

Is Israeli data protection law “adequate” under Article 25?

Dr Omer Tene, Legal Consultant and Lecturer at the College of Management School of Law, provides an update to his article in Volume 8, Issue 1 of Privacy & Data Protection Journal, regarding the adequacy of Israeli data protection compared with the European model

Following a request by the Israeli government in July 2007, the European Commission has recently launched an investigation to assess whether Israeli data protection law provides “an adequate level of protection” under Article 25 of the EU Data Protection Directive.

This article analyses Israeli law under the framework set for adequacy findings in WP 12 of the Article 29 Working Party. Despite a recent spate of changes intended to reform data protection law and increase enforcement, Israeli law lacks critical attributes of an adequate protection jurisdiction.

Sources of data protection law

Israeli data protection law is based on the constitutional right to privacy, statutory protection under the Privacy Protection Act 1981 (‘PPA’), and a set of regulations issued thereunder. Additional legislation impacts data protection on a sector specific basis, such as the Credit Reporting Act 2002, the Genetic Data Act 2000, and the Criminal Procedure Act (Enforcement Powers – Communications Traffic Data) 2007 (the ‘Communications Data Act’). Such legislation is beyond the scope of this article, which will focus on the “core” data protection framework.

Constitutional protection

The right to privacy was elevated to constitutional status in Israel in 1992, pursuant to Section 7 of Basic Law: Human Dignity and Liberty. Israeli law grants courts the power to strike down statutes that infringe on constitutional rights. The Israeli Supreme Court has held that constitutional principles apply to private sector transactions, and not solely to government action.

However, unlike the recently accepted Charter of Fundamental Rights of the European Union, Section 7 of the Basic Law does not explicitly specify a right to data protection. A constitutional amendment currently discussed in the Israeli parliament would add a data protection

right to the Basic Law.

The Privacy Protection Act

Chapter B of the PPA establishes a data protection framework and Chapter D deals with public sector data sharing. Dating from 1981, the PPA is one of the first data protection statutes in the world. A report of a Ministry of Justice committee (the ‘Shoffman Report’) proposed in January 2007 wholesale reform of the data protection statute. The Ministry of Justice is currently drafting a legislative bill amending Chapter B of the PPA based on the Shoffman Report’s recommendations.

Regulations

Certain regulations have been promulgated under the PPA, namely the Privacy Protection Regulations (Transfer of Data to Databases Outside of Israel) 2001 (the ‘International Transfer Regulations’), dealing with international data transfers; the Privacy Protection Regulations (Conditions for Data Storage and Security and Public Sector Data Sharing) 1986 (the ‘Data Storage Regulations’), dealing with data security, public sector data sharing and sensitive data; the Administrative Offences Regulations (Administrative Fine – Privacy Protection) 2004 (the ‘Administrative Fine Regulations’), imposing fines on violations of the data protection Chapter of the PPA; and the Privacy Protection Regulations (Fees) 2000, setting forth fees for the registration of databases under the PPA.

Scope of data protection law

Israel’s data protection law applies to both the public and private sectors. The PPA protects individual data subjects, explicitly excluding legal entities. It applies strictly to computerised databases and excludes databases used for purely personal, non-business purposes. In addition, the PPA does not apply to databases consisting solely of data subjects’ names, addresses and contact details; provided that such databases do not

(Continued on page 10)

(Continued from page 9)

create any characterisation of data subjects and that the data controller does not hold additional databases.

The Shoffman Report recommends extending the PPA to manual files, provided that the data therein may be accessed according to specific criteria. Such an amendment would bring Israeli law closer to the European standard, which does not distinguish between computerised and non-computerised “filing systems.”

Israeli law imposes comprehensive database registration requirements. Under Section 8(c) of the PPA, a database must be registered if it contains:

- (a) data concerning more than 10,000 data subjects;
- (b) sensitive data;
- (c) data which have been collected from third parties; or
- (d) data used for direct marketing services.

In addition, all public sector databases must be registered. Failure to meet registration requirements constitutes a criminal offence punishable by one year's imprisonment, as well as a civil tort. The Shoffman Report advocates relaxing database registration requirements on the one hand while tightening enforcement through private and regulatory means on the other.

The purpose limitation principle

Israeli law complies with the purpose limitation principle. Section 2(9) of the PPA provides: “*The following constitute an invasion of privacy: ...use or transfer of personal data for a purpose other than that for which the data have been provided.*”

Furthermore, under Section 8(b) of the PPA, “*data in a registered database shall not be used for a purpose other than that for which the database had been established.*”

The purpose limitation principle has been applied and upheld by Israeli courts, including the Supreme Court (*Database Registrar v Ventura* [1994]).

The data quality and proportionality principle

The data quality and proportionality principle is conspicuously absent from Israeli data protection law. While data subjects' right of access and rectification, which exist under the PPA, arguably ensure that data are “accurate and, where necessary, kept up to date,” the PPA does not require data to be “adequate, relevant and not excessive.”

There is no restriction under Israeli law on the collection and processing of unnecessary data; nor is there a limitation on the duration of storage. Arguably, the data quality and proportionality principle may be inferred from the general duty of good faith, which permeates Israeli civil law, and from the proportionality test imposed on any infringement upon a constitutional right. In addition, the Database Registrar may restrict the stated purpose of a database as part of the registration process. Yet the absence of these principles from data protection statute does not bode well for Israel's Article 25 adequacy finding. And the situation will not change even if the Shoffman Report's recommendations are adopted into law.

The transparency principle

Under Section 11 of the PPA, data controllers must provide individuals with information as to the purpose of the processing; the compulsory or discretionary nature of data collection; and any intended recipients of the data and purpose of transfer thereof. Section 11 does not explicitly require notification of the identity of the controller and its representative, nor of the existence of the right of access and rectification. The Shoffman Report proposes amending Section 11 to include such notifications. Hence, while not identical to European law, Israeli law appears substantially compatible in this respect and is set to move toward the European standard.

The security principle

Israeli law complies with the security principle. Section 17 of the PPA imposes responsibility for data security on data controllers, processors and

database managers (who are the managers of data controllers or officers that they appointed for the task). Section 16 of the PPA establishes a duty of confidentiality, violation of which constitutes a criminal offence punishable by 5 years imprisonment, the strictest penalty under the PPA.

To supplement the general duties set forth in the PPA, the Data Storage Regulations set forth more detailed security measures, including physical database security, rights of access, and detection of interference or distortion. The Shoffman Report proposes elaboration of the data security standard in the PPA, as well as implementation of a security breach notification requirement, similar to California's 2003 statute (SB 1386).

The rights of access, rectification and opposition

Sections 13-14 of the PPA provide data subjects with rights of access and rectification comparable to those in European law. However, there is no right of opposition allowing an individual to object to the processing of data relating to him or her, except in the context of direct marketing. In addition, individuals are not provided with the right to know the logic involved in automated decisions or to challenge, review or change such decisions.

Finally, the PPA provides broad exemptions to the rights of access and rectification for a long list of national security and law enforcement entities. Security issues, of course, are still Israel's priority; yet the exemptions in the PPA appear overly broad, for example, restricting the right of a police officer to access his or her personal file. Even if implemented, the Shoffman Report would not harmonise the PPA with European law in this respect.

Restrictions on onward transfers

The PPA restricts data transfers to third parties, including corporate affiliates, within or outside of Israel. While the PPA does not specifically address the issue of international transfers, such transfers are author-

ised under the International Transfer Regulations. Transfers to EU Member States and other signatories of Council of Europe Convention 108 are authorised under Regulation 2(8)(1).

Data exports to non-EU countries are authorised in limited circumstances, such as with data subject consent (Regulation 2(1)); from an Israeli corporate parent to a foreign subsidiary (Regulation 2(3)); or provided the data importer enters into a binding agreement with the data exporter to substantially comply with Israeli data protection law (Regulation 2(4)).

While these rules are apparently compatible with EU law, it is easy to make too much of the International Transfer Regulations. To begin with, despite potential civil liability, the Regulations do not specify a criminal sanction for non-compliance.

Consequently, in more than six years since their enactment, there has not been a single enforcement action under the Regulations. Hence, black letter law aside, Israel could very well be used as a “staging post” in data transfers from the EU to further third countries with entirely inadequate protection.

The Shoffman Report proposes rectifying the International Transfer Regulations to impose criminal sanctions on violations.

Sensitive data

Unlike EU law, Israeli data protection law does not provide additional safeguards for sensitive data, such as the requirement that processing be conditioned upon the data subject’s explicit consent.

The sole consequence of data being categorised as “sensitive,” under

Israeli law, is that a database containing such data must be registered. Consequently, Israel does not comply with the sensitive data principle. The Shoffman Report will not change the situation in this respect.

Direct marketing

Section 17F of the PPA currently imposes an opt-out regime on direct marketing, thereby complying with the requirements of EU law. A recently adopted legislative amendment harmonises Israeli law with Article 13 of the Communications Privacy Directive (Directive 2002/58/EC), providing an opt-in regime for unsolicited communications by automatic calling machines, fax, email and SMS, including a “soft” opt-in for existing customers.

Making data processing legitimate

Counter to European data protection law, which provides various criteria for making data processing legitimate, Israeli law requires informed consent, explicit or implicit, for any processing activity.

The lack of additional criteria for processing may compel controllers to solicit consent from large and diffuse groups of customers or employees for even routine business transactions or data transfers. The Shoffman Report would not

add further criteria for fair and lawful processing.

Enforcement mechanisms

Data protection rules contribute to the

protection of individual privacy only if they are followed in practice. Therefore, it is necessary to consider not only the content of Israeli data protection rules, but also the system in place to ensure their effectiveness.

Data protection supervisory authority

The PPA provides for the establishment of a data protection authority, the Database Registrar, charged with enforcing data protection law and keeping a register of databases. Nevertheless, the level of enforcement of data protection law in Israel has traditionally been low to non-existent. The Database Registrar has been under-funded and understaffed, employing less than 10 professionals, only a couple of whom were lawyers. It focused almost exclusively on verifying compliance with registration requirements – for the most part unsuccessfully. It was reactive, not proactive, and rarely engaged in litigation. In addition, it was not authorised to administer fines.

In 2006, as part of an effort to increase data protection compliance and enforcement, Israel established a new data protection authority, the Israeli Law and Information Technologies Authority (‘ILITA’). ILITA is poised to be better funded and staffed than the Database Registrar and intends to focus on proactive law enforcement. In addition, under an amendment to the Administrative Fine Regulations, ILITA is now authorised to administer fines, although these remain low (between US\$250 and US\$750).

The Shoffman Report recommends providing ILITA with additional powers and legal tools, including the authority to intervene in legal proceedings and issue general or industry-specific legal guidance.

Moreover, ILITA is scheduled to enter into a “Twinning Project” with a European data protection authority, targeted at raising Israeli public awareness, compliance and enforcement standards to a European level.

In the past few months ILITA has commenced launching uncoordinated on-site inspections. In addition, it initiated several high-profile

“Israel could very well be used as a “staging post” in data transfers from the EU to further third countries with entirely inadequate protection. The Shoffman Report proposes rectifying the International Transfer Regulations to impose criminal sanctions on violations.”

(Continued on page 12)

(Continued from page 11)

enforcement actions, including barring the use of a database containing details of disabled army veterans by a Ministry of Defence contractor, and restricting transactions in customer data linked to the divestiture by Israeli banks of their holdings in provident funds.

However, several problems remain. First, although its long-term budget was approved, ILITA has not yet been fully staffed. Despite plans to double its workforce in 2008, ILITA continues to employ around 10 professionals, not nearly enough to deal with mounting enforcement tasks. Second, and more substantially, ILITA remains subject to the authority of the Minister of Justice, and cannot act in complete independence as mandated by Article 28 of the EU Data Protection Directive.

The Ministry of Justice oversees various functions besides data protection, not least of which is prosecution of criminal offences. This may place ILITA in an awkward position. For example, in recent legislative hearings preceding the enactment of the Communications Data Act, the Ministry of Justice voiced a position attuned to the needs of the prosecution and law enforcement, despite potential privacy harms. ILITA, as a Ministry of Justice unit, cannot advance a position at odds with that of the Ministry of Justice. The Shoffman Report recommends increasing ILITA's independence, though not to the extent of its removal from the Ministry of Justice.

In light of these issues, it appears that the Israeli supervisory authority, while progressing toward European standards, is not entirely compatible with EU law. However, a similar shortcoming has not prevented Argentina from obtaining a seal of approval under Article 25.

General judicial remedies

Under Sections 31A-31B of the PPA, a violation of data protection provisions constitutes a civil tort as well as a strict liability criminal offence punishable by one year imprisonment. However, private law suits are an expensive and often time-consuming means for individuals to ensure redress under Israeli law, par-

ticularly where a data subject lives abroad.

Under a recent amendment to the PPA, plaintiffs in invasion of privacy claims are entitled in some cases to compensation without proof of damage in an amount of 50,000 NIS (US\$12,500). Although this provision does not apply to the data protection chapter of the PPA, violations of the purpose limitation principle constitute an invasion of privacy under the general privacy chapter and may qualify for statutory compensation. In addition, in order to raise incentives for private law enforcement, the Shoffman Report recommends enabling plaintiffs to file class action lawsuits for data protection violations.

Public awareness

Public awareness in Israel regarding the right to privacy, data protection and their practical implementation is low. Customers are accustomed to sign broad data use and transfer authorisations as part of standard form contracts. In its last annual report, ILITA specified that most customer complaints concern unsolicited communications and SPAM (although untargeted SPAM is not covered by the PPA and not subject to ILITA authority). The sole non-governmental organisation dealing with privacy is the Association for Civil Rights in Israel, which handles a plethora of topics, revolving mainly around the Israeli-Palestinian conflict, and is in no way dedicated to privacy or data protection.

Conclusion

To sum up, Israeli law does not protect the full set of "core" principles required under EU data protection law. More salient, compliance and enforcement levels are low, and while actions have recently been taken to reassert the position of the supervisory authority, Israel appears to fall short of the European standards required for an adequacy finding.

Dr Omer Tene
College of Management,
School of Law
tene.omer@gmail.com
