Israel's data protection reform

Omer Tene, member of the Israeli Ministry of Justice "Schoffman" Committee for reform of data protection legislation, ***explains why reducing bureaucracy and increasing accountability is key. In doing so, he considers some criticisms of the European Data Protection Directive.***

The European Data Protection Directive ('the Directive) is seen by many as rigid and overly bureaucratic. Its notification requirements and restrictions on international transfers have drawn much criticism from the business community in recent years. Given that, alongside the protection of privacy, the goal of the Directive is "to remove the obstacles to flows of personal data," excessive formalities and regulatory restrictions appear counterproductive. Similar arguments have been raised concerning Israel's data protection statute, Chapter B of the Privacy Protection Act, 1981 ('PPA').

Israel is currently redrafting the PPA to account for changes in markets and technologies over the past 28 years. The reform will be based on the recommendations of a Ministry of Justice Committee headed by former Deputy Attorney General Joshua Schoffman. In this article, it is suggested that reducing bureaucracy and increasing accountability should be an organising principle for the new legislation. This essentially means replacing before-the-event, or 'ex ante', regulatory pre-conditions to processing, with after-the-event, or 'ex post', review and liability.

There is broad global consensus on substantive data protection principles, such as purpose limitation, proportionality, transparency, and security. Article 6 of the Directive is not wholly different from equivalent provisions in the guidelines from the Organisation for Economic Cooperation and Development, the Council of Europe Convention 108, and Israel's PPA – all three dating back to 1981; Canada's Personal Information Protection and Electronic Documents Act ('PIPEDA'); Australia's Privacy Act; and the Asia-Pacific Economic Cooperation ('APEC') Privacy Framework.

Yet certain procedures of implementation of these common data protection principles have proven highly contentious, and are seen as overly burdensome without generating proportional benefits to data subjects. For example, in its Review of the European Data Protection Directive sponsored by the UK Information Commissioner's Office, RAND Europe states that "[f]or their part, Independent Supervisory Authorities will need to adopt an approach that is less focused upon process and formality checking, but instead aims for more effective enforcement and ensuring accountability."

The approach described by RAND Europe could be implemented in Israel's new legislation by lessening database registration duties and limits on international data transfers, while increasing private and regulatory enforcement powers.

Replacing notification with internal audits

The PPA sets forth broad database registration requirements. Section 8(c) of the PPA provides that a database must be registered if it contains:

- data concerning more than 10,000 data subjects;
- sensitive data;
- data which have been collected from third parties;
- data used for direct marketing services; or
- data in a public sector database.

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." Consequently, HR databases, for example, must be registered regardless of the number of employees in an organisation, since they typically contain financial and often health related data.

Registration obligations impose an onerous bureaucratic burden on controllers and regulators alike, yielding minimal benefits to data subjects, and diverting resources from substantive enforcement to technical compliance measures. Despite best regulatory efforts, the proportion of databases registered under the PPA remains trivial, and is estimated to account for only 2% of the number of databases subject to registration obligations. Similar figures have been documented in

(Continued on page 14)

(Continued from page 13)
the EU.

The Schoffman Committee recommended amending the legislation on registration. It proposed significantly narrowing registration obligations, making them the exception rather than the rule. In order to maintain the benefits of registration, namely requiring controllers to map their data flows and providing regulators with an initial enforcement tool, while at the same time reducing administrative costs on controllers and regulators, registration could be replaced with a duty to conduct internal audits (or privacy impact assessments), and maintain records thereof. The regulator could then be provided with the authority to request access to such records, thereby gaining preliminary insight into the processing activities of a data controller.

Additional measures may be put in place to increase transparency and provide regulators with valuable information. For example, publicly traded companies or a high risk subset thereof (e.g. financial services, health care, data wholesalers), may be required to include their data protection records, security breach notifications, and pending data protection complaints in their financial reports. This would subject such records not only to audit by trusted third parties (such as certified public accountants), but also to the jurisdiction of securities regulators and potential class action lawsuits. An integrated approach to regulation, relying on the resources and know how of securities, antitrust, consumer protection, and labour market regulators, as well as private litigants, would greatly enhance data protection compliance.

By reducing bureaucracy and increasing accountability, the costs of data protection compliance are minimised, whilst benefits to individual data subjects maintained.

"The approach described by RAND Europe may be implemented in Israel's new legislation by lessening database registration duties and limits on international data transfers, while increasing private and regulatory enforcement powers."

Replacing international transfer restrictions with accountability

The European adequacy model for international data transfers has proven to be not only cumbersome, but also highly contentious. Assessing the adequacy of a foreign legal regime is a delicate exercise, given that review of statutes and regulations may yield misleading results. For example, solid democracies with a long heritage of privacy jurisprudence and culture, such as the US and Australia, may harbor a robust data protection regime even if their laws deviate in certain respects from the EU framework; whereas countries that have emulated the Directive without having the democratic and regulatory institutions to implement it, may have more privacy on their books than on the ground.

European data transfer rules have proven to be outmoded and ineffective. Even potentially useful instruments, such as Binding Corporate Rules and standard contractual clauses, are drowning in red tape and long regulatory response times. Here too, outmoded ex ante controls and prior checking should make room for ex post accountability. This is absolutely essential to accommodate the ubiquity of international data transfers at a time where every businessman carrying a Blackberry transfers numerous databases across borders.

Israel is reconsidering its own model for international data transfers, which is set forth in the Privacy Protection Regulations (Transfer of Data to Databases Outside of Israel), 2001 (the 'Regulations'). Section 1 of the Regulations largely replicates the European adequacy framework. It permits data transfers to countries "whose law provides a level of protection for personal data that is no lesser than that under Israeli law."

Needless to say, adequacy analysis, a thorny undertaking in the EU, is outright unrealistic for a small country such as Israel. Just consider the prospect of Israeli regulators having to assess the adequacy of the Mongolian or Congolese data protection regime.

Taking a constructive approach to interpretation, sections 2 and 3 of the Regulations adopt an accountability model. Section 2 of the Regulations permits international data transfers under certain conditions, e.g. the informed consent of the data subject; transfers from an Israeli parent company to a foreign subsidiary; or subject to a contract "obligating the transferee to comply with the conditions for storage and use of data under Israeli law." Section 3 of the Regulations provides:

"In a data transfer under Regulation 1 or 2, the data exporter will ensure, by obtaining the data importer's written undertaking, that the data importer implements sufficient safeguards to protect data subjects' privacy and promises to refrain from any onward transfer."

Such an undertaking is required regardless of the legal basis for the transfer. Hence, in any event, the Israeli controller remains accountable for the data, even if a legal basis for the transfer exists. That is why Israel views favourably an accountability regime, similar to that in Section IX of the APEC Privacy Framework and Clause 4.3 of Schedule 1 of the Canadian PIPEDA, which provides:

"An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall

use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

Canada is regarded as an adequate jurisdiction under Article 25 of the Directive, despite not subjecting international data transfers to prior restraints. An accountability regime would make controllers responsible for all personal data in their possession, including data that have been transferred to third parties abroad, and impose a requirement to employ contractual mechanisms, corporate codes of conduct or other means to provide a comparable level of protection while the data are being used by such third parties.

This approach is more realistic than the adequacy model, in view of current technological possibilities and business demands, yet holds the data exporter accountable under local data protection law.

Strengthening enforcement

In order to increase data protection compliance while at the same time relaxing ex ante restrictions, enforcement must be reinforced ex post. Indeed, the elimination of bureaucratic burdens tied to database registration and international data transfers would free up regulatory resources for reallocation to proactive enforcement.

Consequently, if legislative amendments to the PPA reduce regulatory formalities, they would have to concurrently strengthen the data protection authority's enforcement powers. Effective enforcement must be based on a multi-pronged strategy, combining private and regulatory enforcement and providing the regulator with a comprehensive enforcement "toolbox."

Regulatory enforcement

The data protection regulator should benefit from a mix of the following enforcement powers:

- search and seizure, including the power to conduct spot checks and seize computers and computer data;
- enforcement notices and enforcement undertakings;
- administrative fines and civil penalties, assessing monetary sanctions based on risk of harm analysis, including the severity of the violations, the scale of processing, the sensitivity of the data, and the sector of activity of the controller (e.g., financial services or healthcare); and
- collaboration with additional regulators. Moreover, integrating data protection into corporate governance, for example, by mandating public disclosure of internal privacy audits would enhance the effectiveness of regulatory enforcement. Securities regulators, antitrust authorities, and employee and consumer protection agencies would thus collaborate with data protection regulators, creating a seamless web of regulation that is difficult to circumvent.

Private enforcement

Private enforcement can provide a strong deterrent against data protection violations.

In the US, despite the lack of an omnibus data protection statute or a dedicated regulatory agency, data subjects have benefited from a degree of protection due to the incidence of class action lawsuits and civil claims.

Given that data protection regulators are often inundated with complaints and advisory work, the privatisation of enforcement can greatly enhance regulatory reach.

The Schoffman Committee recommended introducing a security breach notification requirement into the PPA. Oftentimes, breach notification is a precondition for private enforcement, since in the absence of notice data subjects are not aware of the harm inflicted by imprudent controllers. Yet breach notification requirements must be carefully tailored to avoid a deluge of notices that would desensitise data subjects and impose bureaucratic burdens on controllers and regulators alike.

In 2007, the PPA was amended to provide statutory damages for privacy infringements in an amount of up to 50,000 NIS (€10,000). Statutory damages provide potential plaintiffs with an incentive to file law suits, particularly where damages are difficult to quantify as is often the case in privacy litigation. Israeli courts have awarded statutory damages in an increasing number of privacy cases.

Class action lawsuits serve as a potent deterrent against wrongdoing by business. Class actions are well suited for data protection causes of action, which are typically characterised by small individual harms diffused across a large group of consumers, employees, or citizens. The extent of damages may be difficult to quantify and harms may be too small to bother with on an individual basis. Finally, although it is an ex post remedy for harms already inflicted, the threat of a class action law suit can provide controllers with a strong ex ante incentive to comply with the law in order to avoid uncertain, hefty damages rewards.

Conclusion

Technological developments and business realities have rendered certain procedural aspects of the EU data protection regime and the Israeli PPA obsolete. Substituting bureaucratic compliance mechanisms with an accountability and liability regime would revitalise data protection compliance and free up regulatory resources to enforce the important substantive principles of data protection

Omer Tene
College of Management School of Law
omer.tene@bezeqint.net