Changes ahead for Israel's DP law to bring it in line with EU Directive

The Israeli Data Protection regime is constantly revised. In January, an expert committee recommended further changes. By **Dr Michael D. Birnhack** and **Franck Dumortier**.

The first change took place in August 2006 by means of the establishment of a new agency in the Ministry of Justice, in charge of legal aspects of Information Technology. Under the auspices of the new agency, the enforcement efforts regarding data protection are revised and accelerated. Although the new agency is located within the administration of the Ministry, it is designed to be independent in its activities, ranging from policy making to concrete actions.

The second change is the publication of the *Schoffman Report* in January 2007, based on an expert's committee that considered the matter for two years. The committee was chaired by the Deputy Attorney General Mr Yehoshua Schoffman and members included representatives of the government, academia, private sector and non-governmental organisations. The report was particularly influenced by the European and Canadian data protection regimes. It is now open to public comments and is likely to result in a governmental Bill to amend the Privacy Protection Act. The main recommendations of the report are:

Manual databases: The report proposes to extend the data protection regime to cover manual personal filing data systems. Accordingly, the report proposes to redefine a database: "A database is any set of personal data, which is accessible according to specific criteria." The language is very similar to that used in the EU Directive.

Personal data: The report proposes redefining "personal data" to mean "any information relating to an identified person or to a person who can be identified using reasonable measures". The Committee explicitly refrained from defining "sensitive data" as its only effect would be to trigger the registration of a database. The Committee was of the opinion that the sensitivity of the data can be a relevant consideration in judicial evaluation of violations of privacy.

Registration duty: The report proposes narrowing the situations where there is a duty to register a database with the Database Registrar, a process which is similar to the European notification requirement. The Committee was of the opinion that the current registration requirement is overbroad, impractical and has, *de facto*, failed. Accordingly, registration will be required when data are commercially traded or, in cases of sensitive data, is yet to be clarified. The report recommends that the Minister of Justice will be able to determine the kind of databases subject to the duty or exempt from it and that the Database Registrar has a similar authority regarding individual databases.

Stronger enforcement: The report proposes strengthening the powers of the Database Registrar, regarding the following: general enforcement powers, issuing binding rules, issuing individual orders regarding data security, receiving complaints from data subjects and acting upon them, and redefining the position as a Database Commissioner. All members of the Committee were of the opinion that these are much needed steps. A majority recommended that the Registrar be accorded independent status to join litigation regarding data protection, without being subject to the Attorney General's authority. The report further proposes to allow class actions. Current Israeli law enables such actions only in consumer-related settings. The recommendation would enable class actions also when the database operator is the state or an employer.

Data collector's duties: The report proposes not to add general duties to those already imposed on data collectors. A minority of the committee proposed that an explicit requirement be added, regarding the adequacy, relevancy and excessive collection of data. It also proposes broadening the notice requirement so that a collector should notify the data subject of the exact source of the duty to provide information, and of the data subjects' rights regarding the collector and means of contacting the collector.

Data security: The report proposes (1) to clarify that the duty to undertake data security measures is to be assessed according to a reasonability standard, (2) to authorise the Database Registrar to issue individual orders regarding data security and (3) to impose a duty on a collector to inform data subjects in case of a database security breach.

Access rights. The report proposes to widen the scope of the right of a data subject to access the data about oneself to cover the kind of personal data, the sources of the data, whether the personal data is transferred to third parties, to whom and for which purposes. The cost of the access to the data shall be pre-determined by the law but subject to the review of the Database Registrar.

Transfer to third countries: At the proposal of the Committee, the Ministry of Justice and the Ministry of Foreign Affairs approached the European Commission with a request that the adequacy of the Israeli data protection is assessed, under article 25(2) of the 1995 Directive.

Continued on p.7

Continued from p.1

ECB as a data controller, jointly with SWIFT. He uses his power under the regulation regarding personal data processing by EU institutions to urge the ECB to explore "solutions to make its payment operations fully compliant with data protection legislation and take appropriate measures as soon as possible". He invites the ECB to report back on the measures taken to comply with his opinion by April at the latest. After receiving this report, he will consider "taking into account possible coordination with other data protection supervisory authorities, any further action" on the basis of his powers. The further action obviously could include the imposition of sanctions.

Considering the ECB as policy maker he "stresses that it would not be acceptable that the architecture of the European payment systems would continue to allow and facilitate that personal data relating to any euro payment between Member States are transferred to third countries in breach of the data protection legislation and made available – routinely, massively and without appropriate guarantees – to third countries' authorities". He calls on the ECB "to ensure that European payment systems… are fully compliant with European data protection law".

He concludes that "a wide range of EU and international instruments aimed at fighting crime and terrorism while ensuring protection of fundamental rights are already available" and should be fully exploited before proposing new international agreements. "In any case, the fight against crime and terrorism should not circumvent standards of protection of fundamental rights which characterise democratic societies," he adds.

In his Opinion, the Supervisor remarks that "lack of compliance with data protection legislation may actually hamper … the financial stability of the payment system for at least two reasons: first of all, it could seriously affect consumers' trust in their banks; secondly, it might lead European data protection authorities, as well as judicial authorities, to use their enforcement powers to block the processing of personal data which are not in compliance with data protection law".

This follows a ruling by the data protection authority in Belgium (*PL&B International*, December 2006, pp.1-4), where SWIFT is located, that the secret and continuing disclosure by SWIFT of personal data regarding financial transactions to the US Treasury violated national data protection laws and the European Union Data Protection Directive. The Article 29 Working Party, whose members include all EU national data protection authorities and the Supervisor, also reached the same conclusion in November. There are no sanctions for violating the Directive itself, and neither the Article 29 Working Party nor the Supervisor has the power to impose sanctions. However, the effect of the Working Party's emphatic opinion in November and the Supervisor's equally strong opinion means that if there is no change in the arrangement between SWIFT and the US government when the ECB reports back by April, there is a strong possibility that the Belgian data protection authority may impose sanctions on SWIFT, and that other national data protection authorities may impose coordinated sanctions on banks using SWIFT for communicating their customers' financial transactions.

The Luxembourg Data Protection Commission has already (in December) been assured by banks in that country that "they are actually taking actions in order to ensure compliance with EU law". The Commission has said: "Enforcement could be envisaged in case the current situation remains unchanged. However, we trust that SWIFT and the financial institutions alike will be convinced of the necessity to comply with EU law with regard to SWIFT's transfers to the United States Treasury and will take the necessary steps to achieve this goal."

Australian Commissioner also investigates

In Australia, following a complaint by the Australian Privacy Foundation, the Federal Privacy Commissioner has commenced an investigation of the actions of Australian financial institutions in disclosing personal information. to the SWIFT inter-bank network, particularly once these institutions became aware of SWIFT's disclosures of personal information to the US government. Resolution of this investigation may involve the Commissioner having to consider whether the US provides protection to privacy comparable with that provided by the data export restriction principle (NPP 9) in the Privacy Act 1988's National Privacy Principles.

FURTHER INFORMATION

See www.privacy.org.au/Papers/SWIFT-AustbanksOFPC061012.pdf.

Continued from p.6

Conclusion

From a European point of view, the data protection regime of third countries should be assessed under the core criteria of adequacy, as stated by the 1995 Directive and interpreted by the Article 29 Working Party. As the criterion of "adequate protection" conceptually differs from "equivalent protection", one should not expect the Israeli law to be exactly identical to the law in the Member States. Nonetheless, the *Schoffman Report*'s recommendations would bring, if enacted, the Israeli regime much closer to the EU's regime and to the wording of Directive 95/46/EC. Moreover, the recent establishment of the Agency for Legal Aspects of Information Technologies promise a substantial strengthening of the enforcement of the data protection regime in Israel.

AUTHORS

Dr Michael D. Birnhack is Senior Lecturer and Co-Director of the Haifa Center of Law & Technology, Faculty of Law, University of Haifa, Israel.
E-mail: michaelb@law.haifa.ac.il, website: http://techlaw.haifa.ac.il
Franck Dumortier is Researcher at CRID (Center for Computers and Law), University of Namur, Belgium. E-mail: Franck.dumortier@fundp.ac.be, website: www.crid.be