

Israel's DP law: registration, transfers abroad, employment

Dr Omer Tene outlines the Israeli approach to each of these issues, including notable recent changes and proposals for reform.

Multinational companies operating in Israel typically face several recurring data protection issues, including local database registration requirements; conditions for international data transfers; and monitoring and surveillance of employees at the workplace.

DATABASE REGISTRATION

Israel's data protection authority, the Database Registrar, has traditionally focused almost exclusively on verifying compliance with database registration requirements. The Database Registrar has seldom enforced substantive provisions of Israel's data protection statute,

Chapter B of the Privacy Protection Act (PPA), nor has it initiated civil or criminal litigation. Such an emphasis on form over substance seems set to change with the establishment in 2006 of a new data protection watchdog, the Israeli Law and Information Technologies Authority (ILITA). One of the stated purposes of the ILITA is to increase compliance and enforcement actions.

In addition, a January 2007 report of a Ministry of Justice committee (the Schofman Report) proposes wholesale reform of Israel's data protection statute (*PL&B International*, February 2007, pp.6-7). The Schofman Report focuses on relaxing database registra-

tion requirements on the one hand and tightening enforcement through private and regulatory means on the other hand. The Ministry of Justice is currently drafting a comprehensive bill based on the Schofman Report recommendations. Yet until any of the proposed changes take effect, foreign data controllers must comply with the cumbersome requirements of the current database registration regime.

The database registry in Israel is based on registration of databases, as opposed to data controllers. Hence, if a data controller has several databases that are subject to mandatory registration, such as for human resources or

Privacy Laws & Business recruitment service

Do you need a data protection specialist? Is your organisation thinking of recruiting an experienced person to deal with data protection or to strengthen an existing team?

Privacy Laws & Business will help you select suitable candidates from our list of people looking for new jobs or short-term contracts. Using our extensive international network has already proved to be more cost-efficient for companies than recruiting through agencies or the media.

For further information, contact Glenn Daif-Burns

Tel: +44 (0)20 8868 9200

E-mail: glenn@privacylaws.com

Web: www.privacylaws.com/recruitment

customer data, and suppliers' databases, it must register each separately. A person may not "control or hold" a database subject to mandatory registration without first registering it or filing an application for registration. Failure to meet registration requirements constitutes a criminal offence punishable by one year's imprisonment, as well as a civil tort.

Section 8(c) of the PPA provides that 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 or if the database is in the public sector. The term "sensitive data" is defined broadly under Section 7 of the PPA to include "details concerning an individual's personality, intimate relations, health condition, financial condition, opinions and religious belief."

The upshot of these provisions is that foreign employers typically must register their HR database with the Database Registrar. Data such as an employee's salary, benefits, withholding information, and bank account details constitute sensitive data ("details concerning a person's ... financial condition"), as do data concerning an employee's absence on maternity leave ("details concerning a person's ... health condition"). Israeli data protection law protects the privacy rights of individuals, not legal entities. Thus, a database aggregating information concerning corporate customers or suppliers need not be registered. However, if such a database also contains "sensitive data" (including financial information) pertaining to individuals, for example suppliers' employees, such a database must be registered.

INTERNATIONAL TRANSFERS

The PPA restricts data transfers to third parties, including corporate affiliates, within or outside of Israel. Section 2(9) of the PPA provides that "the use or transfer of personal data for a purpose other than that for which the data have been provided" constitutes an invasion of privacy. Similarly, Section 8(b) of the PPA provides that "data in a registered database shall not be used for a purpose other than that for which the database

had been established". As part of the database registration procedure, controllers must specify "the purposes of the processing for which the data are intended" and "the recipients of the data and purposes of any transfer". These provisions apply to data transfers in general and are not limited to international transfers.

Failure to meet registration requirements constitutes a criminal offence punishable by one year's imprisonment, as well as a civil tort.

Hence, for example, an Israeli subsidiary of a foreign corporation may be barred from transferring HR data to a corporate affiliate, even within Israel. Such a transfer may be regarded as a breach of the purpose limitation provision. To be sure, the transferor may argue that a transfer within the corporate group conforms to the original purpose of collection (that is, HR management). Yet it is risky to rely on regulatory (and possibly judicial) interpretation of the scope of the original purpose. The regulator may view the original purpose of collection as limited to processing by the transferor itself and not any affiliate thereof. The solution is to solicit employee consents.

An additional layer of regulation applies to international data transfers under the Privacy Protection Regulations (Transfer of Data to Databases Outside of Israel), 2001. The regulations are opaque and internally inconsistent. For example, they set adequacy standards for data importing countries which Israel itself does not comply with. In addition, without apparent reason, they authorise data transfers from an Israeli parent company to a foreign subsidiary, but not from an Israeli subsidiary to a foreign parent (Regulation 2(3)).

Most salient for controllers seeking to export data from Israel are the following regulations. First, Regulation 2(8)(1) permits the export of data to countries that are signatories to Council of Europe Convention 108, thereby authorising exports to European Member States. Second, Regulation 2(1) authorises international

transfers based on data subject consent. Under the PPA, such consent must be "informed" but may be "implicit". Third, Regulation 2(4) permits the export of data to parties that "enter into a binding agreement with the data exporter to substantially comply with Israeli legal requirements concerning the storage and usage of data".

Arguably, non-European companies that have entered into standard contractual clauses to comply with Article 26 of the EU Data Protection Directive satisfy Regulation 2(4), since by committing to the higher European standards they inherently accept the lesser included standards of Israeli law (*PL&B International*, February 2007, pp.10-11).

Perhaps most important for foreign controllers, the Regulations do not specify a sanction for noncompliance. And, indeed, in the more than six years since their enactment, the Regulations have not been enforced even once by the Database Registrar. This may change, however, under the new ILITA.

MONITORING AND SURVEILLANCE IN THE WORKPLACE

A recurring issue for foreign employers in Israel is the extent of permissible monitoring and surveillance of employees at the workplace. The odds have been raised by a 2007 amendment to the PPA which provides compensation without proof of damage in an amount of 50,000 NIS (\$10,000) for an invasion of privacy.

A recent decision by the Tel Aviv Labor Court outlines the contours of Israeli law in this respect. The case, *Issakof v. Panaya Ltd.* (decided 15 July 2007), involved a former employee of a high-tech company who sued her employer for unlawful discharge, alleging she was dismissed because she was pregnant. The employer denied that the pregnancy had been grounds for dismissal, arguing that the employee had been fired prior to becoming

pregnant. To substantiate its claim, the employer handed the court transcripts of e-mail correspondence in which the employee sought alternative employment before becoming pregnant. The employee argued that such evidence was inadmissible, based on Section 32 of the PPA, which sets an exclusionary rule for evidence obtained as a result of an invasion of privacy.

The court rejected the employee's claim, accepting the e-mail transcripts as evidence. While paying lip service to privacy as a constitutional right and to an employee's right to privacy at the workplace, the court approved pervasive monitoring by the employer not only of the traffic but also of the contents of employee communications. The decision is based on purported implicit consent by the employee to the employer's monitoring. Such consent was gleaned from the fact that the employer advised employees of its policy of monitoring e-mails to prevent misuse of corporate trade secrets and

protect the system from viruses and security risks. The court rejected another argument of the employee, which was based on a 1997 Labor Court precedent (*Tel Aviv University v. The Histadrut Labor Union*) that in the context of an employment relationship, employee consent is not freely given and should therefore be disregarded.

The court held that employers may generally monitor traffic data, as opposed to the contents of employee communications. However, monitoring of contents would be authorised, as indeed it was in *Issakof* itself, where it is proportional under the circumstances. In assessing proportionality, the court examines a line of factors, such as checking whether the employer established clear monitoring guidelines which were brought to the attention of employees; whether the employee consented to the monitoring implicitly, explicitly, orally or in writing; what the nature is of the employer's business (a

bank, for example, will be treated differently than a pizzeria); what the nature is of the employee's position in the employer's business (a bank's credit chief, for example, may warrant closer scrutiny than the bank's cleaner).

While the *Issakof* court settled for implicit employee consent, employers are advised to obtain explicit employee consent, if possible in writing, to fend off allegations of invasion of privacy. Employers should circulate a clear policy that specifies the extent and methods of monitoring at the workplace. Finally, employers should employ no more monitoring than is necessary given the nature of their business and the risks of wrongdoing by employees.

AUTHOR

Dr Omer Tene is a lecturer at the College of Management School of Law, Rishon Le'zion, Israel, and a legal consultant.
E-mail: tene.omer@gmail.com

Israel's Databases Registrar bans use of personal data by the Ministry of Defence

For the first time since the enactment of the Protection of Privacy Law 5741-1981 in Israel, the Databases Registrar in the Ministry of Justice, which is the personal data protection regulator according to the personal data protection chapters of the Law, has intervened and suspended the use of a registered database of a government ministry.

Advocate Yoram Hacoen, the head of the new Israeli Law, Information and Technology Authority (ILITA) and the Databases Registrar ordered in the first week of September that the Rehabilitation Wing in the Ministry of Defence and Pemi Premium Co. to stop making use of the database, which holds data regarding the medical condition of disabled IDF veterans. This order resulted from a recent supervision performed by the unit during which the inspectors found that the sensitive data was not adequately secured.

The database which is banned from use is held by Pemi Premium Co., which performs, for the Ministry of Defence by outsourcing, processing of

privacy protected data, on a large scale, regarding disabled IDF veterans, such as their medical condition and the treatments they underwent.

Following a complaint received by the unit regarding the legality of the transfer of data from the Ministry of Defence to Pemi Premium Co., the supervision was performed in the company's facilities by supervisors of ILITA, in order to check its compliance with the Law. During that supervision, the sensitive data was found to be not adequately secure, as required for data which is sensitive to this degree.

In addition, the authority's supervisors found a lack of compliance with the guidelines set by the Ministry of Defence, which were detailed in the tender's document and were one of the conditions for the selection of Pemi Premium to provide these services. For example, the company did not perform a reliability test for personnel working in the project team, and some data was transferred to external bodies without informing the Ministry of Defence.

Since this conduct did not improve to the satisfaction of the Registrar, he has ordered the Ministry of Defence that until all the deficiencies are rectified, the database is banned from use in any way. By this, the ILITA, which was established recently in the Ministry of Justice, is starting to use its powers under the Protection of Privacy Law towards government ministries as well.

Yoram Hacoen, the head of ILITA and the Registrar of Databases, said: "The Protection of Privacy Law equally applies to private and public sector bodies. In some aspects, the law is even stricter with the public bodies, which usually collect data by law and without explicit consent to use the data by the data subjects. Public authorities must follow much more strict rules in regards to safeguarding the privacy of citizens and the personal data which is kept about them in governmental databases. Government ministries which fail to do so will be banned from using the database."

• By the Databases Registrar's Office