of ILITA. Furthermore, ILITA also integrates the Certification Authorities Registrar and the Credit Data Services Registrar.

The enforcement capabilities of ILITA are regulated by section 10 of the PPA. In this sense, the Working Party, in accordance with the explanation given above, is aware that these capabilities, granted by Law to the Database Registrar, correspond to ILITA, in which this Registrar is integrated.

In particular, the PPA grants ILITA powers to register and inspect the processing, under the terms mentioned below.

The Working Party takes note of the recent modifications adopted by the Government of the State in relation to the appointment and dismissal of the Head of ILITA and believes that such modifications grant the latter, and therefore the said authority, an adequate degree of independence for the purposes that are established for supervisory authorities regulated by the Directive. In particular, it takes into account that those who integrate ILITA and its Head have the profile of civil servants, and are not subject to any type of mandate or political profile.

To that end, the Working Party takes into account that, in accordance with Government Decision 4660 (HC/195) dated 8 January 2006, the appointment of the Head of ILIRA, as a high ranking official, is subject to prior assessment by an independent committee, composed of five members, with representatives from the public authorities, the Academy and the supervised entities, who set the required conditions for the appointee and propose the appointment of the person chosen.

In addition, the Working Party acknowledges with satisfaction that, according to Government Decision No. 4470 dated 8 February 2009, the term of tenure for the Head of ILITA was set at six years. The functions of Head of ILITA may be terminated only in special circumstances by a special Civil Service Commission committee headed by a former judge. This mechanism is similar to that established in Israel, among others, for the Antitrust Commissioner, the Capital Markets and Insurance Regulator or the Accountant General in the Ministry of Finance. Moreover, any decision to terminate the Head of ILITA would be subject to judicial review in which reasonable grounds would have to be shown. Finally, the Head of ILITA is protected by Israeli labour law, including the provisions of the Basic Law: Freedom of Employment; principles of reasonableness, proportionality and procedural fairness.

With regard to ILITA's budgetary independence, the Working Party takes into account the explanations given by the Israeli authorities in relation to the applicable budget scheme, in general terms, for supervisory authorities in Israel, which is similar to ILITA´s and, at the same time, confirms that assignations given in the last few years make it possible to consider its status of independence as adequate.

Moreover, the Working Party takes into consideration the fact that, pursuant to section 36S (b) of the PPA, the funds resulting from the collection of fees for the registration of databases directly revert to ILITA as the supervisory authority for the development of the functions which have been attributed to it by Law.

The Working Party also takes into consideration the statements made by the Israeli authorities in which they express the independence with which these authorities have carried out their duties, including the performance of inspections to public bodies, such as the Office of the Attorney General, the Ministry of Internal Affairs, the Ministry of Transportation, the Ministry of Defence or even the Ministry of Justice, in which ILITA is integrated.

Finally, the Working Party believes that the competencies attributed to ILITA, which even include the prosecution of criminal offences against privacy, and the fact that ILITA has been designated to organize the 32nd International Conference on Privacy and Personal Data Protection, which is scheduled to be held in Jerusalem in October 2010, reinforce the efforts made by the State of Israel to guarantee the existence of a personal data protection authority and to adequately safeguard this right.

In the light of all of the above, the Working Party concludes at this point that the State of Israel has a supervisory authority for the protection of data that possesses the necessary independence and the adequate enforcement competencies, in similar terms to those provided by Article 28 of the Directive.

Enforcement and sanctioning measures

After investigating a complaint, ILITA decides whether it is justified. If so, ILITA has the power to issue compliance instructions to the database controller.

Section 31A of PPA provides a list of criminal offences in cases of infringment. It should be noted that, as aforementioned, ILITA has been granted the authority to investigate, according to its enforcement powers, those offences a previous phase or the criminal procedure sustained by the courts of justice.

In addition, ILITA has the power to impose administrative fines for the offences listed in sec. 31A and according to an annex to the *Regulations of Administrative Offenses (Administrative Fines – Privacy Protection), 2004*, which were issued by the Minister of Justice under the authority vested in him by the *Administrative Offenses Act of 1985*. The system of administrative fines allows the relevant executive to impose a fine, and allows the defendant to either pay the fine or require that a trial is held.

Together with the abovementioned sanctions, section 10 (f) of the PPA provides that *"Where the possessor or owner of a database infringes any provision of this Law or the regulations thereunder, or fails to comply with a request made to him by the Registrar, the Registrar may suspend the registration for a period that he shall determine or cancel the registration of the database in the Register, provided that prior to the suspension or cancellation the owner of the database was given the opportunity to be heard"*.

In the light of all this, the Working Party believes that the Israeli legislation has put in place the necessary elements to guarantee a good level of compliance with the rules on data protection.

> **b)** To provide **support and help to individual data subjects** in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. In order to do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

The Working Party believes that this principle is sufficiently guaranteed by the Israeli legislation. In particular, subsections (d) and (e1) of Section 10 establish the following:

> *"(d) The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, shall establish by order, a supervisory unit that will supervise the databases, their registration, and the information security therein; the unit shall be sized accordingly with the supervision needs.*
>
> *(e) The Registrar shall head the supervisory unit, and shall appoint inspectors to carry out the supervision pursuant to this Law; no person shall be appointed inspector unless he received the appropriate professional training in the field of computerization and information security and exercising powers under this Law, and the Israel Police did not object to his appointment for reasons of public safety.*
>
> *(e1) In carrying out his functions, an inspector may –*

(1) demand every relevant person to deliver to him information and documents relating to a database;

(2) enter a place as to which he has reasonable belief that a database is being operated, search the place and seize objects, if he is convinced that doing so is necessary to ensure implementation of this Law and to prevent violation of its provisions; the provisions of the Criminal Procedure (Arrest and Search) Ordinance [New Version], 5869 – 1969 shall apply to an object that has been seized under this section; arrangements for entering a military installation or an installation of a security authority within its meaning in section 19(c) shall be determined by the Minister of Justice upon consultation with the minister in charge of the security authority, as the case may be; in this paragraph, "object" includes computer material and output as defined in the Computers Law, 5765 – 1995;

(3) notwithstanding the provisions of paragraph (2), an inspector shall not enter a place that is used solely as a residence, other than pursuant to an order given by a judge of the Magistrate's Court."

c) To provide **appropriate redress** to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

Together with the previously analysed sanctioning measures, both at an administrative and at a criminal level, section 31B of the PPA states that *"An act or omission in violation of the provisions of chapters two or four or in violation of regulations enacted under this Law shall be a wrong under the Civil Wrongs Ordinance"*.

Therefore, the Working Party believes that Israeli law sufficiently guarantees the right of the data subject to be compensated for any damage infringing upon his rights or property as a consequence of the illicit processing of his personal data.

4. RESULTS OF THE ASSESSMENT

In conclusion, taking all of the above into account, the Working Party believes that **Israel guarantees an adequate level of protection** according to provision 6 of Article 25 of Directive 95/46/EC of the European Parliament and of the Council, dated 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in relation to automated international data transfers or, where they are not automated, they are subject to further automated processing in Israeli territory.

At the same time, the Working Party encourages the Israeli authorities in future legislative developments, and in particular those related to the implementation of the "Schoffman Report", to adopt provisions that envisage:

- The application of Israeli legislation to manual databases, in order to extend the adequation assessment to those cases that have not been included in the conclusions of the opinion stated herein.

- The express application of the proportionality principle in relation to the totality of personal data processing carried out by the private sector.

- An interpretation of the exemptions in international data tranfers online envisaged in Article 26(1) of the Directive.

Finally, the Working Party states that, within the framework to be established by the Decision finally adopted by the Commission, it will closely follow the measures adopted within the framework of the issues discussed above.

Done at Brussels, on 1 December 2009

For the Working Party
The Chairman
Alex TÜRK