Israel asks EU to assess its DP law for adequacy

After a short description of the Israeli data protection regime, which was passed in 1981 and amended since, **Dr Michael D. Birnhack** and **Franck Dumortier** assess the main principles of the Israeli law according to the core criteria suggested by the EU Art. 29 DP Working Party.

Article 25.1 of European Union Directive 95/46/EC prohibits transfers of personal data from Member States of the European Union (EU) to "third countries" – that is, countries outside the EU (and EEA) if the third country in question does not ensure an "adequate level of protection". The power to make binding adequacy determinations lies with the European Commission (Art 25(6)).

The principal methodological criteria for assessing the adequacy of a data protection regime are set out by the Article 29 Data Protection Working Party in WP12: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. WP12 reflects the main requirements of Directive 95/46/EC and other international data protection instruments. While the core criteria listed in WP12 do not have any formal legal standing, they serve, *de facto*, as the measure against which the adequacy of data protection regimes is evaluated.

The Israeli DP regime

The highest norm protecting privacy is found in s.7(a) of Israel's Basic Law: Human Dignity and Liberty, which provides that "All persons have the right to privacy and to intimacy." As the Israeli Supreme Court has recognised, the Basic Law elevated privacy to a status of a constitutional right. The second level in the normative pyramid is the Privacy Protection Act of 1981 (hereafter: PPA), which has been amended eight times (*PL&B International*, September 2002, pp.25-27).

Chapter 1 of the PPA applies to both manual and electronic data. It prohibits the violation of privacy of any person without that person's consent, and provides for civil and criminal liability. Chapter 2, which regulates databases, includes both a general arrangement (subchapter 1) and concrete rules regarding direct marketing (subchapter 2). Chapter 4 of the PPA contains rules about the transfer of data held by the government and other statutory bodies among themselves and to private bodies.

The PPA's database regime defines a database as "a collection of data, kept by magnetic or optical means and intended for computer processing". Manual records are thus excluded from chapter 2 of the PPA. However, manual databases are subject to the general right to privacy.

The law distinguishes between "information" and "sensitive information". "Information" is defined as details regarding a person's personality, personal status, private affairs, health, economic situation, professional qualifications, opinions and faith. "Sensitive information" includes all elements of "information" with the exceptions of personal status and professional status. Therefore, it should be underlined that the concept of "sensitive information" in Israeli law encompasses a much broader set of data than it does in the European Directive 95/46.

The PPA vests most of the powers for enforcing the data protection regime in the Database Registrar. The Registrar is appointed by the government and integrated within the structure of the Ministry of Justice and, in that sense, is part of the executive branch. However, in practice, we are unaware of any intervention with the decisions of the Registrar. Moreover, having several quasi-judicial powers (mostly the registration of databases), some of the Registrar's decisions can be appealed to a court, and all activities are subject to general judicial review under principles of constitutional and administrative law.

Is the Israeli DP regime adequate?

According to the European Commission's WP12, the concept of adequate protection differs from the concepts of equivalent protection or sufficient protection. Equivalency would have required a strict analytical comparison between the third country's legal scheme and the EU Directive. In other words, the criterion of an equivalent protection would have required third countries to adopt legislation which might be considered as an exact copy of the Directive. With the adequate protection requirement, the question is different. The use of the term "adequate" is meaningful and perfectly translates the pragmatism of the European approach.

As stated in WP12, the approach takes into account the content of the applicable regulations (the purpose limitation principle, data quality and proportionality principle, transparency principle, security principle, rights of access, rectification and right to object, restrictions on onward transfers) and the effectiveness. We examine the Israeli data protection regime according to this approach.

1. The purpose limitation principle is a central pillar of the PPA: In the context of the general right to privacy, it appears in s.2(9), which defines, as a violation of privacy, the "using or transferring information on a person's private affairs, otherwise than for the purpose for which it was given". As for databases, s.8(b) states: "No person shall use information in a database that must be registered under this section, except for the purposes for which the database was set up."

2. Accurate and up-to-date data: No explicit provision in the PPA imposes on the owner or possessor of manual data or manual databases a requirement

to update or amend inaccurate data. However, in the context of electronic databases, these principles are assured through s.14 of the PPA, which accords data subjects the right to require the amendment of data.

3. Adequate, relevant and not excessive data: Unlike article 6(c) of the European Directive, the PPA does not explicitly require that data should be "adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed", nor does the PPA contain a provision ensuring that data are only conserved for a reasonable time given the purpose for which they were collected. However, given the importance of the data subject's consent in the underlying philosophy of the law (PPA s.1 reads: "No person shall infringe the privacy of another without his consent"), one could claim that it has the same effect as the European principle. When inadequate, irrelevant or excessive data collection is required by a contract, a data subject can petition the special court on "standard contracts" and request that the contractual section be invalidated. Usually, it is the Attorney General who initiates such procedures, including in the Bank Leumi case, in which the court interfered with the standard contract on data protection issues.

4. Principle of transparency: In the context of manual data and manual databases, no explicit provision in the PPA requires a data controller to notify the data subject as to the purpose of the processing. As for the database regime, PPA, s.11 requires that an application to a person to collect information for the purpose of keeping it in a database should be accompanied by a notice, referring, *inter alia*, to the purpose of the processing and the identity of the data controller. Furthermore, a database that meets one of several situations listed in s.8(c) needs to be registered with the Database Registrar.

5. Security principle: An owner of a database, its possessor or operator, are under duty to maintain the security of the data (s.17). Data Security is defined as the "protection of the integrity of data, or protection of the data against exposure, use or copying, all when done without due permission".

6. The rights of access, rectification and objection: Israeli law accords the data subject with rights of access and rectification, accompanied with procedural guarantees. Moreover, in the context of databases having a direct marketing purpose, the PPA grants the data subjects a right to object to the processing of data relating to them.

7. Onward transfers to third countries: Special regulations address the transfer of data to databases which are located outside Israel: Regulations for Protection of Privacy (Transfer of Data to Databases outside the Country), 2001. It is evident that these regulations are inspired by the EU Directive since these are based on the same principles.

8. Sensitive data: An additional particular safeguard concerning sensitive information is the fact that if a database includes such information, this immediately triggers the duty to register the database with the Database Registrar.

9. Direct Marketing: The operation and holding of a database for the purpose of direct marketing triggers stricter regulation than a "regular" database. In addition to the duties imposed on regular databases, a direct marketing database must be registered with the Registrar. Moreover, s.17F(b) allows a data subject to object, in writing, to the processing of data relating to him, that is, the data subject can require that data referring to him or her be deleted. Alternatively, the data subject can require the database owner that the data referring to him or her will not be transferred by the database owner to third parties, for a limited time or for any time.

10. Automated decisions: Current Israeli law does not contain any specific instructions regarding automated decisions. However, it is clear that when such automated decisions are taken by a public body, they are subject to judicial scrutiny like any other executive decision.

11. Enforcement: Apart from the informal Registrar's competence to receive individual complaints, administrative and judicial routes of enforcement are foreseen. The Registrar can impose administrative fines and the PPA provides for dissuasive criminal sanctions and private civil enforcement.

Continued from p.9

its mistake and stopped sending the e-mails. Although most of the messages sent were retrieved with the help of a portal site operator, 640 had already been opened.

Coincidentally, a decision taken by a court in South Korea at the same time provided the affected bank customers with some encouragement. An online game-site operator that had managed its users' information poorly (*PL&B International*, December 2006, pp.12-13) was ordered by the court to pay 500,000 won ($500) compensation to each to game player in question. In April 2006, the court ruled that the online game company has contractual and legal responsibilities to protect the private information of game players. In other words, providers of internet-based services, such as online game operators, are required to perform a duty of special care to protect the private information of their users as they make commercial profit from their services.

The internet lottery players demanded 3 million won ($3,000) per person from the bank for the mental suffering that arose out of their private information being leaked. The total amount of compensation demanded by the plaintiffs amounted to more than 4 billion won ($4 million).

On February 8, 2007, the Seoul Central District Court held that the bank in the case of the internet lottery players should pay 100,000 won ($1,000) to each person whose name, e-mail address and national ID number were accidentally leaked. The court said that the plaintiffs suffered because their fundamental right to preserve their private information in safety was trespassed contrary to their will and that they deserved the compensation for the mental suffering they experienced. Also, the court pointed out that the bank had made every effort to stop the leakage of private information and there was no report of actual damage. Accordingly, the court limited the compensation to 100,000 won ($100) per person. The representative lawyer was disappointed to hear the court ruling but was satisfied with the court's acknowledgement that in this information society a simple leak of personal information can cause mental suffering.